©2026 Romanian Association of Nonconventional Technologies

OPERATIONALIZING ETHICAL AND REGULATORY STANDARDS THROUGH THE INTEGRATION OF ISO/IEC 42001 ON ARTIFICIAL INTELLIGENCE IN RISK-AWARE AUTONOMOUS NONCONVENTIONAL TECHNOLOGIES

Claudiu Florin Iuonas[1], Aurel Mihail Titu[2,3] and Dan Nitoi[4]
[1]National University of Science and Technology POLITEHNICA Bucharest, 313 Splaiul Independenței, Bucharest, Romania, ORCID No. 0000-0001-8031-3212, f.iuonas@outlook.com
[2]Lucian Blaga University of Sibiu, 10 Victoriei Street, Sibiu, Romania, Corresponding author, ORCID No. 0000-0002-0054-6535, mihail.titu@ulbsibiu.ro
[3]Academy of Romanian Scientists, 3 Ilfov Street, Bucharest, Romania
[4]National University of Science and Technology POLITEHNICA Bucharest, 313 Splaiul Independenței, Bucharest, Romania, ORCID No. 0000-0002-8929-2059, dan.nitoi@upb.ro

ABSTRACT: The accelerated development of artificial intelligence has introduced a growing disconnect between technological capabilities and the governance mechanisms required to manage them responsibly. While AI systems are increasingly deployed in critical domains, the lack of structured and unified governance approaches raises concerns related to accountability, transparency, and regulatory compliance.This paper proposes a conceptual and operational framework that integrates ISO/IEC 42001, as a management system standard for artificial intelligence, with the European Union Artificial Intelligence Act, which introduces a risk-based regulatory model. The objective is to move beyond theoretical principles and provide a structured approach for embedding ethical and regulatory requirements into the lifecycle of AI systems. The proposed solution is based on a layered governance model, designed to separate strategic decision-making from operational execution and real-time monitoring. In addition, a risk-based audit methodology is introduced to support continuous validation and early detection of deviations. The paper argues that the integration of management standards with regulatory frameworks creates a more coherent and actionable governance structure, particularly in the case of complex and adaptive AI systems. The approach contributes to the development of trustworthy AI by offering a practical pathway for aligning innovation with accountability.
KEYWORDS: Artificial Intelligence Governance, ISO/IEC 42001, EU AI Act, Risk-Based Audit, Trustworthy AI

1. INTRODUCTION

Artificial intelligence has transitioned from an experimental technology to a core component of modern digital systems. Its applications now extend across domains where decisions have significant economic, social, and operational consequences. While these capabilities offer substantial benefits, they also introduce new categories of risk that traditional governance mechanisms are not fully equipped to handle[1] [10].

One of the main challenges is the lack of a unified approach to AI governance. Existing practices are often fragmented, combining internal policies, external guidelines, and ad-hoc compliance measures. This fragmentation leads to inconsistencies in how AI systems are designed, monitored, and evaluated [2].

Another issue is the gap between ethical principles and practical implementation. Concepts such as fairness, explainability, or human oversight are widely discussed in academic and policy contexts, yet their translation into operational processes remains limited. In practice, organizations often lack clear procedures for embedding these principles into system design and lifecycle management [3]. At the same time, the increasing autonomy of AI systems complicates governance even further. Systems that adapt over time or operate in distributed environments cannot be effectively controlled using static rules or periodic audits. Instead, they require continuous monitoring and dynamic validation mechanisms. In response to these challenges, this paper proposes an integrated framework that combines a management system perspective with a regulatory, risk-based approach. The goal is to provide a structured method for operationalizing governance, rather than simply defining it.

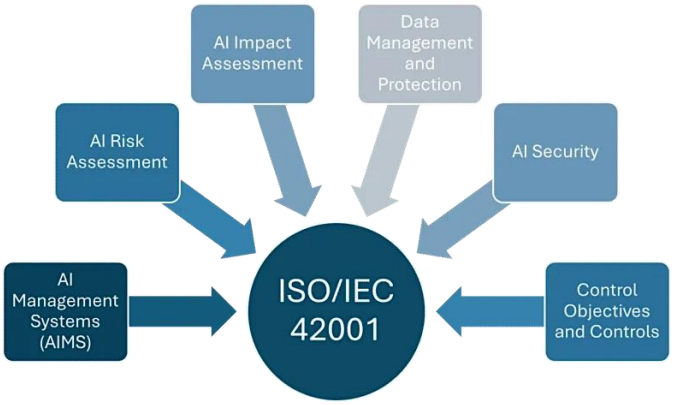

Figure 1. Core components of ISO/IEC 42001 Artificial Intelligence Management System (AIMS) and their role in supporting governance, risk management, and regulatory alignment.

Source: Glocert International

As illustrated in Figure 1, ISO/IEC 42001 provides a structured framework that integrates key components such as risk assessment, impact evaluation, data management, and security controls. These elements form the operational foundation required to support governance and ensure alignment with regulatory requirements.

2. RESEARCH CONTEXT AND RELATED WORK

The need for trustworthy AI has been widely recognized in both academic research and policy development. Various international initiatives have introduced principles aimed at ensuring ethical and responsible AI deployment [4]. However, these initiatives often remain at a conceptual level.

A recurring limitation in existing work is the lack of operational integration. While ethical guidelines define what should be achieved, they rarely explain how these objectives can be implemented within organizational processes. This creates a disconnect between strategic intent and technical execution [5] [11].

In addition, regulatory frameworks are evolving rapidly, particularly in the European context. The introduction of risk-based classification systems represents a significant step forward, yet it also increases the complexity of compliance. Organizations must not only understand the requirements but also demonstrate that their systems meet them [6] [12].

Another important aspect highlighted in recent research is the need for continuous validation. Traditional governance models rely on periodic assessments, which are insufficient for systems that evolve over time. This has led to increased interest in audit mechanisms that operate throughout the system lifecycle.

The present work builds on these observations by proposing a model that combines structured management processes with regulatory alignment and continuous auditing.

3. ISO/IEC 42001 AND THE EU AI ACTENHANCED PROJECT PRIORITIZATION MECHANISMS

ISO/IEC 42001 introduces a management system specifically designed for artificial intelligence. Its purpose is to provide organizations with a structured approach to governing AI systems, similar to existing standards for quality or information security.

A key feature of this standard is its focus on process integration. Rather than treating governance as a separate function, it embeds it within the operational structure of the organization. This includes defining responsibilities, establishing control mechanisms, and implementing continuous monitoring processes.

The standard also emphasizes risk management as a central component. Organizations are encouraged to identify, assess, and mitigate risks associated with AI systems in a systematic manner. This aligns well with the needs of complex and adaptive systems, where risks are not always predictable in advance.

3.1 ISO/IEC 42001 Overview

ISO/IEC 42001 introduces a management system specifically designed for artificial intelligence. Its purpose is to provide organizations with a structured approach to governing AI systems, similar to existing standards for quality or information security [7] [13].

A key feature of this standard is its focus on process integration. Rather than treating governance as a separate function, it embeds it within the operational structure of the organization. This includes defining responsibilities, establishing control mechanisms, and implementing continuous monitoring processes.

The standard also emphasizes risk management as a central component. Organizations are encouraged to identify, assess, and mitigate risks associated with AI systems in a systematic manner. This aligns well with the needs of complex and adaptive systems, where risks are not always predictable in advance

3.2 The European Union AI Act

The EU AI Act introduces a regulatory framework based on the classification of AI systems according to their level of risk. This approach recognizes that not all AI systems require the same level of control [8] [14].

High-risk systems are subject to strict requirements, including documentation, traceability, and ongoing monitoring. These requirements are designed to ensure that systems operating in critical contexts remain transparent and accountable.

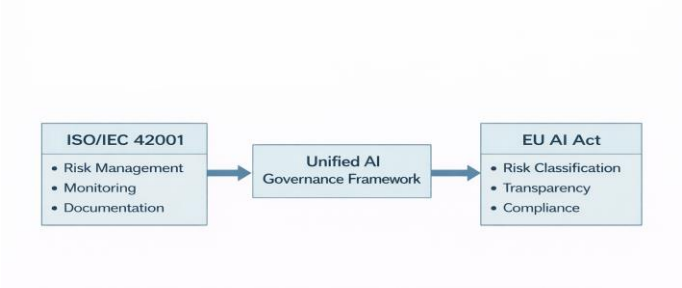

Figure 2. Conceptual integration between ISO/IEC 42001 management system and EU AI Act regulatory requirements.
Source: Personal Creation

As illustrated in Figure 2, the integration between ISO/IEC 42001 and the EU AI Act creates a unified governance framework that connects internal management processes with external regulatory requirements.

3.3 Complementarity Between Standard and Regulation

The management system and the regulatory framework address different aspects of governance. The standard focuses on internal processes, while the regulation defines external obligations.

When combined, they create a complementary structure. The standard provides the mechanisms needed to implement the requirements defined by the regulation. This reduces ambiguity and supports a more consistent approach to compliance.

Table 1. Mapping between ISO/IEC 42001 and EU AI Act requirements

ISO/IEC 42001 Element	EU AI Act Requirement	Purpose
Risk Management	High-risk classification	Risk control
Documentation & Traceability	Transparency	Accountability
Monitoring	Post-market surveillance	Continuous compliance
Control Mechanisms	Conformity requirements	Regulatory alignment

The relationship between management system components and regulatory requirements is summarized in Table 1.

4. PROPOSED LAYERED GOVERNANCE MODEL

The proposed governance model is designed to address the complexity of modern AI systems by organizing responsibilities across multiple levels. Unlike traditional governance approaches, which often rely on static controls, this model introduces a dynamic and structured framework that enables continuous alignment between strategic intent, operational execution, and real-time system behavior.

By separating decision-making into distinct layers, the model ensures clarity of responsibilities while maintaining strong interconnections between them. This structure is particularly relevant in the context of adaptive and autonomous AI systems, where governance must evolve alongside system behavior.

4.1 Strategic Layer

The strategic layer is responsible for defining the overall direction of AI governance within the organization. It operates at the highest level of decision-making and establishes the foundation upon which all other governance activities are built.

This layer includes the definition of governance policies, ethical guidelines, and compliance objectives. It also ensures alignment with external regulatory frameworks, such as the EU AI Act, as well as internal organizational values and risk tolerance. At this level, key decisions are made regarding the acceptable use of AI technologies, prioritization of initiatives, and allocation of resources.

In addition, the strategic layer plays a critical role in risk anticipation. Rather than reacting to issues after they occur, it focuses on identifying potential areas of concern and defining preventive measures. This proactive approach is essential for maintaining control over complex AI systems.

Another important function of this layer is stakeholder alignment. It ensures that executive management, compliance teams, and technical departments share a common understanding of governance objectives. Without this alignment, governance efforts may become fragmented and ineffective.

4.2 Operational Layer

The operational layer translates strategic objectives into concrete processes and technical implementations. It represents the bridge between high-level governance decisions and the actual functioning of AI systems.

At this level, governance is embedded into system design, development, and deployment processes. This includes the implementation of risk management procedures, data governance frameworks, and control mechanisms that ensure system behavior remains within defined boundaries.

The operational layer is also responsible for maintaining documentation and traceability. This is particularly important in regulated environments, where organizations must demonstrate how decisions are made and how risks are managed. By ensuring that all relevant processes are properly documented, this layer supports both internal oversight and external audits.

Furthermore, the operational layer enables consistency across systems. By standardizing processes and controls, it reduces variability and ensures that governance principles are applied uniformly. This is especially valuable in large organizations or distributed environments, where multiple AI systems may operate simultaneously.

4.3 Tactical Layer

The tactical layer focuses on real-time monitoring, validation, and response. It operates at the execution level and is directly connected to the behavior of AI systems in production environments.

This layer enables the continuous observation of system performance, allowing organizations to detect deviations from expected behavior. These deviations may include performance degradation, unexpected outputs, or violations of predefined constraints.

A key characteristic of the tactical layer is its responsiveness. Unlike higher layers, which focus on planning and design, this level is concerned with immediate action. When anomalies are detected, corrective measures can be applied quickly, minimizing potential impact.

The tactical layer also supports adaptive decision-making. In dynamic environments, where conditions change rapidly, static controls are not sufficient. Continuous monitoring allows systems to be adjusted in real time, ensuring that governance remains effective even as the system evolves.

In addition, this layer provides valuable feedback to higher levels. Insights generated through monitoring and validation are used to refine both operational processes and strategic decisions.

4.4 Integration Mechanism

The effectiveness of the proposed governance model depends on the interaction between the three layers. While each layer has distinct responsibilities, they are not independent. Instead, they form an interconnected system supported by continuous information flow.

The integration mechanism ensures that decisions made at the strategic level are properly implemented at the operational level and validated at the tactical level. At the same time, feedback from the tactical layer is used to improve both operational processes and strategic policies.

This creates a closed-loop governance system, where information circulates continuously between layers. Such a structure enables continuous improvement and allows organizations to adapt to new risks, regulatory changes, and technological developments.

Moreover, the integration mechanism supports consistency and traceability. By maintaining clear connections between decisions and outcomes, it becomes easier to understand how governance actions influence system behavior. This is particularly important for accountability and auditability.

Overall, the integration of layers transforms governance from a static framework into a dynamic process, capable of evolving alongside AI systems and ensuring long-term sustainability.

5. VALIDATION AND RISK-BASED AUDIT METHODOLOGY

The validation methodology proposed in this paper is based on the principle that governance must be continuous rather than episodic [9].

The process begins with the classification of AI systems according to risk. Based on this classification, appropriate controls are applied. Monitoring mechanisms are then used to track system behavior over time.

An important aspect of this approach is the combination of automated and human-driven processes. Automation allows for scalability and efficiency, while human oversight ensures contextual understanding and ethical judgment.

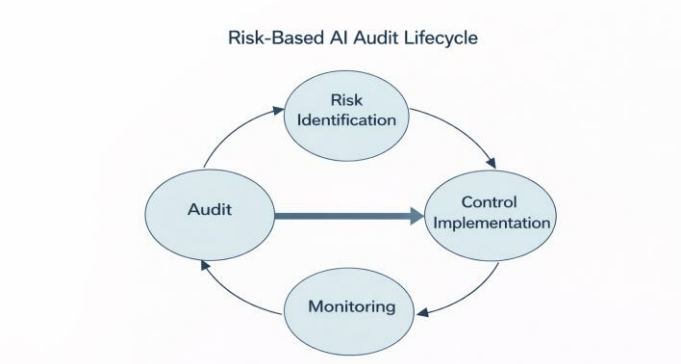

Figure 3. Risk-based AI audit lifecycle applied to AI systems. Source: personal creation

Corrective actions are triggered when deviations are detected, ensuring that the system remains aligned with governance objectives. As illustrated in Figure 3, the validation methodology is based on a continuous risk-based audit lifecycle that integrates risk identification, control implementation, monitoring, and audit processes.

6. RESULTS AND OBSERVED BENEFITS

The implementation of the proposed framework leads to several observable outcomes.

First, it improves compliance by providing a structured method for aligning systems with regulatory requirements. This reduces uncertainty and supports more efficient audits.

Second, it enhances transparency by ensuring that system behavior can be traced and explained. This is essential for building trust among stakeholders.

Third, it increases resilience by enabling systems to adapt while maintaining control. The layered structure allows for flexible responses without compromising governance.

Finally, the approach demonstrates scalability, making it applicable across different domains and system types.

7. CONCLUSIONS

7.1 Discussion And Implications

The findings of this study highlight the importance of integrating governance mechanisms directly into the lifecycle of AI systems. Treating governance as an external or secondary function is no longer sufficient, particularly in the case of adaptive and autonomous systems that continuously evolve in response to changing environments [3] [9].

The proposed layered model demonstrates that effective governance must be embedded at multiple levels, combining strategic direction with operational control and real-time validation. This multi-layered approach reduces fragmentation and enables organizations to maintain consistency between policy, implementation, and system behavior.

One of the key implications of this work is the shift from static governance models toward continuous governance processes. Traditional approaches, based on periodic reviews and isolated controls, are not capable of addressing the dynamic nature of modern AI systems. In contrast, the integration of monitoring and audit mechanisms throughout the lifecycle allows for early detection of deviations and supports timely corrective actions.

At the same time, implementation requires a strong organizational commitment. It involves not only the adoption of new technical solutions, but also changes in processes, roles, and responsibilities. Governance becomes a shared responsibility across multiple functions, including management, compliance, and engineering teams. Without this alignment, even well-designed frameworks may fail in practice.

Another important implication is related to scalability. The proposed model is not limited to a specific domain and can be adapted to different types of AI systems, from centralized decision-support tools to distributed and autonomous environments. This flexibility makes it particularly relevant in the context of rapidly evolving technological ecosystems.

However, the model also introduces challenges. Increased governance complexity may lead to higher implementation costs, and the need for continuous monitoring may require additional computational and organizational resources. Balancing control and efficiency remains an open challenge that organizations must address carefully.

7.2 Conclusions And Future Work

This paper presents a structured approach to AI governance that combines management system principles with risk-based regulatory frameworks. By integrating ISO/IEC 42001 with the EU AI Act, the proposed model provides a coherent mechanism for translating high-level requirements into operational practices.

The layered governance structure ensures that responsibilities are clearly distributed while maintaining strong connections between strategic objectives, operational processes, and real-time system behavior. In addition, the risk-based audit methodology supports continuous validation, enhancing both transparency and accountability.

The main contribution of this work lies in the operationalization of AI governance. Rather than focusing solely on principles, the proposed framework demonstrates how governance can be embedded into the lifecycle of AI systems, enabling organizations to manage complexity in a structured and scalable manner.

Future research will focus on extending this approach to more complex environments, including distributed AI systems, collaborative platforms, and cyber-physical ecosystems. These environments introduce

additional challenges related to coordination, interoperability, and decentralized decision-making.

Another important direction for future work is the development of quantitative metrics for evaluating governance effectiveness. While the current model provides a conceptual and structural foundation, measurable indicators are needed to assess performance, compliance, and risk exposure in a consistent way.

In addition, further validation through real-world case studies would strengthen the applicability of the proposed framework. Implementing the model in practical scenarios would provide valuable insights into its strengths, limitations, and potential areas for refinement.

Overall, this work contributes to the development of trustworthy AI by offering a practical and adaptable governance framework, capable of supporting responsible innovation in increasingly complex technological environments.

8. REFERENCES

1. National Institute of Standards and Technology (NIST). (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). U.S. Department of Commerce.
2. European Commission. (2019). Ethics guidelines for trustworthy AI. Publications Office of the European Union.
3. Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. Nature Machine Intelligence, 1(9), 389–399.
4. Organisation for Economic Co-operation and Development (OECD). (2019). OECD principles on artificial intelligence.
5. Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., ... & Vayena, E. (2018). AI4People—An ethical framework for a good AI society. Minds and Machines, 28(4), 689–707.
6. European Union. (2024). Artificial Intelligence Act (Regulation (EU) 2024/1689).
7. International Organization for Standardization (ISO). (2023). ISO/IEC 42001: Artificial intelligence management system.
8. European Parliament. (2024). EU AI Act: Risk classification framework.
9. Raji, I. D., Smart, A., White, R. N., Mitchell, M., Gebru, T., Hutchinson, B., ... & Barnes, P. (2020). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. Proceedings of the FAT* Conference.
10. International Organization for Standardization (ISO). (2023). ISO/IEC 23894: Artificial intelligence — Risk management.
11. Dignum, V. (2019). Responsible artificial intelligence: How to develop and use AI in a responsible way. Springer.
12. Veale, M., & Borgesius, F. Z. (2021). Demystifying the draft EU Artificial Intelligence Act. Computer Law Review International, 22(4), 97–112.
13. International Organization for Standardization (ISO). (2022). ISO/IEC 38507: Governance implications of the use of artificial intelligence by organizations.
14. National Institute of Standards and Technology (NIST). (2022). Towards a standard for identifying and managing bias in artificial intelligence.