Journal of Artificial Intelligence and Computing (JAIC)
ISSN (e): 3005-3358
Volume: 4, Number: 1, Pages: 56 - 64, Year: 2026

Governing Artificial Intelligence by Standard and by Statute: A Comparative Review of ISO/IEC 42001 and the EU Artificial Intelligence Act

Muhammad Hammad Younas, and Irshad Ahmed Sumra

School of Systems and Technology, University of Management and Technology, Lahore, 54000, Pakistan
Corresponding author: Muhammad Hammad Younas (Email: hammadyns01@gmail.com)

Received: 12/03/2026, Revised: 22/05/2026, Accepted: 10/06/2026

***Abstract*—Artificial Intelligence is increasingly deployed across healthcare, finance, public administration, and education, creating value while introducing technical, ethical, and legal risks that require effective governance. ISO/IEC 42001:2023, the first certifiable AI management system standard, and the EU Artificial Intelligence Act, the first comprehensive binding AI regulation, have emerged as the two most influential governance instruments. This review compares their origins, scope, architecture, and governance approaches, examining their concerns, overlap, complementarity, strengths, and limitations. Findings show that the two instruments are complementary rather than competing: ISO/IEC 42001 offers a voluntary, process-based, organization-wide framework for responsible AI governance, while the EU AI Act establishes a product-centric, risk-based legal framework backed by enforcement, together forming a two-tier governance structure. The review recommends an integrated approach in which ISO/IEC 42001, supported by the NIST AI Risk Management Framework, helps operationalize compliance with the Act, and calls for dynamic risk assessment, sector-specific adaptation, and greater international harmonization.**

***Index Terms*— AI governance, ISO/IEC 42001, EU AI Act; AI risk management; AI management system.**

I. Introduction

Over the last decade, Generative AI, large language models, and natural-language processing have evolved into complex decision-making systems [1]. As AI becomes increasingly important in organizations, the need for effective governance continues to grow significantly. AI risks extend beyond technical inaccuracies to include ethical concerns, privacy breaches, legal obligations, and reputational damage [2]. Several studies have developed ethical principles and governance frameworks for AI, including global AI ethics guidelines and the AI4People framework [3], [4]. Other studies have examined the darker implications of AI deployment within organizations [5], [6]. However, operational tools capable of translating these principles into auditable organizational practices remained largely unavailable until recently.

Two instruments have since become central references in contemporary AI-governance discussions. The first is ISO/IEC 42001:2023, the first international standard dedicated specifically to managing AI systems [7], [8]. Published in December 2023, the standard focuses on organizational governance and management of AI systems. The second instrument is the EU Artificial Intelligence Act, adopted by the European Parliament in March 2024 [1], [9], [10]. The Act represents the first standalone and horizontal legislation dedicated specifically to AI governance. Although both instruments address similar concerns, they differ fundamentally in legal authority and governance approach. ISO/IEC 42001 is a voluntary management standard, whereas the EU AI Act is binding supranational legislation.

This review provides a structured and evidence-based comparison of ISO/IEC 42001 and the EU AI Act. The analysis examines each instrument's concerns, coverage, strengths, limitations, and areas of convergence. Four questions guide the review. First, what is each instrument fundamentally concerned with, and what does it cover? Second, where do both instruments converge, and where do they diverge? Third, what advantages and limitations characterize each instrument? Finally, how can both instruments be integrated into a coherent AI-governance framework?

The remainder of this review is organized as follows. Section II traces the origins of both instruments, Section III examines their scope and architecture, and Section IV presents a thematic comparison across legal, risk, and governance dimensions. Section V discusses convergence and complementarity, Sections VI and VII assess sectoral perspectives and comparative strengths and limitations, and Sections VIII–X identify open challenges, discuss integrated governance, and conclude with directions for future research.

II. Background and Genesis of the Two Instruments

A. ISO/IEC 42001:2023

ISO/IEC 42001:2023 provides guidance for developing,

implementing, maintaining, and continually improving an organization's Artificial Intelligence Management System (AIMS). The standard follows the structure used by other ISO management-system standards, including requirements for organizational context, leadership, planning, support, operation, performance evaluation, and improvement. These requirements resemble those found in ISO 9001 for quality management and ISO/IEC 27001 for information security management [7], [8]. This design intentionally reduces adoption costs for organizations already operating certified management systems. It also allows the AIMS to complement rather than replace existing governance frameworks [7].

The standard focuses on aligning AI objectives with broader organizational goals and strategic priorities. It promotes ethical, accountable, and transparent AI use while encouraging continuous organizational improvement. Transparency and improvement are treated as ongoing practices rather than one-time initiatives. The standard emphasizes responsible governance throughout the AI lifecycle and seeks to embed accountability into organizational operations.

ISO/IEC 42001 is also certifiable through accredited third-party certification bodies and external assessment processes [8]. External certification provides assurance that internal policy documents alone cannot deliver effectively. The standard is intentionally industry-agnostic and applicable across different sectors and organizational contexts. Rather than prescribing sector-specific requirements, organizations must identify, document, and justify appropriate controls through their own risk-assessment processes [8].

B. The EU AI Act

European legislators-initiated development of a binding AI regulation in April 2021. The regulation was published in the Official Journal in July 2024 and entered into force in August 2024 [11]. Full application will occur over a thirty-six-month period extending until August 2027. Certain obligations, including prohibited practices, begin applying from February 2025 [9].

The EU AI Act draws inspiration from the European Union's established product-safety framework. This framework reflects decades of institutional experience in ensuring safe products enter the European single market [12]. The Act pursues two primary objectives. First, it seeks to protect the health, safety, and fundamental rights of European citizens. Second, it aims to support innovation and maintain the competitiveness of the European AI industry [10], [1].

The regulation is extensive and complex, comprising 113 articles and thirteen annexes across 144 pages in its English version [12]. Its implementation involves multiple actors, including European institutions, national authorities, and private stakeholders. A European Artificial Intelligence Office has been established alongside an advisory forum, a scientific panel, and national competent authorities. Together, these bodies form a collaborative governance structure for AI regulation across the European Union [10].

Many observers expect the Act to generate a "Brussels Effect" similar to that associated with the General Data Protection Regulation (GDPR). As a result, the EU AI Act is widely viewed as a potential template for future AI regulation worldwide [10].

III. Scope, Architecture, and Core Concerns

Both instruments share a common concern that powerful AI systems may cause harm if improperly designed or used. However, they differ significantly in how such risks should be governed and managed. The EU AI Act focuses primarily on AI systems and models placed on the market. In contrast, ISO/IEC 42001 governs the organizational structures and management processes used to develop and operate those systems. This difference in the unit of governance shapes the architecture, objectives, and implementation requirements of each instrument.

A. The Architecture of ISO/IEC 42001

ISO/IEC 42001 is built upon the Plan–Do–Check–Act cycle of continuous improvement that underpins the ISO management-system family [7]. The standard requires organizations to understand their operating context and relevant stakeholders. It also requires leadership commitment, including the development of an organizational AI policy. Organizations must identify risks and opportunities, allocate appropriate resources, and ensure personnel possess the necessary competencies. The standard further requires controls across the AI lifecycle and ongoing monitoring of organizational performance [13], [7].

Performance evaluation includes monitoring, measurement, internal audits, and management reviews. Organizations must also implement corrective actions to address identified nonconformities and governance weaknesses [13], [7]. The annexes provide reference controls, including structured AI System Impact Assessments and explicit lifecycle considerations for AI systems [7]. Consequently, the standard focuses less on determining whether a system is inherently safe. Instead, it evaluates whether an organization maintains a credible, evidence-based, and continuously improving governance process for responsible AI deployment.

A major strength of ISO/IEC 42001 is its ability to integrate with adjacent governance frameworks. AI governance can be combined with information-security management to improve organizational risk management, traceability, and system integrity. This integration enables organizations to maximize AI's value as a strategic asset while maintaining effective governance controls [7].

The Act treats AI as a market product and regulates two primary categories of actors. These actors include providers who develop and market AI systems and deployers who use those systems in practice [12]. As a result, regulatory obligations vary according to both risk classification and stakeholder role.

Enforcement is supported by a graduated penalty regime. The most serious infringements attract the highest administrative fines, particularly for prohibited AI practices. Providers of general-purpose AI models may also face substantial financial penalties, including fines based on worldwide annual turnover

[1]. The Act further establishes an EU database for high-risk AI systems and introduces obligations through a phased implementation timeline. These requirements become applicable over periods ranging from six months to thirty-six months, depending on the category involved [1], [10].

B. The Architecture of the EU AI Act: A Risk-Based Pyramid

The EU AI Act classifies AI applications into four risk categories and assigns obligations according to risk level [2], [10], as illustrated in Fig. 1. AI practices presenting unacceptable risk are prohibited under Article 5. High-risk systems may be deployed only if they satisfy extensive requirements concerning risk management, data governance, technical documentation, record keeping, transparency, human oversight, accuracy, robustness, and cybersecurity [1], [9]. Limited-risk systems must comply primarily with transparency obligations, whereas minimal-risk systems remain largely unregulated.

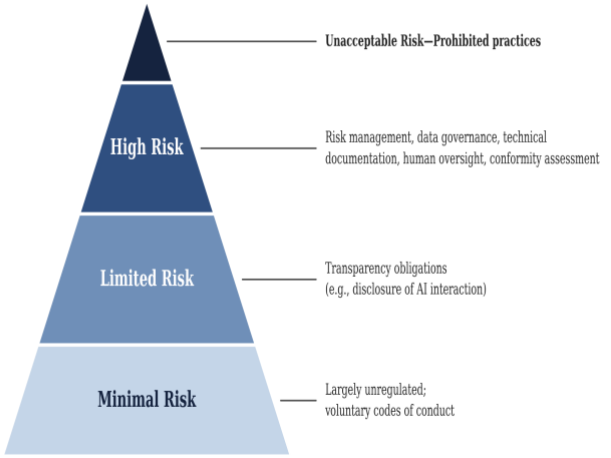

Fig. 1. The EU AI Act's four-tier risk-based regulatory pyramid, showing the obligations attached to each risk category [10].

C. Fundamental Concerns of Each Instrument

Although both instruments address AI governance, they focus on different foundational questions. ISO/IEC 42001 concentrates on organizational capability, accountability, and governance maturity. Its central question is whether an organization manages AI responsibly throughout the system lifecycle. The EU AI Act focuses on legality, market access, and protection of fundamental rights. Its primary concern is whether a specific AI system or model can legally enter and remain within the European market.

Therefore, ISO/IEC 42001 evaluates governance processes, organizational responsibility, and continual improvement mechanisms. The EU AI Act evaluates product compliance, risk classification, and legal obligations associated with market participation. Together, these instruments address complementary dimensions of AI governance, combining organizational accountability with regulatory oversight and legal compliance (Table I).

TABLE I
FOUNDATIONAL PROFILE OF THE TWO INSTRUMENTS

Dimension	**ISO/IEC 42001:2023**	**EU AI Act (Reg. (EU) 2024/1689)**
Type	International voluntary management-system standard (certifiable)	Binding supranational regulation / law
Published / in force	December 2023	Adopted Mar 2024; in force Aug 2024; full application Aug 2027
Unit of governance	The organization and its AI management processes	The AI system / GPAI model as a market product
Primary objective	Responsible, accountable, continually improving AI governance	Protect health, safety & fundamental rights; enable a single AI market
Mechanism	Plan–Do–Check–Act management system + Annex controls	Risk-tiered obligations + prohibitions + conformity assessment
Reach	Any organization, any sector, anywhere (by choice)	EU market; extraterritorial where output is used in the EU
Enforcement	Third-party certification & surveillance audits	Regulators, conformity assessment, administrative fines

IV. Thematic Comparative Analysis

This section compares ISO/IEC 42001 and the EU AI Act across dimensions most relevant to practitioners and researchers. Each subsection examines a specific area of comparison and highlights key similarities and differences between the two instruments.

A. Legal Status: Voluntary Standard versus Binding Law

The most important distinction between the two instruments concerns their legal force. ISO/IEC 42001 is a voluntary standard whose implementation depends on certification benefits and organizational commitment [8], [7]. Compliance is encouraged through commercial advantages, reputational benefits, and the possibility of losing certification during surveillance audits. In contrast, the EU AI Act is legally binding for organizations operating within its scope. Non-compliance may result in administrative penalties and restrictions on access to the European market [1], [9]. Nevertheless, the two instruments intersect because Articles 32 and 40 recognize harmonized standards as evidence of conformity with regulatory requirements [1]. The Act also encourages voluntary codes of conduct for AI systems outside the high-risk category [1].

B. Risk Philosophy: Managed Process versus Tiered Product Safety

ISO/IEC 42001 treats risk as an ongoing organizational responsibility requiring continuous identification, assessment, monitoring, and improvement throughout the AI lifecycle [13]. Organizations must demonstrate that risks and opportunities are systematically managed through documented governance processes. By contrast, the EU AI Act classifies AI systems into predefined risk categories and assigns obligations according to those categories [2]. This approach directs greater regulatory

scrutiny toward systems considered high risk. In practice, organizations often create AI Risk Assessment Registers to categorize systems according to EU risk tiers. They then use ISO- or NIST-based controls to design appropriate mitigation measures [2]. Consequently, the Act identifies which systems require strict oversight, whereas ISO/IEC 42001 provides governance mechanisms for delivering that oversight effectively.

C. Transparency and Explainability

Transparency is a central requirement within both instruments, although each address it differently. The EU AI Act imposes explicit transparency obligations intended to address concerns surrounding the "black box" nature of advanced AI systems and large language models [13], [10]. Organizations must document system capabilities, limitations, and user interactions where applicable. ISO/IEC 42001 approaches transparency as a governance objective and provides documentation processes, impact assessments, and management controls that support transparency goals. Research suggests that ISO/IEC 42001 addresses approximately eighty-five percent of the transparency and explainability requirements contained within the EU AI Act. Furthermore, combining governance practices with explainable AI techniques has been shown to improve public trust significantly [14].

D. Human Oversight

Human oversight represents another area of convergence between the two instruments. The EU AI Act requires meaningful human oversight for high-risk AI systems and distinguishes between human-in-the-loop, human-on-the-loop, and human-out-of-the-loop approaches [8]. These requirements establish clear expectations regarding human involvement in AI decision-making processes. ISO/IEC 42001 also recognizes the importance of oversight but provides fewer specific requirements. As a general-purpose management standard, it does not define who must oversee high-risk decisions, how oversight should occur, or what constitutes meaningful intervention [8]. The standard similarly avoids prescribing response times, escalation procedures, or minimum levels of human involvement. Therefore, the EU AI Act establishes the obligation for human oversight, whereas ISO/IEC 42001 provides a governance structure for implementing that obligation effectively.

E. Documentation, Traceability, and Conformity

Documentation is a fundamental requirement within both ISO/IEC 42001 and the EU AI Act. Effective documentation enables regulators, auditors, and stakeholders to evaluate compliance, accountability, and system integrity [2]. The EU AI Act requires providers of high-risk AI systems to maintain extensive technical documentation. This documentation includes system design information, training-data specifications, risk assessments, and performance metrics. Similarly, ISO/IEC 42001 requires organizations to document AI objectives, risk-management processes, governance controls, and continual-improvement activities [2].

These requirements increasingly support the development of centralized and version-controlled documentation repositories. Such repositories may contain impact assessments, compliance evidence, governance records, and audit documentation. They can also serve as a single source of truth for certification auditors and regulatory authorities. Emerging approaches such as machine-readable AI Cards demonstrate how documentation and traceability may become increasingly standardized in practice [15].

F. Enforcement, Penalties, and Certification

The two instruments differ substantially regarding enforcement mechanisms, penalties, and certification requirements. ISO/IEC 42001 relies primarily on market-driven enforcement through accredited certification, surveillance audits, and reputational incentives [8]. Organizations maintain compliance by demonstrating continued adherence to management-system requirements. Failure to satisfy certification requirements may result in loss of certification status.

In contrast, enforcement under the EU AI Act is regulatory and coercive. Competent authorities may impose administrative fines and other sanctions for non-compliance with legal obligations [1], [13]. High-risk systems must also undergo conformity assessments and post-market monitoring activities. Cost considerations further distinguish the two approaches. Full ISO/IEC 42001 certification has been estimated to cost between US$30,000 and US$108,000 for medium-sized organizations over four to twelve months [8]. Although lower-cost readiness pathways exist, compliance with the EU AI Act remains mandatory for organizations falling within its scope.

G. Scope of Application and Extraterritoriality

ISO/IEC 42001 can be adopted voluntarily by any organization regardless of sector, size, or geographic location [7]. Its impact therefore depends entirely on organizational willingness to implement the standard. The EU AI Act adopts a much broader regulatory reach through its extraterritorial provisions. Organizations located outside the European Union may still fall within the Act's scope when outputs from their AI systems are used within the EU market [1].

This broad jurisdictional reach is expected to influence AI-governance practices globally. However, researchers caution against assuming that the Act can function as a universal regulatory model. The regulation reflects unique European legal traditions, product-safety principles, and geopolitical considerations. Consequently, direct transplantation into other jurisdictions may not always address local governance needs effectively [12].

H. Ethics and Fundamental-Rights Coverage

The EU AI Act is explicitly grounded in the protection of fundamental rights, democracy, and the rule of law. It adopts a strongly human-centric approach to AI governance and regulation [10], [1]. ISO/IEC 42001 also addresses ethical concerns but does so through governance processes and management controls rather than explicit rights-based provisions.

Comparative analyses suggest that ISO/IEC 42001 provides

a robust governance framework while remaining less explicit regarding principles such as justice, fairness, responsibility, and accountability [16]. Researchers have argued that the standard could become more forward-looking through stronger integration of internationally recognized ethical principles. Evidence from public-sector studies further indicates that ISO/IEC 42001 provides only partial coverage of social-impact assessment requirements contained within the EU AI Act (Table II). Approximately forty-five percent coverage has been reported, suggesting limitations in addressing broader social consequences systematically [14].

TABLE II
THEMATIC COMPARISON OF ISO/IEC 42001 AND THE EU AI ACT

Dimension	ISO/IEC 42001:2023	EU AI Act
Legal force	Voluntary; enforced via certification & market reputation	Mandatory law; fines and market exclusion for breach
Risk model	Continuous, organization-wide risk management (PDCA)	Fixed four-tier classification with tier-specific duties
Transparency	Management objective; documentation procedures (≈85% coverage of Act's requirement)	Explicit transparency obligations (e.g., Art. 13)
Human oversight	Required but not quantified (no defined modes/thresholds)	Meaningful oversight mandated for high-risk (Art. 14)
Documentation	AI objectives, controls, improvement records	Extensive technical documentation for high-risk (Art. 11–12)
Enforcement	Accredited certification + surveillance audits	Regulators, conformity assessment, fines (Art. 99, 101)
Reach	Any organization/sector by choice	EU market + extraterritorial via output used in EU
Ethics / rights	Ethics as process; partial social-impact coverage (≈45%)	Explicit fundamental-rights protection; human-centric framing
Cost profile	~US$30k–108k for full certification; readiness tiers cheaper	Non-optional compliance cost for in-scope actors

V. Convergence and Complementarity

Although ISO/IEC 42001 and the EU AI Act differ in legal status and governance approach, they converge substantially in content. Empirical studies conducted within public-sector environments have mapped the requirements of the EU AI Act against ISO/IEC 42001 controls and governance practices. These studies demonstrate high levels of alignment across several important compliance dimensions. At the same time, they identify weaker alignment in broader areas involving social impacts and reliability evidence [14].

Research indicates that ISO/IEC 42001 provides particularly strong coverage of transparency, explainability, and risk-management requirements contained within the Act. The standard fully supports risk-management lifecycle activities and offers satisfactory documentation procedures for transparency obligations. However, coverage becomes more limited regarding reliability documentation and systematic assessment of social consequences. These findings suggest that ISO/IEC 42001 provides an important governance foundation but cannot independently satisfy all requirements established by the EU AI Act Table III [14].

TABLE III
REPORTED COVERAGE OF EU AI ACT REQUIREMENTS BY ISO/IEC 42001 (PUBLIC-SECTOR STUDY)

AI Act requirement	Coverage by ISO/IEC 42001	Comment
Transparency & explainability	High (≈85%)	Satisfactory documentation procedures provided
Risk management	High	Standard fully covers the risk-management lifecycle
Reliability documentation	Partial (≈60%)	Does not fully meet the Act's reliability evidence demands
Social-impact analysis	Partial (≈45%)	Insufficient systematic assessment of social consequences

The complementarity between the two instruments is intentional rather than accidental. The EU AI Act explicitly recognizes conformity with harmonized standards as evidence supporting regulatory compliance. Consequently, alignment with ISO/IEC 42001 may help organizations demonstrate compliance with several legal obligations under the Act [8], [1]. This relationship encourages organizations to integrate voluntary standards and regulatory requirements into a unified governance framework.

Several researchers further recommend combining ISO/IEC 42001 and the EU AI Act with the NIST AI Risk Management Framework (RMF). The NIST framework introduces a Govern–Map–Measure–Manage approach for addressing multidimensional AI risks [17], [2], [18]. Together, these instruments create a complementary governance structure. The EU AI Act provides legal obligations and risk-based classification. ISO/IEC 42001 supplies a certifiable management system and governance controls. The NIST RMF contributes technical methods for identifying, assessing, and managing AI-related risks.

This integrated approach creates mutually reinforcing governance capabilities. These capabilities include risk categorization, risk mapping, control design, continuous monitoring, governance oversight, and evidence-based documentation [2]. Research also indicates that organizations implementing RMF-style governance programs often experience fewer challenges during later ISO certification processes [8].

VI. Sectoral and Contextual Perspectives

Because the EU AI Act is horizontal and ISO/IEC 42001 is general-purpose, both instruments require contextual adaptation. Recent literature provides valuable insights into how these governance frameworks operate across different sectors and applications.

A. Healthcare

Healthcare represents one of the most significant areas for AI

deployment and governance. The EU AI Act introduces binding requirements affecting the use of AI in diagnosis, treatment, and patient care [9]. These requirements have important implications for healthcare technology and regulatory policy. However, researchers argue that the Act's horizontal structure does not fully address sector-specific challenges. These challenges include interactions with the Medical Device Regulation, management of clinical bias, digital ageism, and transparency obligations toward patients [9], [19].

As a result, additional guidance and standardization efforts will likely be required during implementation. Within this environment, ISO/IEC 42001 can provide structured governance processes and organizational discipline that legislation alone cannot fully deliver. A certifiable Artificial Intelligence Management System may therefore support more effective implementation of healthcare-specific AI governance requirements.

B. Banking and Financial Services

AI has transformed banking operations, business processes, and risk-management activities. At the same time, its adoption has generated concerns regarding privacy, algorithmic bias, fairness, transparency, and regulatory compliance [20]. Systematic reviews of the banking literature reveal extensive discussion of responsible AI deployment and governance principles. However, significant challenges remain regarding practical implementation and empirical validation.

Researchers identify continuing concerns regarding customer trust, limited evidence supporting governance effectiveness, and insufficient harmonization across regulatory frameworks [20]. Many governance principles remain largely theoretical rather than operationalized in practice. Combining a legally enforceable framework with a certifiable management system may therefore strengthen accountability and improve governance outcomes within financial institutions.

C. Public Sector and Business Adoption

Evidence from public-sector and business environments demonstrates several positive outcomes associated with ISO/IEC 42001 implementation. Municipal and private-sector case studies report improvements in transparency, decision-making processes, operational efficiency, and stakeholder trust [14]. Organizations adopting the standard have also reported reduced maintenance costs, decreased bias, and faster response times.

Despite these benefits, adoption remains uneven across organizational contexts. Larger organizations generally demonstrate higher adoption rates than smaller enterprises. Research suggests that successful implementation depends on technological maturity, availability of skilled personnel, and compatibility with existing management systems [14], [21]. These factors significantly influence an organization's ability to adopt and sustain AI-governance practices effectively.

D. Education

The education sector illustrates the challenges associated with applying general governance frameworks to specialized environments. AI technologies increasingly support admissions processes, assessment activities, tutoring functions, and administrative operations. Despite growing adoption, many educational institutions lack formal policies governing AI use. Furthermore, ISO/IEC 42001 does not specifically address issues such as child-data protection, parental consent, or academic integrity [8].

For many schools and educational institutions, full certification may not be immediately feasible. Nevertheless, an important intermediate step involves preparing for certification through implementation of deployer-relevant controls. These controls should generate auditable evidence demonstrating responsible AI governance practices. This approach aligns with recommendations emerging from both the EU AI Act and developing regulatory initiatives within the United States [8], [22].

E. Large Language Models and General-Purpose AI

Large language models present particularly complex governance challenges because they generate content at scale and operate across numerous domains. Their deployment introduces risks relating to misinformation, vulnerabilities, transparency, accountability, and decision-making processes [13]. Effective governance therefore requires comprehensive monitoring, record keeping, incident reporting, and post-market oversight mechanisms.

Research evaluating governance frameworks for large language models concludes that no single framework adequately addresses all governance requirements independently. Although ISO/IEC 42001 demonstrated the strongest readiness for supporting AI opportunities, researchers cautioned against developing a false sense of security [13]. Important gaps remain regarding real-time bias management, policy compliance, and model-specific governance requirements. Consequently, additional guidance and complementary controls remain necessary for effective governance of large language models and general-purpose AI systems.

VII. Comparative Strengths and Limitations

A. ISO/IEC 42001: Strengths and Limitations

ISO/IEC 42001 offers several significant advantages for organizations seeking structured AI governance. One major strength is its certifiability, which allows independent validation through accredited external assessment processes. Another advantage is its familiar management-system architecture, which supports integration with ISO 9001 and ISO/IEC 27001. This compatibility reduces implementation complexity and lowers adoption costs for organizations already operating established management systems [7], [8].

The standard's industry-neutral design also increases its applicability across diverse organizational contexts. Organizations from different sectors can adopt the framework while tailoring controls to their specific operational requirements. Empirical evidence suggests that implementation may contribute to reduced algorithmic bias, improved operational efficiency, lower maintenance costs, and greater stakeholder trust [14]. Comparative evaluations further identify

ISO/IEC 42001 as one of the most comprehensive governance frameworks for facilitating AI opportunities, particularly in relation to large language models [13].

Despite these strengths, several limitations remain. The standard does not provide sector-specific requirements or hazard-specific controls. It also avoids defining measurable thresholds for meaningful human oversight. As a result, organizations must determine appropriate oversight mechanisms independently. Furthermore, the standard provides only partial coverage of social-impact assessment requirements and several risks associated with large language models [8], [14].

Studies evaluating governance readiness for large language models found strong performance in areas such as monitoring, data security, incident response, and security awareness. However, weaknesses remained regarding misleading content generation, policy compliance, and real-time bias management [13]. Certification costs may also create challenges for smaller organizations with limited financial and human resources. This burden has been described as a form of "compliance debt" that may discourage adoption among resource-constrained institutions [8].

B. The EU AI Act: Strengths and Limitations

The EU AI Act's principal strength lies in its legally binding nature and enforceable requirements. It represents the first comprehensive horizontal law specifically addressing AI governance across multiple sectors. Through its risk-based framework, the Act prohibits particularly harmful practices while imposing proportionate obligations on other categories of AI systems [1], [10].

Another advantage is its strong commitment to protecting fundamental rights through a human-centric regulatory approach. The governance structure supporting implementation includes the AI Office, AI Board, advisory forum, scientific panel, and national authorities. Together, these institutions aim to promote consistent enforcement and regulatory coordination throughout the European Union [10].

Nevertheless, the Act also faces several challenges. Its horizontal design may not adequately address the specialized needs of particular sectors. Healthcare studies, for example, identify gaps relating to sector-specific implementation requirements and interactions with existing medical regulations [9]. Civil-society organizations have also highlighted potential loopholes affecting protection of fundamental rights and civic space [9].

Complexity presents an additional challenge. The Act contains 113 articles and thirteen annexes while interacting with multiple existing European legal instruments [12]. This complexity may increase implementation costs and create compliance burdens for affected organizations Table IV. Furthermore, the phased implementation timeline creates uncertainty during the transition period as obligations become applicable gradually over several years [9], [10].

TABLE IV
PROS AND CONS OF ISO/IEC 42001 AND EU AI ACT

	Strengths	**Limitations**
ISO/IEC 42001	Certifiable & externally validated; integrates with ISO 9001/27001; sector-agnostic; documented bias/efficiency/trust gains; strongest AIMS facilitation for LLM opportunities	General-purpose (no sector/hazard specifics); does not quantify oversight; partial social-impact & LLM-risk coverage; certification cost can be prohibitive ("compliance debt")
EU AI Act	Binding & enforceable; comprehensive, human-centric, rights-protective; clear proportionate risk tiers; EU-wide governance machinery	Horizontal approach weak on sectoral needs; alleged rights/loophole gaps; high complexity & compliance burden; phased timeline creates uncertainty; contested as a global template

VIII. Critical Gaps and Open Challenges

Three major gaps emerge consistently throughout the literature on AI governance. The first is a research–regulation gap. Bibliometric studies indicate that knowledge regarding AI governance under the EU AI Act remains limited compared with the broader AI literature. This imbalance creates challenges for policymakers and practitioners attempting to govern rapidly evolving technologies. It also highlights the difficulty of aligning research developments with regulatory implementation, particularly for high-risk AI systems regulated under the Act [23].

The second gap concerns enforcement and validation. Across sectors, governance principles are more common than evidence demonstrating effective implementation. Questions remain regarding the practical effectiveness of governance frameworks and their impact on stakeholder trust. Empirical evidence supporting governance outcomes remains limited, particularly regarding customer trust, organizational accountability, and long-term effectiveness [20].

The third gap relates to specificity. General governance instruments often fail to address specialized risks associated with particular domains. Healthcare, education, and large language models each present unique challenges requiring additional controls and sector-specific guidance. Existing frameworks therefore require adaptation to address domain-specific risks adequately [9], [8], [13].

Addressing these challenges requires a coordinated governance agenda. Researchers emphasize the importance of flexible risk-assessment models, sector-specific adaptations, cross-jurisdictional harmonization, and improved automation capabilities [2]. Broader organizational-governance research similarly suggests that AI governance remains an evolving field characterized by unresolved questions and emerging research priorities [24], [25].

IX. Discussion: Toward Integrated AI Governance

The comparison between ISO/IEC 42001 and the EU AI Act supports a clear conclusion. ISO/IEC 42001 should not be viewed as a replacement for the EU AI Act. Instead, it functions

as an additional layer within a broader AI-governance framework. The Act focuses on determining whether an AI system may legally enter the market while protecting health, safety, and fundamental rights. ISO/IEC 42001 addresses a different question by evaluating whether an organization governs AI responsibly and continuously improves its governance processes.

This distinction creates a complementary relationship between the two instruments. The EU AI Act provides legal obligations and regulatory pressure that encourage adoption of structured governance practices. ISO/IEC 42001 offers practical mechanisms that help organizations operationalize those obligations effectively. Because the Act recognizes harmonized standards as evidence of compliance, implementation of an Artificial Intelligence Management System may assist organizations in satisfying regulatory requirements [1], [8].

Researchers increasingly advocate integrating three governance instruments into a unified framework. These instruments include the EU AI Act, ISO/IEC 42001, and the NIST AI Risk Management Framework [2]. Within this arrangement, the Act provides legal obligations and risk classification. ISO/IEC 42001 supplies governance controls and a certifiable management system. The NIST framework contributes methods for technical risk identification, assessment, and management[26] [27].

An integrated governance framework may include an AI governance board, a risk register aligned with EU risk tiers, responsible-AI control matrices, continuous monitoring mechanisms, and centralized documentation repositories [2]. Together, these components enable organizations to move beyond fragmented compliance activities toward a unified framework supporting innovation, accountability, and ethical AI deployment. Empirical evidence suggests that such integrated approaches can improve efficiency, reduce bias, and strengthen stakeholder trust [14], [7].

X. Conclusion and Future Directions

ISO/IEC 42001:2023 and the EU AI Act currently represent the two most influential instruments in AI governance. ISO/IEC 42001 is a voluntary, process-driven, organization-wide management standard. The EU AI Act is a mandatory, product-focused, risk-based legal framework supported by enforcement mechanisms and sanctions. Although both instruments emphasize transparency, risk management, documentation, and human oversight, they differ substantially regarding legal authority, governance scope, enforcement, and treatment of social impacts. ISO/IEC 42001 provides a structured governance framework but lacks legally binding force and sector-specific requirements. The EU AI Act establishes enforceable obligations but does not provide an internal management system and may not fully address specialized sectoral needs. When combined, however, these instruments offer a strong foundation for responsible AI governance. Responsible AI governance is no longer optional for modern organizations. Institutions adopting comprehensive and credible governance frameworks will be better positioned to manage regulatory obligations, reduce reputational risks, and strengthen stakeholder trust.

CONFLICTS OF INTEREST

The authors declare no conflicts of interest to report regarding the present study.

AUTHOR CONTRIBUTIONS

Conceptualization, M.H.Y. and I.A.S.; methodology, M.H.Y.; software, M.H.Y. and I.A.S.; validation, I.A.S.; writing—original draft preparation, M.H.Y.; writing—review and editing, I.A.S.

FUNDING STATEMENT

This research received no external funding.

INSTITUTIONAL REVIEW BOARD STATEMENT

Not applicable.

INFORMED CONSENT STATEMENT

Not applicable.

DATA AVAILABILITY STATEMENT

Data is available on reasonable request.

References

[1] J. S. Butt, “Analytical study of the world’s first EU Artificial Intelligence (AI) Act, 2024,” *Int. J. Res. Publ. Rev.*, vol. 5, no. 3, pp. 7343–7364, 2024.

[2] R. B. Chellappan, “Responsible innovation in artificial intelligence: A unified risk management approach integrating NIST, ISO 42001, and the EU AI Act,” unpublished, 2025.

[3] A. Jobin, M. Ienca, and E. Vayena, “The global landscape of AI ethics guidelines,” *Nat. Mach. Intell.*, vol. 1, no. 9, pp. 389–399, 2019.

[4] L. Floridi et al., “AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations,” *Minds Mach.*, vol. 28, no. 4, pp. 689–707, 2018.

[5] P. Mikalef, K. Conboy, J. E. Lundström, and A. Popovič, “Thinking responsibly about responsible AI and ‘the dark side’ of AI,” *Eur. J. Inf. Syst.*, vol. 31, no. 3, pp. 257–268, 2022.

[6] B. W. Wirtz, J. C. Weyerer, and B. J. Sturm, “The dark sides of artificial intelligence: An integrated AI governance framework for public administration,” *Int. J. Public Admin.*, vol. 43, no. 9, pp. 818–829, 2020.

[7] S. Biroğul, Ö. Şahin, and H. Əsgərli, “Exploring the impact of ISO/IEC 42001:2023 AI management standard on organizational practices,” *Adv. Artif. Intell. Res.*, vol. 5, no. 1, pp. 14–22, 2025.

[8] R. J. Purdy, “ISO/IEC 42001 and the education sector: A critical analysis,” Purdy House Publishing and Consulting, Memorandum no. 4, 2026.

[9] H. van Kolfschooten and J. van Oirschot, “The EU Artificial Intelligence Act (2024): Implications for healthcare,” *Health Policy*, vol. 149, art. 105152, 2024.

[10] C. Cancela-Outeda, “The EU’s AI Act: A framework for collaborative governance,” *Internet of Things*, vol. 27, art. 101291, 2024.

[11] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), *Off. J. Eur. Union*, L 2024/1689, Jul. 12, 2024.

[12] M. Almada, “The EU AI Act in a global perspective,” in *Handbook on the Global Governance of AI*, S. Furendal and M. Lundgren, Eds. Cheltenham, U.K.: Edward Elgar, 2025, forthcoming.

[13] T. R. McIntosh et al., “From COBIT to ISO 42001: Evaluating cybersecurity frameworks for opportunities, risks, and regulatory compliance in commercializing large language models,” *Comput. Secur.*, vol. 144, art. 103964, 2024.

[14] C. Mouchtari and A. Davalas, “Review of the ISO/IEC 42001 artificial intelligence management system standard, application in public organizations and businesses,” *Int. J. Soc. Sci. Econ. Res.*, vol. 11, no. 2, pp. 139–149, 2026.

[15] H. J. Pandit, S. Schade, D. O'Sullivan, and D. Lewis, "AI cards: Towards an applied framework for machine-readable AI and risk documentation inspired by the EU AI Act," in *Proc. Eur. Conf. Artif. Intell. (ECAI)*, 2024, pp. 45–56.

[16] P. S. Suri, "Aligning ethics and AI governance: A comparative study of ISO 42001 and global standards," M.S. thesis, Pennsylvania State Univ., University Park, PA, USA, 2024.

[17] National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, NIST AI 100-1, U.S. Dept. Commerce, Gaithersburg, MD, USA, 2023.

[18] M. F. I. Khan, "Risk management framework in the AI Act," *Int. J. Sci. Res. Arch.*, vol. 14, no. 3, pp. 466–471, 2025.

[19] D. Onitiu, S. Wachter, and B. Mittelstadt, "How AI challenges the medical device regulation: Patient safety, benefits, and intended uses," *J. Law Biosci.*, vol. 11, no. 1, art. lsae007, 2024.

[20] M. Fundira and C. Mbohwa, "AI ethics in banking services: A systematic and bibliometric review of regulatory and consumer perspectives," *Discov. Artif. Intell.*, vol. 5, art. 319, 2025.

[21] A. Pandy, A. Fernandes, and J. C. Correa, "Assessment of the benefits of the ISO/IEC 42001 AI management system: Insights from selected Brazilian logistics experts, an empirical study," *Standards*, vol. 5, no. 2, art. 10, 2025.

[22] State of Colorado, *Senate Bill 24-205: Consumer Protections for Artificial Intelligence*, Colorado Gen. Assem., 2024.

[23] B.-J. Kim, S. Jeong, B.-K. Cho, and J.-B. Chung, "AI governance in the context of the EU AI Act," *IEEE Access*, vol. 13, 2025.

[24] T. Birkstedt, M. Minkkinen, A. Tandon, and M. Mäntymäki, "AI governance: Themes, knowledge gaps and future agendas," *Internet Res.*, vol. 33, no. 7, pp. 133–167, 2023.

[25] M. Mäntymäki, M. Minkkinen, T. Birkstedt, and M. Viljanen, "Defining organizational AI governance," *AI Ethics*, vol. 2, no. 4, pp. 603–609, 2022.

[26] I. A. Sumra, I. Ahmad, H. Hasbullah and J. -l. bin Ab Manan, "Behavior of attacker and some new possible attacks in Vehicular Ad hoc Network (VANET)," 2011 3rd International Congress on Ultra-Modern Telecommunications and Control Systems and Workshops (ICUMT), Budapest, Hungary, 2011, pp. 1-8.

[27] I. A. Sumra, H. Hasbullah and J. -l. A. Manan, "VANET security research and development ecosystem," 2011 National Postgraduate Conference, Perak, Malaysia, 2011, pp. 1-4, doi: 10.1109/NatPC.2011.6136344