Review

Gaps in AI-Compliant Complementary Governance Frameworks' Suitability (for Low-Capacity Actors), and Structural Asymmetries (in the Compliance Ecosystem)—A Review

William Walter Finch * and Marya Butt *

Posted Date: 24 September 2025

doi: 10.20944/preprints202509.1979.v1

Keywords: EU AI Act; ALTAI; trustworthy AI; AI governance; ISO/IEC 42001; NIST AI RMF; OECD AI Principles; compliance; SMEs; proportionality; ethics; low-capacity actors; cybersecurity governance

Review

Gaps in AI-Compliant Complementary Governance Frameworks' Suitability (for Low-Capacity Actors), and Structural Asymmetries (in the Compliance Ecosystem)—A Review

William Walter Finch [1] and Marya Butt [2]

[1] Inholland University of Applied Sciences, Haarlem
[2] Data-Driven Smart Society, DDSS, Alkmaar
* Correspondence: Wiley.Finch@inholland.nl; Tel.: +316 12567040

Abstract

The European Union Artificial Intelligence Act, Regulation (EU) 2024/1689 of the European Parliament and of the Council, dated 13 March 2024, on artificial intelligence, marks the first comprehensive legal framework for artificial intelligence. It establishes a risk-based regulatory architecture that distributes obligations across diverse actors in the AI value chain. While its provisions emphasize proportionality and trustworthiness, significant asymmetries emerge between technologically advanced providers and low-capacity actors such as SMEs, municipalities, and public authorities. This article conducts a structured literature review of regulatory, ethical, and governance sources to examine how compliance responsibilities are operationalized across risk tiers and actor roles. In particular, it analyses the Assessment List for Trustworthy AI (ALTAI) as a soft-law ethics instrument, the EU AI Act as hard law, and comparative frameworks such as ISO/IEC 42001, the NIST AI Risk Management Framework, and the OECD AI Principles. The findings reveal gaps in enforceability, proportionality, and auditability that limit the accessibility of compliance for under-resourced organizations. To address these gaps, the article outlines the need for lightweight compliance frameworks that extend ALTAI's normative scaffolding into actionable and auditable processes. By mapping role-specific obligations against the structural capacities of actors, the analysis contributes to ongoing debates on operationalizing trustworthy and lawful AI in the European context.

Keywords: EU AI Act; ALTAI; trustworthy AI; AI governance; ISO/IEC 42001; NIST AI RMF; OECD AI Principles; compliance; SMEs; proportionality; ethics; low-capacity actors; cybersecurity governance

1. Introduction

Artificial Intelligence (AI) has rapidly evolved into a foundational technology, with general-purpose models like ChatGPT-3.5 accelerating adoption across sectors [1]. While the transformative potential of AI is widely recognized [2,3], regulatory frameworks have struggled to keep pace. Regulation (EU) 2024/1689, commonly known as the European (EU) AI Act, represents the first attempt to impose binding, risk-tiered obligations on AI providers and deployers. Translating these obligations into scalable, auditable compliance processes remains an unresolved challenge, particularly for actors lacking institutional capacity. Existing AI governance frameworks, such as the OECD AI Principles, the NIST AI Risk Management Framework, and ISO/IEC 42001, provide high-level guidance but often fall short in terms of operational specificity, proportionality, and enforceability [4]. ALTAI (the European Commission's Assessment List for Trustworthy AI) is more

 doi:10.20944/preprints202509.1979.v1

accessible, but has been shown to omit key technical safeguards. It was found that ALTAI overlooks 69% of known AI security vulnerabilities [5]. While ALTAI promotes essential ethical values as transparency, fairness, and human oversight, it requires extension to function as a compliance foundation under the EU AI Act. Compounding the complexity is the overlap between the EU AI Act and the General Data Protection Regulation (GDPR), which imposes its own requirements for AI systems that process personal data. Although the EU AI Act does not supersede the GDPR, the interaction between the two creates legal uncertainty, particularly for organizations lacking specialized compliance capacity.

The paper provides a structured review of literature and regulatory instruments relevant to AI compliance, with a particular focus on legally binding frameworks (e.g., the EU AI Act) and normative tools (e.g., ALTAI). The objective is to identify structural gaps in enforceability and practical implementation, particularly for actors with limited institutional capacity.

The key objectives of the study are listed below:

1. Analyze the regulatory landscape and actor-specific obligations under the EU AI Act, focusing on the distribution of legal burdens across providers, deployers, importers, and related roles.
2. Assess the limitations of ALTAI as a soft-law instrument, especially in traceability and enforceability.
3. Review complementary governance frameworks (e.g., ISO/IEC 42001, NIST AI RMF) and identify gaps in their suitability for low-capacity actors.
4. Identify structural asymmetries in the compliance ecosystem that call for proportionate, role-sensitive approaches.

2. Methodology

This review followed a structured, hybrid systematic–scoping design. The process was inspired by the systematic review protocol PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) [6], but adapted to the interdisciplinary nature of AI governance and the inclusion of both academic and policy sources. The systematic dimension ensured comprehensive coverage of rapidly evolving governance and regulatory frameworks. In contrast, the scoping dimension enabled the integration of earlier works on contextual actors (e.g., SMEs, public authorities), particularly those with longstanding structural capacity constraints. This dual approach provided both up-to-date insights into the EU AI Act and related frameworks, as well as a longitudinal perspective on persistent governance challenges.

2.1. Research Design

The review proceeded in four phases:

1. Source identification across academic and policy databases.
2. Screening against predefined legal, ethical, and governance relevance criteria.
3. Temporal scoping, distinguishing between recent frameworks and longer-standing actor constraints.
4. Corpus construction and thematic coding.

This process is illustrated in Figure 1, which summarizes the flow from initial identification to final thematic clusters.

 doi:10.20944/preprints202509.1979.v1

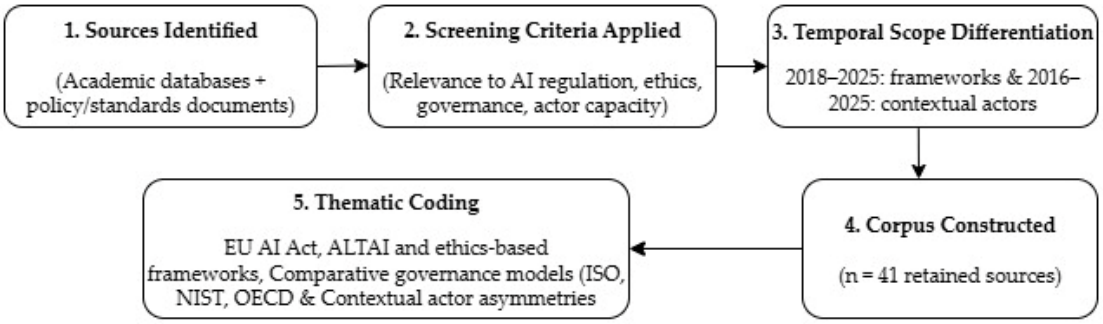

Figure 1. Methodology for literature selection.

2.2. Search Strategy

The search drew on major academic databases (Scopus, Web of Science, IEEE Xplore, ScienceDirect, SpringerLink, Wiley Online Library, Taylor & Francis, SAGE, Emerald Insight), complemented by official EU documents and standards repositories (e.g., OECD, ISO, NIST, European Commission). Search strings combined regulatory and governance terms ("AI Act," "Artificial Intelligence Act," "EU AI regulation," "ISO/IEC 42001," "NIST AI RMF," "OECD Principles"), ethics terms ("Trustworthy AI," "ALTAI," "ethics checklist"), and actor-related terms ("SMEs," "public sector," "low-capacity actors").

2.3. Inclusion and Exclusion Criteria

The following exclusion and inclusion criteria are used to select the relevant articles.

2.3.1. Inclusion Criteria

-For technical, legal, and governance-focused studies: be published between 2018 and 2025, reflecting the consolidation period of AI governance frameworks.

-For studies on contextual actors (SMEs, public authorities, low-capacity organizations), also include earlier works (2016 onwards) that provide enduring insights into structural challenges, such as compliance capacity, resource constraints, and organizational readiness.

-Be written in English.

-Present empirical, conceptual, or normative contributions to AI governance, compliance, or risk management.

-Include at least one reference to the EU AI Act, ALTAI, or comparative frameworks (OECD, NIST RMF, ISO/IEC 42001).

2.3.2. Exclusion Criteria

-Non-peer-reviewed opinion pieces, blogs, or news items without substantive analysis.

-Conference abstracts without full papers.

-Sources not addressing governance, regulation, ethics, or structural actor capacity in relation to AI.

2.4. Temporal Scope of Sources

The differentiated temporal scope reflects(as shown in Table 2.4) the uneven pace of development across domains. Governance frameworks are recent and dynamic, while structural actor issues are long-standing.

 doi:10.20944/preprints202509.1979.v1

Table 1. Temporal scope of the chosen articles.

Category	Oldest Source in Review	Temporal Scope Applied	Rationale
Governance & Ethics Frameworks (ALTAI, OECD, NIST, ISO)	OECD AI Principles (2019)	2018–2025	A rapidly evolving field; earlier sources predate the formalization of AI governance.
ALTAI (HLEG)	2020	2018–2025	Originated in 2019, Ethics Guidelines; operationalised in 2020.
NIST AI RMF	Draft 2021, final 2023	2018–2025	Framework development intensified post-2019; older sources are not directly relevant.
ISO/IEC 42001	2023	2018–2025	Standard finalised in late 2023; included as a cutting-edge regulatory benchmark.
Contextual Actors (SMEs, Public Sector, Low-Capacity Actors)	Safa, Solms & Furnell (2016)	2016–2025	Structural constraints (resources, compliance capacity) are long-standing; older sources remain relevant.

2.5. Data Extraction and Synthesis

From the final corpus (n = 41), each document was coded across four thematic axes:

1. The EU AI Act (regulatory scope, obligations, proportionality).
2. Ethics-based frameworks (ALTAI and related governance checklists).
3. Comparative governance models (ISO/IEC 42001, NIST AI RMF, OECD AI Principles).
4. Contextual actor asymmetries (SMEs, public authorities, non-specialist deployers).

Coding was performed manually, focusing on both explicit references and latent themes that cut across categories. The synthesis informed the structuring of Section 2.1 and subsequent analytical discussion.

2.6. Limitations

The hybrid design carries limitations. First, limiting technical and governance sources to the 2018–2025 window risks excluding early conceptual debates; this was mitigated by including contextual actor sources back to 2016. Second, reliance on English-language sources may omit perspectives from Member States where implementation debates occur in national languages. Third, although multiple databases were used, database bias cannot be entirely ruled out. These limitations were balanced by deliberately diversifying source types (academic, policy, and standards) and applying a transparent thematic coding framework.

3. Materials and Methods

3.1. The Regulatory Landscape: The EU AI Act

3.1.1. Objectives, Scope, and Risk-Based Classification

The European Union Artificial Intelligence Act (EU AI Act), formally Regulation (EU) 2024/1689, was adopted by the European Parliament on 13 March 2024 and by the Council on 21 May 2024. It was signed on June 13, published in the Official Journal on July 12, and entered into force on August 1, 2024. It constitutes the world's first comprehensive legal framework for AI, advancing the European Commission's digital strategy by transitioning from non-binding ethical principles to legally enforceable obligations. Central to the EU AI Act is a risk-based regulatory model, introduced in Recitals 5–9, that tailors legal obligations to the level of risk posed by AI systems. At the core of the EU AI Act lies a horizontal, tiered governance model that aligns compliance obligations with the level of systemic and individual risk posed by AI systems. This model distinguishes four risk categories: unacceptable risk (Article 5), high risk (Article 6), limited risk (Article 50), and minimal risk (exempt

 doi:10.20944/preprints202509.1979.v1

from obligations). Article 7 empowers the Commission to update Annex III, which lists high-risk use cases. Each category carries distinct legal consequences, from outright prohibition to transparency duties or voluntary self-regulation. The specific characteristics, examples, and legal obligations for each category are analyzed in Sections 3.1.2 through 3.1.5.

3.1.2. Unacceptable-Risk Systems and Implications for Compliance

Unacceptable-risk AI systems are generally prohibited under Article 5 of the EU AI Act. These include applications that contravene fundamental rights, such as systems that exploit vulnerabilities in specific populations (e.g., children or persons with disabilities) and AI used for social scoring by public authorities. The use of real-time remote biometric identification in publicly accessible spaces by law enforcement is also prohibited, except in narrowly defined circumstances, such as searching for missing persons or preventing imminent threats to life or safety, subject to prior judicial or administrative authorization, ex ante registration, and strict safeguards. Their prohibition is grounded in the normative stance that such applications are inherently incompatible with EU democratic values and cannot be justified solely based on risk mitigation.

3.1.3. Limited-Risk Systems and Implications for Compliance

Limited-risk systems are not banned but are subject to specific transparency obligations under Article 50. These obligations require that users be informed when they interact with AI, especially in contexts involving chatbots, biometric categorization, or AI-generated content, such as deepfakes. The aim is to foster informed human agency while avoiding the use of deceptive or manipulative AI. The limited-risk category applies broadly to systems that could mislead users or erode trust if left undisclosed.

3.1.4. Minimal-Risk Systems

Minimal-risk AI systems represent the largest category and include tools such as spam filters, email sorting algorithms, and recommendation engines, which typically do not fall into any of the other three categories. These systems are exempt from binding requirements under the AI Act.

3.1.5. High-Risk Systems and Implications for Compliance

High-risk applications, such as automated lie detection at EU borders (e.g., iBorderCtrl), illustrate the ethical and regulatory complexity of the AI Act. These systems raise concerns about biometric surveillance, bias, and the structural compliance burdens, particularly when multiple actors share responsibilities for risk management and documentation [7]. The EU AI Act mandates a comprehensive suite of obligations for providers of high-risk AI systems, encompassing lifecycle risk management (Article 9), data governance (Article 10), human oversight (Article 14), and robustness (Article 15). These requirements are formalized through technical documentation (Article 11), logging capabilities (Article 12), transparency and user instructions (Article 13), and provider identification obligations (Article 16(b)). Additionally, providers must implement a quality management system (Article 17), maintain up-to-date technical documentation (Article 18), log system operation (Article 19), and take corrective actions when risks or non-compliance are identified (Article 20). Conformity assessments (Article 43), CE marking (Article 48), and EU declarations of conformity (Article 47) anchor legal accountability, while Article 49 requires registration of high-risk systems in the EU database established under Article 71. Under Article 16(k)–(l) and Recital 80, providers must also ensure accessibility and demonstrate compliance on request by competent authorities.

To navigate these burdens, particularly for complex or sensitive systems (e.g., biometric categorization or risk scoring), organizations are increasingly turning to Fundamental Rights Impact Assessments (FRIsAs). Legally, Article 27 requires FRIAs for certain deployers, such as public authorities and entities providing public services, when using Annex III high-risk systems. However, many providers and other actors adopt FRIAs voluntarily as governance tools to complement mandatory conformity processes. Unlike Data Protection Impact Assessments (DPIAs), which focus

 doi:10.20944/preprints202509.1979.v1

narrowly on privacy, FRIAs examine a broader array of rights such as non-discrimination, freedom of expression, and access to justice [8,9]. Without harmonized FRIA methodologies, structured scaffolding tools such as ontologies, AI risk cards, and ethical checklists are often deployed [9,10]. The ALTAI checklist, developed by the European Commission as a soft-law instrument for trustworthy AI, is frequently used in this context. While voluntary, ALTAI's structured interrogation of fairness, oversight, and societal impact enables operationalization of abstract governance principles and supports early-stage risk mapping [11]. RegTech solutions, including the AI Risk Ontology (AIRO), system transparency cards, and modular FRIA ontologies, are being explored as ways to bridge high-level legal obligations with technical workflows [9,10]. These tools enable traceable, machine-readable documentation and may lower the procedural burden of conformity assessments and audit readiness.

Non-compliance with the AI Act can result in administrative fines of up to €35 million or 7% of global annual turnover for infringements of prohibited practices, €15 million or 3% for other violations, and €7.5 million or 1% for supplying incorrect information (Article 99). Enforcement, however, depends on the harmonization of standards (Articles 40–42) and the administrative capabilities of Member States. In this context, "compliance realism" suggests that incremental adherence, supported by modular frameworks like ALTAI or risk ontologies, may be more feasible for many organizations than complete alignment with aspirational governance ideals. These structural gaps and their implications for compliance tooling are further discussed in Sections 3.4 and 3.5.

3.1.6. General Purpose AI (GPAI)

Although not a risk category within the EU AI Act, the Regulation introduces a distinct regime for General Purpose AI (GPAI), defined as AI models trained on broad datasets that are capable of serving multiple downstream purposes without requiring fine-tuning. These typically include large language models (LLMs), vision transformers, and multimodal systems used across domains. Articles 51–55 establish obligations for GPAI providers, including:

- Transparency documentation on model capabilities, limitations, and risk areas (Article 53).
- Risk mitigation plans, including systemic and societal risk analysis (Article 55 for systemic-risk GPAI).
- Technical documentation detailing architecture, training, and dataset provenance (Article 53).
- Protocols for responsible open release, particularly for systemic-risk GPAI models (Article 55).

Downstream AI system providers that integrate GPAI models into high-risk contexts must obtain and use information provided under Article 53 to meet their own obligations. Furthermore, if a deployer, distributor, or importer substantially modifies or alters the intended purpose of a GPAI model so that it becomes a high-risk system under Article 6, they are legally reclassified as providers under Article 25. This entails full compliance with provider obligations, including technical documentation, conformity assessment, and risk management. These dynamics create a compliance chain in which multiple entities may share accountability for the same outcome.

The regulatory treatment of GPAI thus introduces a shift in focus from application-specific compliance to model-level governance. It also blurs traditional actor categories by distributing compliance responsibilities across development and deployment phases. These dynamics will influence how actor roles are defined and operationalized, which is the focus of the next section.

3.1.7. The AI Value Chain and Role-Specific Compliance

The preceding sections have outlined the EU AI Act's risk-based structure and associated obligations. To understand how these requirements are applied in practice, however, they must be examined within the broader AI value chain. While the Act assigns distinct legal responsibilities to roles such as providers and deployers, these actors operate within a larger ecosystem of interdependent entities. The EU AI Act establishes a structured taxonomy of actors involved in the development, distribution, and use of AI systems. Article 3 defines:

 doi:10.20944/preprints202509.1979.v1

- Provider (Art. 3(2)): the natural or legal person who develops an AI system or has it developed, and places it on the market or puts it into service under their name or trademark.
- Deployer (Art. 3(4)): a natural or legal person using an AI system in the course of their professional activities.
- Authorised Representative (Art. 3(5)): a legal entity established in the Union that is appointed in writing by a non-EU provider to act on their behalf concerning regulatory obligations.
- Importer (Art. 3(6)): any natural or legal person established in the Union who places an AI system on the Union market that originates from a third country.
- Distributor (Art. 3(7)): any natural or legal person in the supply chain, other than the provider or importer, who makes an AI system available on the Union market without modifying its properties.
- Product Manufacturer (Art. 3(8)): a manufacturer placing a product on the market or putting it into service under their own name, and who integrates an AI system into that product.

Although not formally recognized as actors, individuals affected by the deployment of AI systems are central to the risk-based logic of the Act, particularly in Recitals 5–9 and 61–63.

A detailed analysis of the corresponding obligations and liability implications for each actor type, categorized by risk level, is presented in Section 3.1.8. Figure 2 illustrates an exemplary flow, mapping the journey of AI systems from development to deployment and societal impact, and identifying key actors, including providers, importers, authorized representatives, distributors, and deployers.

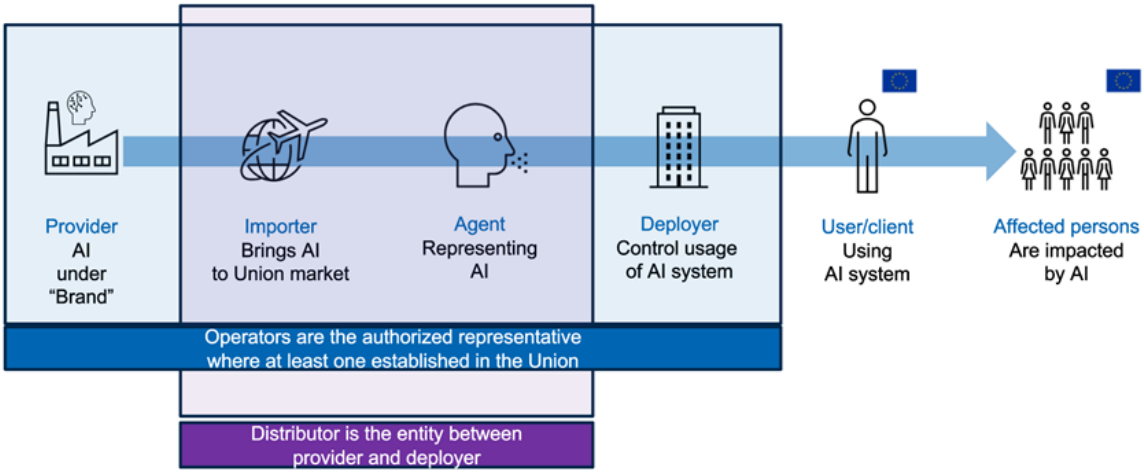

Figure 2. Flow of AI Systems and different Actors.

3.1.8. Summary of Role-Based Obligations under the EU AI Act

The preceding analysis of the EU AI Act's risk-based structure and value chain logic demonstrates that legal responsibilities are both tiered by risk and distributed across multiple actor types. However, these obligations are not evenly applied. Instead, they depend on both the actor's role, as defined in Article 3, and the classification of the AI system they develop, distribute, or use. To synthesize this complexity, Table 2 presents a role–risk matrix that maps the core legal duties imposed on each actor type across the risk categories outlined in Articles 5, 6, and 50. All actors marked with an asterisk (*) in Table 2 are subject to Article 25, meaning that they become a provider of high-risk AI systems and assume the corresponding provider obligations if the conditions of Article 25(1) are met. Since "unacceptable risks" have been banned under Article 5, they entail no obligations for any roles and have not been included in Table 2. Likewise, "minimal-risk" systems have no obligations, as noted in Section 3.1.3, and are therefore excluded from Table 2. As mentioned in Section 3.1.7, although protected by the EU AI Act, both users and affected persons (illustrated in Figure 2) are not considered actors under the Act and have therefore been excluded from the actor–

 doi:10.20944/preprints202509.1979.v1

risk obligations matrix. Their rights and interests, rather than the normative structure of the Act, are informed by Recitals 5–9 and 61–63.

The matrix of actor-specific obligations across risk levels reveals a fundamental regulatory asymmetry within the EU AI Act: entities situated closer to the development phase, such as providers, bear expansive and technically intensive compliance responsibilities. In contrast, actors downstream in the value chain, including distributors, importers, and deployers, are often expected to fulfil operational, ethical, and legal duties without comparable access to system architecture, training data, or design rationale. This fragmented accountability structure gives rise to misaligned incentives and enforcement gaps. For example, deployers must ensure proper human oversight and operational use in accordance with Articles 14 and 26, and in some instances, conduct a Fundamental Rights Impact Assessment under Article 27. Distributors and importers are likewise tasked with verifying compliance under Articles 23 and 24, but may lack the expertise or authority to interrogate opaque algorithmic systems.

While these asymmetries are structurally embedded in the value chain, the EU AI Act also seeks to temper them through explicit proportionality safeguards. The Act does not impose uniform obligations irrespective of context; instead, it acknowledges that compliance must remain reasonable and proportionate to both the risk category of the AI system and the role and capacity of the actor involved. Article 9(3) and (5) stipulate that risks need only be mitigated insofar as they can be "reasonably mitigated or eliminated" to achieve an "acceptable residual risk." Similarly, Recital 109 clarifies that obligations imposed on providers of general-purpose AI models must be "commensurate and proportionate to the type of model provider," thereby recognizing the disparity between multinational AI developers and smaller firms. In addition, Recital 143, together with Articles 58 and 62, mandates tailored support for SMEs and start-ups, including preferential and, in some cases, cost-free access to regulatory sandboxes, with costs required to remain "fair and proportionate." Taken together, these provisions acknowledge that the capacities of actors vary significantly, and that legal obligations should be calibrated accordingly—particularly when comparing global technology providers to municipal agencies, SMEs, or non-specialist deployers.

This uneven playing field employs one-size-fits-all compliance strategies, which are both impractical and potentially exclusionary. Moreover, as discussed in Section 3.1.6, the rise of General Purpose AI (GPAI) further blurs traditional role distinctions. Under Article 25, distributors, importers, or deployers that substantially modify a system, alter its intended purpose so that it falls within the high-risk categories of Article 6, or place the system on the market under their own name or trademark, are legally reclassified as providers. In such cases, they inherit the complete set of provider obligations under Article 16. This regulatory role fluidity introduces additional compliance complexity and risk, particularly for actors with limited institutional or technical capacity.

Table 2. Legal obligations per role and risk level (EU Regulation 2024/1689).

Actor Type	High Risk	Limited Risk
Provider	Lifecycle risk management (Art. 9), data governance (Art. 10), technical documentation (Art. 11), logging capabilities (Art. 12), transparency and instructions (Art. 13), human oversight (Art. 14), robustness, accuracy, and cybersecurity (Art. 15), Provider Identification (Art. 16(b)), Quality Management System (Art. 17), Maintain Technical Documentation (Art. 18), Logging Obligations (Art. 19),	Ensure Users Are Informed When Interacting with AI Systems (Art. 50(1), Recital 132), Mark Synthetic Content as Artificially Generated or Manipulated in Machine-Readable Format (Art. 50(2), Recital 133).

 doi:10.20944/preprints202509.1979.v1

	Corrective Actions & Reporting (Art. 20), Conformity Assessment (Art. 43), EU Declaration of Conformity (Art. 47), CE Marking (Art. 48), Registration in the EU Database (Art. 49(1)), Demonstrate Compliance upon Authority Request (Art. 16(k)), Accessibility Compliance (Art. 16(l), Recital 80)	
Importer	Verify Conformity Assessment by Provider (Art. 23(1)(a)), Verify Technical Documentation Exists (Art. 23(1)(b)), Ensure CE Marking, Declaration of Conformity, and Instructions Are Present (Art. 23(1)(c)), Verify Appointment of Authorised Representative (Art. 23(1)(d)), Withhold Market Placement if Non-compliant or Falsified (Art. 23(2)), Inform Authorities if System Poses a Risk (Art. 23(2)), Importer Identity and Contact Information (Art. 23(3)), Ensure Storage and Transport Do Not Jeopardise Compliance (Art. 23(4)), Retain Key Documentation for 10 Years (Art. 23(5)), Provide Authorities with Documentation Upon Request (Art. 23(6)), Ensure Technical Documentation Availability (Art. 23(6)), Cooperate with Authorities in Risk Mitigation Actions (Art. 23(7)).	No obligations specified under the EU AI Act
Distributor	Verify CE Marking, EU Declaration, Instructions, and Upstream Compliance (Art. 24(1)), Withhold Market Availability if Non-compliant or Risky (Art. 24(2)), Inform Provider or Importer if Risk is Identified (Art. 24(2)), Ensure Storage and Transport Conditions Preserve Compliance (Art. 24(3)), Take or Ensure Corrective Action, Withdrawal, or Recall if Non-compliant (Art. 24(4)), Inform Provider, Importer, and Authorities if System Poses a Risk (Art. 24(4)), Provide Documentation on Compliance Actions to Authorities Upon Request (Art. 24(5)), Cooperate with Authorities in Risk Mitigation Actions (Art. 24(6)).	No obligations specified under the EU AI Act
Deployer	Perform a FRIA (Art. 27) Ensure Use by Instructions for Use (Art. 29(1)), Assign Competent Human Oversight (Art. 29(2)), Ensure Relevant and Representative Input Data Under Their Control (Art. 29(4)), Monitor Operation and Inform Provider or Authorities in Case of Risk or Serious Incident (Art. 29(5)), Retain System Logs for a Minimum of Six Months if Under Their Control (Art. 29(6)),	Inform Individuals of Emotion Recognition or Biometric Categorisation Systems (Art. 50(3), Recital 132), Disclose Artificial Generation or Manipulation of Deepfake Content and Public-Facing

 doi:10.20944/preprints202509.1979.v1

	Inform Workers and Representatives Prior to Workplace Deployment (Art. 29(7), Recital 92), Public Deployers Must Verify Registration in EU Database (Art. 29(8)), Use Art. 13 Information for DPIA Compliance Where Applicable (Art. 29(9)), Request Judicial or Administrative Authorisation Before Using Post-Remote Biometric ID Systems in Criminal Investigations (Art. 29(10), Recital 94–95), Inform Natural Persons When Affected by Decisions from Annex III Systems (Art. 29(11)), Cooperate with Competent Authorities (Art. 29(12)).	AI-Generated Text (Art. 50(4), Recital 134)systems (Art. 52)
Product Manufacturer	Ensure Prevention and Mitigation of Safety Risks from AI Components in Products, Including Autonomous Robots and Diagnostic Systems in High-Stakes Contexts like Health and Manufacturing (Recital 47), Ensure Safety of Non-High-Risk AI Systems via General Product Safety Regulation (EU) 2023/988 as a Complementary Safeguard (Recital 166)	No obligations specified under the EU AI Act
Authorized Representative (Agent)	Appointment by Written Mandate (Art. 22(1)), Task Performance as Mandated by Provider (Art. 22(2)), Provide Mandate Copy to Authorities Upon Request (Art. 22(3)), Verify EU Declaration and Technical Documentation (Art. 22(3)(a Retain Provider Contact Details and Compliance Documentation for 10 Years (Art. 22(3)(b)), Provide Information and Access to Logs to Authorities Upon Request (Art. 22(3)(c)), Cooperate with Authorities in Risk Mitigation (Art. 22(3)(d)), Ensure Registration Compliance or Verify Accuracy if Done by Provider (Art. 22(3)(e)), Accept Regulatory Contact on Provider's Behalf (Art. 22(3), final sentence), Terminate Mandate if Provider Breaches Obligations and Inform Authorities (Art. 22(4)).	No obligations specified under the EU AI Act

3.2. Ethics and Governance: The ALTAI Checklist

3.2.1. Origins and Principles

The Assessment List for Trustworthy Artificial Intelligence (ALTAI) was introduced in 2020 by the European Commission's High-Level Expert Group on AI as a self-assessment tool grounded in the Ethics Guidelines for Trustworthy AI. It operationalizes seven core requirements identified in the Guidelines: human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity, non-discrimination, and fairness, societal and environmental well-being, and accountability. These principles reflect a normative commitment to ensuring AI is not only technically efficient but also aligned with fundamental rights and societal values. [12]. ALTAI's strength lies in translating these abstract ethical ideals into structured, measurable

 doi:10.20944/preprints202509.1979.v1

dimensions. Unlike high-level declarations such as the OECD Principles or UNESCO's Recommendations, ALTAI is designed explicitly for practical deployment by developers and deployers, making it a cornerstone in the EU's AI governance ecosystem [13].

3.2.2. Role in EU Governance

Within the EU regulatory landscape, ALTAI is a foundational instrument and a bridge between soft law and formal regulation. Though voluntary, it has been influential in shaping the ethical underpinnings of the EU AI Act and guiding principles in the European AI Strategy and Coordinated Plan [14]. It enables entities to align their operations with expectations of transparency, accountability, and fairness, without yet being subject to direct legal mandates. ALTAI helps operationalize the EU's emphasis on trustworthy AI by translating principles into data governance tasks, particularly in areas of auditability and data traceability [11]. However, this integration is still evolving. While the EU AI Act mandates conformity assessments and documentation, it does not codify ALTAI as a binding checklist. Thus, ALTAI's influence is normative, serving more as ethical scaffolding than enforceable regulation. While ALTAI is formally a soft law instrument, non-binding and not directly referenced in the EU AI Act's legal text, it has gained practical traction as an auxiliary tool in semi-formal governance settings. Notably, it is increasingly deployed to support Fundamental Rights Impact Assessments (FRIAs), especially in contexts where no sector-specific templates exist. This functional absorption gives ALTAI quasi-regulatory influence despite its voluntary nature. The implication is twofold. First, its ethical framing is shaping compliance expectations even in the absence of legal obligation. Second, its operational under-specification limits its utility unless translated into auditable processes.

3.2.3. Strengths and Normative Value

The key strength of ALTAI is its accessibility and comprehensiveness. It provides a step-by-step tool with questions and indicators that organizations can use to self-assess compliance with the EU's ethical AI vision. ALTAI is particularly effective in articulating the ethical pillars of accountability, explainability, and usability in a manner that is intelligible to non-specialist audiences [15]. Furthermore, ALTAI represents a significant shift toward procedural ethics, ensuring that ethical principles are embedded throughout the system design and development processes, rather than merely evaluated ex post. ALTAI's modular design can be tailored to varied contexts, making it a flexible and scalable ethics tool [16]. Normatively, ALTAI reinforces the idea of ethics as a continuous, systemic obligation in AI governance, rather than a one-time evaluation. Its emphasis on human oversight and technical robustness ensures alignment with broader EU policy on fundamental rights and sustainable development. It exemplifies governance by design, embedding compliance and accountability directly into the development pipeline [17].

3.2.4. Sector-Specific Ethical Tensions

While the ALTAI checklist provides a high-level overview of ethical principles, concrete deployments of AI systems reveal practical tensions between these ideals. In healthcare, large language models used in clinical decision support often lack explainability, raising concerns about patient autonomy and trust [18]. In law enforcement contexts such as border control, the use of biometric surveillance tools like iBorderCtrl has sparked criticism over proportionality, privacy, and discriminatory risk [7]. Ethical principles also frequently conflict with one another. Transparency and explainability may undermine data minimization or expose sensitive operational logic, while fairness-enhancing techniques may reduce model performance or introduce new trade-offs. These tensions underscore the need for ethical frameworks that not only articulate principles but also provide mechanisms for prioritizing and resolving competing values in context-specific applications.

3.2.5. Limitations in Security and Enforceability

 doi:10.20944/preprints202509.1979.v1

Despite its normative strengths, ALTAI has several limitations that constrain its practical utility. First, its voluntary nature means there are no formal enforcement mechanisms, leading to questions about its impact in commercial settings where ethical commitments may be deprioritized [19]. Second, the checklist prioritizes procedural ethics over outcome accountability, providing limited guidance on evaluative metrics or real-world benchmarks. This self-assessment structure leaves room for performative ethics, also known as "ethics washing" [20]. Third, ALTAI is inadequate for applications in high-risk areas such as law enforcement or military systems, where adversarial robustness and technical security standards are essential; it remains too general for these contexts [8]. Lastly, ALTAI assumes organizational capacities, including technical, financial, and human, that are often unavailable to small and medium-sized enterprises. Without standardized compliance tools or external audit mechanisms, ALTAI risks being inaccessible or ineffectual for under-resourced actors [16]. These structural limitations frame ALTAI as a foundational, yet ultimately limited, ethical governance instrument.

3.3. Comparative Compliance Frameworks

Existing AI governance models differ not only in scope and application but also in their underlying assumptions about how compliance should be structured. Some reflect a "governance by audit" paradigm, emphasizing post-deployment documentation and oversight. In contrast, others adopt a "governance by design" approach, embedding legal and ethical obligations into the development lifecycle itself. This distinction is particularly relevant for this research, which seeks to develop a compliance framework that is both auditable and adaptable. Section 3.3.1 examines audit-oriented models such as the OECD AI Principles and the NIST AI Risk Management Framework (RMF), which provide voluntary, checklist-based governance structures. Section 3.3.2 turns to design-integrated approaches, including ISO/IEC 42001 and Responsible AI models, which reflect a shift toward iterative, feedback-driven governance. These models conceptualize compliance not as a static certification event, but as a dynamic process—an approach increasingly reflected in modern cybersecurity and risk frameworks, particularly suited to complex socio-technical systems.

3.3.1. Audit-Oriented Frameworks

NIST AI Risk Management Framework (RMF)

The National Institute of Standards and Technology (NIST) introduced its AI Risk Management Framework in 2023 to provide voluntary, sector-agnostic guidance for managing AI-related risks. Structured around four core functions —Map, Measure, Manage, and Govern —the RMF supports innovation while promoting responsible AI use [21]. However, the RMF's emphasis on post-deployment monitoring limits its adaptability in fast-evolving or adversarial contexts. RMF tends to treat risk as a static entity rather than a co-evolving relationship between the system and its context [22]. Furthermore, its uptake among SMEs remains low, mainly due to the high documentation burdens and limited tailoring for lower-resourced actors. Its focus on governance by audit risks overlooks upstream design flaws that could otherwise be mitigated through embedded safeguards.

OECD AI Principles

The OECD's 2019 AI Principles, endorsed by over 40 countries, articulate five core commitments: inclusive growth, human-centered values, transparency, robustness and security, and accountability. These principles have informed numerous national AI strategies, including the ethical foundations of the EU AI Act. However, the OECD framework remains non-binding and conceptually broad. Its implementation is inconsistent across jurisdictions, and its guidance lacks operational specificity [23]. While it contributes to normative alignment, its function remains primarily aspirational and symbolic, with its effect heavily dependent on local political will and the degree of regulatory integration.

3.3.2. Design-Integrated Frameworks

ISO/IEC 42001 – AI Management Systems

 doi:10.20944/preprints202509.1979.v1

ISO/IEC 42001, released in late 2023, is the first international standard for AI Management Systems (AIMS). Developed by ISO and the IEC, it provides organizations with structured procedures for risk management, traceability, and continuous improvement. It is designed to be compatible with ISO/IEC 27001 and 9001, embedding AI governance into the broader strategic and operational fabric of organizations. This framework embodies "governance by design" by requiring organizations to treat AI compliance as an ongoing management process, rather than a one-time audit. Its emphasis on continuous documentation, leadership engagement, and iterative improvement closely mirrors the PDCA cycle, an established model for quality and security governance. However, ISO 42001 poses high entry barriers for SMEs, both in terms of cost and procedural formality [24]. Its uptake remains skewed toward large institutions, particularly in regulated sectors like finance [25].

Responsible AI Models

Responsible AI (RAI) models aim to bridge the gap between normative ethics and legal compliance by integrating embedded technical safeguards. These models often draw from design philosophy, integrating obligations directly into system architecture. For instance, using deontic logic to encode legal and ethical rules as system constraints, effectively "building in" responsibility [26]. Other emerging RAI models utilize decentralized governance architectures, such as blockchain-based tokenized compliance tools. While these promote traceability and stakeholder participation, they face challenges in institutional adoption and interoperability. RAI models must possess context-aware, interdisciplinary, and adaptive qualities that align well with circular compliance strategies, but are challenging to implement without clear regulatory scaffolding or technical maturity [27].

2.3.3. Alignment and Gaps

Despite differences in enforcement, scope, and formality, audit- and design-oriented frameworks share broad commitments to transparency, accountability, and fairness. However, key implementation gaps remain. For example, while the EU AI Act mandates non-discrimination, it does not specify computational fairness standards, leaving technical choices to providers [28]. More fundamentally, the divide between governance by design and governance by audit is not merely procedural but epistemological: the former views compliance as embedded and evolving. At the same time, the latter treats it as external and retrospective. Effective AI governance must treat systems as socio-technical artifacts, requiring continuous oversight, contextual adaptation, and cross-functional collaboration [22]—principles that are poorly reflected in static audit regimes. This analysis supports the argument that a living, auditable framework, capable of balancing minimal enforceability with real-world adaptability, is necessary for supporting low-capacity actors within the EU AI compliance ecosystem.

3.4. Implementation Gaps and Legal Complexity

3.4.1. Challenges in Translating Regulation to Practice

While the EU AI Act outlines a detailed framework for managing the risks associated with artificial intelligence, the practical implementation of its provisions into everyday institutional operations remains highly uneven. This is particularly evident in high-risk domains, such as healthcare and finance, where the complexity of AI systems often outpaces current legal and technical infrastructures. In the healthcare context, compliance mechanisms vary significantly across jurisdictions, and regulatory clarity is often lacking, despite the AI Act's harmonizing intent [29]. The financial sector emphasizes the importance of early compliance integration and transparent documentation [25], noting that while many institutions recognize the need for regulatory oversight, few have successfully implemented continuous monitoring practices. This lag is symptomatic of a broader implementation challenge: translating legal requirements into organizational behavior in a timely, consistent manner.

 doi:10.20944/preprints202509.1979.v1

3.4.2. Resource Asymmetry

The Burden on SMEs A recurring concern in AI governance is the disproportionate burden of regulatory compliance on small and medium-sized enterprises (SMEs). ISO/IEC 42001, while comprehensive, imposes significant documentation, monitoring, and auditing requirements that may exceed the capacity of resource-constrained actors. SMEs struggle to adapt management processes to align with ISO/IEC 42001 due to both technical and human resource limitations [24]. Similarly, the EU AI Act mandates conformity assessments, data quality checks, and traceability obligations for high-risk systems, requirements that often demand legal, technical, and regulatory expertise well beyond the operational scope of smaller firms. The redrafting of the AI Act prioritized fundamental rights but failed to account for resource disparities across the innovation ecosystem [30]. This imbalance raises concerns about the inclusivity of the regulation and its potential to stifle smaller-scale innovation unintentionally. For such actors, RegTech tools can serve as scaffolding mechanisms, automating routine checks, generating documentation, or embedding legal logic, thereby reducing the compliance burden without sacrificing legal sufficiency [31].

3.4.3. Fragmentation and Contradictions GDPR vs EU AI Act

Another layer of complexity emerges from the legal fragmentation between the EU AI Act and the General Data Protection Regulation (GDPR). While both frameworks aim to safeguard fundamental rights, they originate from different regulatory logics: product safety in the case of the AI Act, and privacy protection in the case of the GDPR. This divergence creates inconsistencies in implementation, particularly around lawful data processing, consent requirements, and impact assessments. For instance, Article 14 of the AI Act mandates human oversight in high-risk AI systems, whereas Article 22 of the GDPR places strict limitations on automated decision-making. Similarly, GDPR's emphasis on data minimization (Art. 5(1)(c)) and purpose limitation (Art. 5(1)(b)) can conflict with AI models that require large, diverse datasets for practical training. The AI Act's lack of computational specificity in defining fairness and non-discrimination further complicates its alignment with the GDPR's more explicit mandates on individual rights [28]. These contradictions underscore the need for interpretive guidance and integrated regulatory oversight. Without a harmonized interface between the GDPR and the EU AI Act, deployers are left to navigate overlapping obligations and inconsistent audit demands. Effective compliance will likely depend on sector-specific interpretations, greater administrative coordination, and improved regulatory literacy among AI providers [32].

3.4.4. Iterative Governance as a Low-Burden Strategy for SMEs

While regulatory frameworks such as the EU AI Act and ISO/IEC 42001 offer structured approaches to AI governance, their implementation often presumes institutional capacities, legal, technical, and administrative, that many small and medium-sized enterprises (SMEs) may struggle to meet. This does not imply that SMEs cannot or should not achieve compliance; instead, it suggests that the means of achieving compliance must be adapted to their specific realities. Several studies have noted that static, audit-heavy models impose disproportionate burdens on under-resourced actors [24,33], creating barriers to entry even for actors committed to compliance. As a response, iterative governance has emerged as a more sustainable and SME-aligned approach. Rather than treating compliance as a one-time certification or exhaustive audit, iterative models conceptualize it as a continuous, cyclical process of incremental improvement. This reduces immediate administrative pressure while embedding compliance into everyday organizational behavior. Studies of lightweight quality systems have demonstrated that scalable, feedback-driven models significantly lower adoption thresholds by prioritizing contextual flexibility, progressive alignment, and organizational learning [34,35]. Conventional cybersecurity and governance standards, including the NIST framework, often fail to accommodate the Specific constraints of SMEs [36]. Their study emphasizes the need for dynamic, responsive, and technologically tailored governance strategies that evolve with an organization's maturity and risk exposure. Iterative approaches offer SMEs a pathway to

 doi:10.20944/preprints202509.1979.v1

regulatory legitimacy, including under the EU AI Act, without requiring immediate full-spectrum compliance. This vision of iterative, low-friction compliance aligns with emerging regulatory thinking that emphasizes dynamic, context-aware governance. Scholars have advocated for anticipatory and agile regulation in digital domains, where compliance tools are embedded in daily operations and refined over time through feedback, risk exposure, and institutional learning [37]. Rather than relying solely on static, audit-based mechanisms, these models promote compliance as a process, a living system that adapts to both technological change and evolving organizational capacity. Such models suggest that effective AI governance for SMEs may require compliance infrastructures that evolve in parallel with institutional capabilities, rather than demanding immediate, full-spectrum implementation.

3.5. Framing Least Responsible AI Controls

3.5.1. Rationale and Structural Asymmetry

As outlined in Section 3.1.8, the EU AI Act formally allocates responsibilities across various roles, including providers, deployers, and importers. However, real-world enforcement patterns are far less symmetrical. Small and medium-sized enterprises SMEs in financial services face extensive documentation and impact assessment requirements despite lacking the internal governance structures to meet them [25]. Similarly, public institutions, although subject to strict transparency and oversight expectations, are structurally under-resourced to fulfil them [38]. This reveals a critical governance flaw: formal role-based compliance often demands more than what constrained actors can realistically implement. Their operational capacity does not match the legal exposure of these actors. This disconnect can be referred to as regulatory realism, which involves assessing legal obligations not by their normative ambition, but by their implementability within uneven institutional landscapes [22]. In this context, the central question becomes: What constitutes a legally sufficient and auditable set of controls when full-spectrum compliance is infeasible? For many actors, especially those without access to technical system design or legal expertise, the answer lies not in aspirational ethics but in minimum viable compliance: a control set that fulfils the letter of the law while remaining feasible, traceable, and role-sensitive.

3.5.2. Idealism vs Legal Sufficiency

Mainstream AI governance frameworks, such as ALTAI, ISO/IEC 42001, and the NIST AI RMF, promote extensive normative values: fairness, explainability, robustness, and human oversight. However, empirical evaluations have highlighted critical gaps. These frameworks fail to account for approximately 69% of known AI security vulnerabilities, particularly in cases where actors lack the capacity for technical implementation [5]. While valuable as aspirational instruments, these frameworks frequently fall short of providing enforceable or auditable pathways to compliance. Moreover, regulatory capture by dominant AI providers tends to shift obligations downstream [39]. As a result, deployers, system integrators, and even public sector actors are expected to retain logs, implement oversight, and document risks, often without access to internal model architecture or training data. These role asymmetries turn formal accountability into a structural mismatch. Rather than pursue frameworks that presume full ethical maturity, AI compliance must prioritize what is strictly required. A minimal set of legally anchored controls, clearly mapped to articles of the EU AI Act, auditable through evidence, and feasibly actionable by constrained actors, provides a more realistic foundation for compliance. This does not imply an abandonment of ethics but recognizes the need for structured enablement over idealistic projection.

3.5.3. Enabling Compliance in Low-Capacity Settings

Legal obligations must be translated into structured organizational routines to be effective [29]. Compliance must be enabled, not merely demanded. This argument holds particular weight in AI governance, where obligations such as risk management (Art. 9) or data governance (Art. 10) cannot be fulfilled without accompanying operational structures. Cloud-based, interoperable compliance

 doi:10.20944/preprints202509.1979.v1

systems should lower entry barriers for auditability, documentation, and traceability [33]. The AGORA database [40], which catalogues over 330 global AI governance instruments, confirms that most tools lack implementation mechanisms for low-capacity actors. Without tangible compliance infrastructures, legal requirements risk becoming symbolic, reinforcing inequality rather than accountability. As such, the concept of Least Responsible AI Controls offers a governance logic that does not rely on voluntary overcompliance or institutional abundance. Instead, it reflects a baseline of defensible, minimum obligations that actors must meet to comply with the EU AI Act under real-world conditions.

4. Results

The earlier sections demonstrate that, while the European Union's AI governance system, including the EU AI Act, the ALTAI checklist, and other tools, is broadly structured, it also presents several conceptual and operational challenges. Despite its broad aims, the EU AI Act has unclear definitions (such as fairness), mismatched with other legal frameworks (like the GDPR), and limited enforcement capacity across Member States [28,32]. Moreover, as Sections 3.2 and 3.3 highlight, governance tools such as ALTAI, NIST RMF, ISO/IEC 42001, and the OECD Principles are effective at establishing high-level values but struggle in real-world ecosystems with multiple actors and complex risks. These frameworks often assume that organizations have high levels of maturity and technical skill, which is not always the case in the public and private sectors. Notably, ALTAI's procedural ethics model lacks direct enforceability and does not provide clear metrics to measure outcomes, thereby limiting its usefulness in high-risk areas [8,20]. Research on compliance also shows issues with scalability. For example, the NIST RMF is flexible but not ideal for dynamic, evolving AI systems. Similarly, ISO/IEC 42001, as it attempts to integrate AI into existing management systems, faces challenges due to high costs and stringent requirements, particularly for small and medium-sized enterprises [24,25]. The central assumption across these frameworks is that organizations have sufficient resources, transparency, and an understanding of regulations, conditions that are often not present in practice. Instead of aiming for perfect or all-encompassing governance, a more fit approach should focus on the smallest set of enforceable obligations that actors with limited capacity, such as SMEs and public sector entities, can realistically meet. These actors typically lack access to detailed system internals and specialized compliance infrastructure, making full compliance impossible. Frameworks should emphasize a set of minimal requirements to address the identified accountability gap that arises when legal demands exceed operational capabilities.

5. Suggestions for Future Research

The literature reveals an unmet need for minimal governance instruments (in terms of administrative overhead), auditable (traceable and transparent), and secure (robust against adversarial risk). Such tools should prioritize baseline legal sufficiency over aspirational ethics, particularly for low-capacity actors. The current global regulatory environment lacks interoperable, role-specific compliance that can be embedded into technical systems and institutional workflows [40]. Cloud-native, plug-and-play governance modules to support compliance among less mature actors [33]. These perspectives support the case for designing compliance frameworks that serve as both legal instruments and scalable infrastructure. The literature also calls for enhanced meta-regulatory coordination. There is a need for cross-sectoral harmonization, particularly where the EU AI Act and GDPR impose overlapping but potentially contradictory obligations [29,41]. Without integrated regulatory guidance or shared compliance tools, fragmented governance will persist. The literature reveals that AI compliance is not a binary state, but rather a gradient ranging from strict legal sufficiency to aspirational ethical governance.

Author Contributions: "Conceptualization, W.W.F.; methodology, W.W.F.; validation, W.W.F.; writing—original draft preparation, W.W.F.; writing—review and editing, M.B. All authors have read and agreed to the published version of the manuscript.

 doi:10.20944/preprints202509.1979.v1

Funding: This research received no external funding.

Data Availability Statement: All data are available from the article. Any data and any code that readers are not able to (re)produce are available upon request.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Zhao, W.X.; Zhou, K.; Li, J.; Tang, T.; Wang, X.; Hou, Y.; Min, Y.; Zhang, B.; Zhang, J.; Dong, Z.; et al. A Survey of Large Language Models 2023.
2. Iyelolu, T.V.; Agu, E.E.; Idemudia, C.; Ijomah, T.I. Driving SME Innovation with AI Solutions: Overcoming Adoption Barriers and Future Growth Opportunities. *International Journal of Science and Technology Research Archive* **2024**, *7*, 036–054.
3. Jafarzadeh, P.; Vähämäki, T.; Nevalainen, P.; Tuomisto, A.; Heikkonen, J. Supporting SME Companies in Mapping out AI Potential: A Finnish AI Development Case. *J Technol Transf* **2024**, doi:10.1007/s10961-024-10122-5.
4. Golpayegani, D.; Pandit, H.J.; Lewis, D. Comparison and Analysis of 3 Key AI Documents: EU's Proposed AI Act, Assessment List for Trustworthy AI (ALTAI), and ISO/IEC 42001 AI Management System. In *Artificial Intelligence and Cognitive Science*; Longo, L., O'Reilly, R., Eds.; Communications in Computer and Information Science; Springer Nature Switzerland: Cham, 2023; Vol. 1662, pp. 189–200 ISBN 978-3-031-26437-5.
5. Madhavan, K.; Yazdinejad, A.; Zarrinkalam, F.; Dehghantanha, A. Quantifying Security Vulnerabilities: A Metric-Driven Security Analysis of Gaps in Current AI Standards 2025.
6. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews. *BMJ* **2021**, n71, doi:10.1136/bmj.n71.
7. Kalodanis, K.; Rizomiliotis, P.; Feretzakis, G.; Papapavlou, C.; Anagnostopoulos, D. High-Risk AI Systems—Lie Detection Application. *Future Internet* **2025**, *17*, 26.
8. Li, Z. AI Ethics and Transparency in Operations Management: How Governance Mechanisms Can Reduce Data Bias and Privacy Risks. *Journal of Applied Economics and Policy Studies* **2024**, *13*, 89–93, doi:10.54254/2977-5701/13/2024130.
9. Rintamaki, T.; Pandit, H.J. Developing an Ontology for AI Act Fundamental Rights Impact Assessments 2024.
10. Golpayegani, D. Semantic Frameworks to Support the EU AI Act's Risk Management and Documentation. PhD Thesis, Trinity College, 2024.
11. Bhouri, H. Navigating Data Governance: A Critical Analysis of European Regulatory Framework for Artificial Intelligence. *Recent Advances in Public Sector Management* **2025**, 171.
12. Kriebitz, A.; Corrigan, C.; Boch, A.; Evans, K.D. Decoding the EU AI Act in the Context of Ethics and Fundamental Rights. In *The Elgar Companion to Applied AI Ethics*; Edward Elgar Publishing, 2024; pp. 123–152 ISBN 1-80392-824-7.
13. Sun, N.; Miao, Y.; Jiang, H.; Ding, M.; Zhang, J. From Principles to Practice: A Deep Dive into AI Ethics and Regulations. *arXiv preprint arXiv:2412.04683* **2024**.
14. Karami, A. Artificial Intelligence Governance in the European Union. *Journal of Electrical Systems* **2024**, *20*, 2706–2720, doi:10.52783/jes.7938.
15. Iyer, V.; Manshad, M.; Brannon, D. A Value-Based Approach to AI Ethics: Accountability, Transparency, Explainability, and Usability. *Mercados y negocios* **2025**, *26*, 3–12.
16. Aiyankovil, K.G.; Lewis, D. Harmonizing AI Data Governance: Profiling ISO/IEC 5259 to Meet the Requirements of the EU AI Act. In *Legal Knowledge and Information Systems*; IOS Press, 2024; pp. 363–365.
17. Ashraf, Z.A.; Mustafa, N. AI Standards and Regulations. *Intersection of Human Rights and AI in Healthcare* **2025**, 325–352.
18. Comeau, D.S.; Bitterman, D.S.; Celi, L.A. Preventing Unrestricted and Unmonitored AI Experimentation in Healthcare through Transparency and Accountability. *npj Digital Medicine* **2025**, *8*, 42.

 doi:10.20944/preprints202509.1979.v1

19. Scherz, P. Principles and Virtues in AI Ethics. *Journal of Military Ethics* **2024**, *23*, 251–263.
20. Ho, C.-Y. A Risk-Based Regulatory Framework for Algorithm Auditing: Rethinking "Who," "When," and "What." *Tennessee Journal of Law and Policy* **2025**, *17*, doi:10.70658/1940-4131.1268.
21. NIST AI Risk Management Framework. *NIST* **2021**.
22. Janssen, M. Responsible Governance of Generative AI: Conceptualizing GenAI as Complex Adaptive Systems. *Policy and Society* **2025**, puae040.
23. Al-Omari, O.; Alyousef, A.; Fati, S.; Shannaq, F.; Omari, A. Governance and Ethical Frameworks for AI Integration in Higher Education: Enhancing Personalized Learning and Legal Compliance. *Journal of Ecohumanism* **2025**, *4*, 80-86-80–86.
24. Proietti, S.; Magnani, R. Assessing AI Adoption and Digitalization in SMEs: A Framework for Implementation. *arXiv preprint arXiv:2501.08184* **2025**.
25. Thoom, S.R. Lessons from AI in Finance: Governance and Compliance in Practice. *Int. J. Sci. Res. Arch.* **2025**, *14*, 1387–1395, doi:10.30574/ijsra.2025.14.1.0235.
26. Dimitrios, Z.; Petros, S. Towards Responsible AI: A Framework for Ethical Design Utilizing Deontic Logic. *International Journal on Artificial Intelligence Tools* **2025**.
27. Ajibesin, A.A.; Çela, E.; Vajjhala, N.R.; Eappen, P. Future Directions and Responsible AI for Social Impact. In *AI for Humanitarianism*; CRC Press, 2025; pp. 206–220.
28. Meding, K. It's Complicated. The Relationship of Algorithmic Fairness and Non-Discrimination Regulations in the EU AI Act 2025.
29. Busch, F.; Geis, R.; Wang, Y.-C.; Kather, J.N.; Khori, N.A.; Makowski, M.R.; Kolawole, I.K.; Truhn, D.; Clements, W.; Gilbert, S.; et al. AI Regulation in Healthcare around the World: What Is the Status Quo? 2025.
30. Palmiotto, F. The AI Act Roller Coaster: The Evolution of Fundamental Rights Protection in the Legislative Process and the Future of the Regulation. *European Journal of Risk Regulation* **2025**, 1–24, doi:10.1017/err.2024.97.
31. Liang, P. Leveraging Artificial Intelligence in Regulatory Technology (RegTech) for Financial Compliance. *Applied and Computational Engineering* **2024**, *93*, 166–171.
32. Paolini E Silva, M.; Tamo-Larrieux, A.; Ammann, O. AI Literacy Under the AI Act: Tracing the Evolution of a Weakened Norm 2025.
33. Olufunbi Babalola; Adebisi Adedoyin; Foyeke Ogundipe; Adebola Folorunso; Chineme Edger Nwatu Policy Framework for Cloud Computing: AI, Governance, Compliance and Management. *Global J. Eng. Technol. Adv.* **2024**, *21*, 114–126, doi:10.30574/gjeta.2024.21.2.0212.
34. Gasser, U.; Almeida, V.A.F. A Layered Model for AI Governance. *IEEE Internet Comput.* **2017**, *21*, 58–62, doi:10.1109/MIC.2017.4180835.
35. Heeks, R.; Renken, J. Data Justice for Development: What Would It Mean? *Information Development* **2018**, *34*, 90–102, doi:10.1177/0266666916678282.
36. Safa, N.S.; Solms, R.V.; Furnell, S. Information Security Policy Compliance Model in Organizations. *Computers & Security* **2016**, *56*, 70–82, doi:https://doi.org/10.1016/j.cose.2015.10.006.
37. Yeung, K.; Lodge, M. *Algorithmic Regulation*; Oxford University Press, 2019; ISBN 0-19-257543-0.
38. Popa, D.M. Frontrunner Model for Responsible AI Governance in the Public Sector: The Dutch Perspective. *AI Ethics* **2024**, doi:10.1007/s43681-024-00596-2.
39. Wei, K.; Ezell, C.; Gabrieli, N.; Deshpande, C. How Do AI Companies "Fine-Tune" Policy? Examining Regulatory Capture in AI Governance. *AIES* **2024**, *7*, 1539–1555, doi:10.1609/aies.v7i1.31745.
40. Arnold, Z.; Schiff, D.S.; Schiff, K.J.; Love, B.; Melot, J.; Singh, N.; Jenkins, L.; Lin, A.; Pilz, K.; Enweareazu, O.; et al. Introducing the AI Governance and Regulatory Archive (AGORA): An Analytic Infrastructure for Navigating the Emerging AI Governance Landscape. *AIES* **2024**, *7*, 39–48, doi:10.1609/aies.v7i1.31615.
41. Singh, L.; Randhelia, A.; Jain, A.; Choudhary, A.K. Ethical and Regulatory Compliance Challenges of Generative AI in Human Resources. In *Generative Artificial Intelligence in Finance*; Chelliah, P.R., Dutta, P.K., Kumar, A., Gonzalez, E.D.R.S., Mittal, M., Gupta, S., Eds.; Wiley, 2025; pp. 199–214 ISBN 978-1-394-27104-7.

 doi:10.20944/preprints202509.1979.v1