Legal Autonomous Web-based Governance (LAW)
Vol. 1, No. 2, October 2026, pp. 214∼227
E-ISSN: XXXX-XXXX | P-ISSN: xxxx-xxxx

Legal Frameworks for Responsible Artificial Intelligence in Digital Business

Adam Faturahman[1], Sherli Triandari[2], Ramzi Zainum Ikhsan[3], Aswadi Jaya [4], Emilyani[5*]
[1,2]Faculty of Science and Technology, Universitas Raharja, Indonesia
[3]Faculty of Economics and Business, Universitas Raharja, Indonesia
[4]Master's Program in English Language Education, Universitas PGRI Palembang, Indonesia
[5]Department of Law and Technology, Rey Incorporation, United States
[1]adam.faturahman@raharja.info, [2]sherli@raharja.info, [3]ramzi.zainum@raharja.info, [4]aswadijaya@univpgri-palembang.ac.id, [5]Emilyani@rey.zone
***Corresponding Author**

Article Info

Article history:

Submission April 22, 2026
Revised August 26, 2026
Accepted August 30, 2026
Published August 31, 2026

Keywords:

Legal
Governance
Digital
Responsible
Business

ABSTRACT

The growing integration of Artificial Intelligence (AI) across digital business ecosystems has transformed how organizations pursue automation, foster innovation, and utilize data in decision-making processes. However, these technological developments also generate significant legal considerations concerning accountability, transparency, privacy, algorithmic discrimination, and human supervision. **This study examines an integrated legal framework for responsible AI governance** that balances technological innovation, legal certainty, stakeholder protection, and sustainable digital transformation. **Using a normative juridical and comparative legal approach**, the study analyzes legal instruments, international AI governance frameworks, academic literature, and policy documents, including the EU AI Act, OECD AI Principles, UNESCO AI Ethics Recommendation, and NIST AI Risk Management Framework. **The results indicate that existing frameworks** provide important but differentiated foundations for responsible AI but remain fragmented in regulatory status, scope, and implementation mechanisms; therefore, this study develops an integrated framework comprising four dimensions: Legal Accountability, Transparency and Explainability, Risk-Based Compliance, and Human-Centric Oversight. **These dimensions operate throughout the AI** lifecycle through preventive, monitoring, and corrective governance mechanisms, linking legal responsibilities with organizational controls, risk management, transparency, and meaningful human intervention. The study concludes that integrated AI governance provides a conceptual basis for translating responsible AI principles into organizational policies and lifecycle-based governance while supporting fairness, privacy, safety, accountability, stakeholder trust, and sustainable digital business development.

This is an open access article under the CC BY 4.0 license.

This is an open access article under the CC BY license (https://creativecommons.org/licenses/by/4.0/)
©Authors retain all copyrights

1. INTRODUCTION

AI has become a strategic component of digital business, supporting market analysis, customer personalization, supply-chain optimization, fraud detection, human-resource management, automation, and managerial decision-making. The integration of machine learning, generative AI, automated decision systems, and algorithmic analytics improves efficiency, scalability, innovation, and competitiveness but also creates legal,

ethical, and governance challenges due to probabilistic models, evolving datasets, and opaque decision-making processes [1]. AI-supported decisions in areas such as recruitment, credit assessment, pricing, advertising, and customer profiling may produce biased, inaccurate, discriminatory, unsafe, or opaque outcomes. These challenges demonstrate the need to integrate technological innovation with legal accountability, human rights, privacy, transparency, cybersecurity, and organizational responsibility through responsible AI governance [2]. The regulatory landscape increasingly reflects this need. The European Union AI Act, Regulation (EU) 2024/1689, establishes risk-based requirements covering prohibited practices, high-risk systems, transparency, governance, and enforcement [11]. The OECD AI Principles emphasize trustworthy AI, human rights, democratic values, accountability, traceability, and risk management throughout the AI lifecycle [3]. UNESCO promotes human dignity, transparency, fairness, accountability, privacy, and human oversight, while NIST's Artificial Intelligence Risk Management Framework (AI RMF 1.0) provides an organizational approach to identifying, assessing, and managing AI risks across the AI lifecycle, complemented by its Generative AI Profile [4]. Collectively, these instruments demonstrate a shift toward combining legal requirements, organizational governance, and lifecycle-based risk management.

However, these frameworks differ in legal status, institutional scope, and implementation mechanisms. The EU AI Act establishes binding obligations, whereas the OECD and UNESCO frameworks primarily provide normative principles and NIST offers a voluntary operational risk-management structure [5]. Consequently, digital businesses may face difficulties translating principles such as accountability, transparency, human oversight, and fairness into concrete responsibilities and compliance procedures, particularly when operating across jurisdictions, relying on third-party AI providers, processing extensive personal data, or distributing responsibility among multiple AI actors [6]. The central research gap is therefore not the absence of responsible AI principles but their limited integration into a coherent legal and organizational governance structure. Existing approaches often address human rights, ethics, regulatory compliance, or technical risk management separately, without fully explaining how legal responsibility, transparency, risk-based compliance, and human oversight can operate together throughout the AI lifecycle. This study addresses this gap by developing an integrated legal framework comprising four dimensions: Legal Accountability, Transparency and Explainability, Risk-Based Compliance, and Human-Centric Oversight [7]. The framework integrates legal obligations, organizational controls, and human intervention from AI design and development through deployment, monitoring, evaluation, and remediation.

The framework also seeks to balance technological innovation with regulatory proportionality. Excessive regulation may increase compliance costs and constrain AI adoption, while insufficient regulation may increase risks involving privacy, discrimination, unsafe systems, opaque decisions, legal liability, and stakeholder trust [8]. A risk-based approach therefore differentiates governance requirements according to the potential impact and severity of AI-related risks, with stronger controls for higher-impact applications and proportionate requirements for lower-risk systems [9]. Responsible AI governance is also relevant to sustainable digital transformation. Sustainability should encompass not only technological and economic efficiency but also social, institutional, and environmental dimensions. Responsible AI can support privacy, fairness, human dignity, accountability, transparency, human oversight, institutional resilience, and responsible resource use throughout the AI lifecycle [10]. This perspective reinforces its relevance to SDG 9 on Industry, Innovation and Infrastructure and SDG 16 on Peace, Justice and Strong Institutions.

These challenges are particularly relevant in emerging regulatory environments such as Indonesia, where AI adoption is developing alongside evolving legal and institutional arrangements. Responsible AI implementation requires coordination among regulators, organizations, developers, platform operators, and users, as well as organizational capacity for risk assessment, documentation, monitoring, human review, and remediation [11]. Indonesia therefore provides an important institutional context for considering how international AI governance principles can be operationalized within an emerging digital economy. However, this study treats Indonesia as a regulatory and institutional context rather than empirically measuring organizational compliance. Accordingly, this study examines the legal foundations and governance mechanisms necessary to ensure that AI adoption in digital business remains innovative, accountable, transparent, human-centric, risk-sensitive, and consistent with fundamental rights. It synthesizes existing legal and governance instruments into an integrated framework that defines stakeholder responsibilities, establishes transparency and explainability requirements, applies proportional risk-based compliance, and maintains meaningful human oversight throughout the AI lifecycle [12]. The framework provides a conceptual basis for regulators and digital businesses to translate responsible AI principles into organizational policies, compliance procedures, monitoring

mechanisms, and decision-making processes, thereby connecting technological innovation with legal certainty, stakeholder protection, institutional accountability, and responsible digital development.

Figure 1. Contribution of AI Legal Governance to the Sustainable Development Goals

Figure 1 illustrates the contribution of this research to the Sustainable Development Goals (SDGs), particularly SDG 9 on Industry, Innovation and Infrastructure and SDG 16 on Peace, Justice and Strong Institutions. The development of responsible AI in digital business supports sustainable digital transformation by integrating Legal Accountability, Transparency and Explainability, Risk-Based Compliance, and Human-Centric Oversight throughout the AI lifecycle [13]. These governance dimensions contribute to sustainability in three interconnected ways. First, they support social sustainability by protecting fundamental rights, privacy, fairness, human dignity, and meaningful opportunities for review and redress in AI-supported decision-making. Second, they strengthen institutional sustainability by establishing clear responsibilities, traceability, compliance procedures, human oversight, and governance mechanisms for managing emerging technological risks over time. Third, risk-based and lifecycle-oriented governance promotes more responsible technological deployment by encouraging organizations to assess the necessity, potential impacts, and risks associated with AI systems rather than pursuing technological adoption solely for efficiency or competitiveness [14]. Accordingly, the proposed integrated legal framework connects technological innovation with stakeholder protection, institutional accountability, and responsible digital development, thereby supporting inclusive and sustainable digital transformation consistent with human rights, legal certainty, and the rule of law.

2. LITERATURE REVIEW

2.1. Responsible Artificial Intelligence and Legal Governance

The rapid adoption of AI in digital business has shifted attention from technological capabilities toward responsible development, deployment, and governance [15]. Recent literature conceptualizes responsible AI as a multidisciplinary approach that integrates legal, ethical, organizational, and technical safeguards to promote human rights, fairness, transparency, safety, and accountability. The OECD AI Principles, updated in 2024, emphasize human agency and oversight, transparency and explainability, robustness, security, safety, accountability, traceability, and risk management throughout the AI lifecycle. Similarly, UNESCO emphasizes responsibility, accountability, transparency, privacy, fairness, non-discrimination, and human oversight as essential elements of human-centered AI governance [16]. NIST's (AI RMF 1.0) complements these normative principles by providing an operational approach to identifying and managing AI risks across design, development, deployment, and evaluation, further supported by its 2024 Generative AI Profile [17]. Taken together, these developments indicate a transition from principle-based AI ethics toward lifecycle-based governance, in which responsible AI principles are translated into organizational responsibilities, risk controls, documentation,

monitoring, and remedial mechanisms. This approach is particularly important for digital businesses because legal and social risks may arise not only from AI outputs but also from data practices, inadequate testing, insufficient human oversight, discriminatory model behavior, cybersecurity vulnerabilities, and failures to monitor deployed systems.

2.2. Legal Accountability, Transparency, and Explainability in AI Decision-Making

Legal accountability is a central challenge in AI governance because AI-supported decisions may involve multiple actors, including developers, technology providers, deployers, business users, and data-related actors. The distribution of responsibilities among these actors can create accountability gaps when AI systems produce discriminatory, inaccurate, unsafe, or otherwise harmful outcomes. The 2024 OECD AI Principles address this challenge by linking accountability with the traceability of datasets, processes, and decisions throughout the AI lifecycle [18]. Transparency and explainability are equally important because affected individuals may require meaningful information about how AI contributes to a prediction, recommendation, or decision and, where appropriate, the ability to challenge adverse outcomes. UNESCO similarly emphasizes auditability, traceability, oversight, impact assessment, due diligence, enforcement, and redress as essential elements of responsible AI governance [19]. From a legal perspective, explainability should therefore function not only as a technical mechanism for interpreting AI models but also as a means of supporting procedural fairness, contestability, and accountability. NIST's AI Risk Management Framework (AI RMF) further connects accountability and transparency with explainability, privacy, and fairness as interrelated characteristics of trustworthy AI, while its 2024 Generative AI Profile highlights the need for governance mechanisms to evolve in response to emerging AI risks [20]. Accordingly, effective AI governance requires clearly allocated responsibilities, appropriate documentation and traceability, meaningful transparency, human review of consequential decisions, and accessible mechanisms for complaint, correction, and remedy.

2.3. Risk-Based Regulation and AI Compliance in Digital Business

Risk-based governance has become a significant approach in contemporary AI regulation because AI applications differ in their potential levels and types of harm. Rather than imposing identical obligations on all AI systems, emerging regulatory approaches differentiate requirements according to the risks and impacts associated with particular applications. The European Union AI Act, Regulation (EU) 2024/1689, provides a prominent example by establishing risk-based requirements covering prohibited practices, high-risk systems, transparency, governance, and enforcement [21]. This regulatory approach is complemented by organizational risk-management frameworks, as the NIST AI Risk Management Framework (AI RMF) 1.0 provides a voluntary structure for identifying, assessing, and managing AI risks, while its Generative AI Profile addresses risks specific to generative AI systems [22]. The OECD AI Principles similarly emphasize systematic risk management throughout the AI lifecycle, including mechanisms to override, repair, or safely decommission systems that generate undue harm. These developments indicate that AI compliance should be understood as a continuous governance process rather than a one-time assessment before deployment. This process involves risk identification, impact assessment, validation, documentation, monitoring, human oversight, incident response, and periodic review [23]. For digital businesses, this lifecycle approach enables regulatory requirements to be translated into proportionate organizational controls that can adapt to changes in AI models, data, applications, and operating environments.

2.4. Human-Centric AI Governance and the Research Gap

Human-centric governance provides a normative foundation for ensuring that AI serves human interests rather than treating technological efficiency as the sole measure of successful implementation. UNESCO emphasizes human responsibility, accountability, human dignity, and human oversight, while the OECD stresses human agency, oversight, transparency, accountability, and the ability to challenge AI-supported decisions that adversely affect individuals [24]. NIST complements these principles by translating trustworthy AI principles into organizational risk-management practices across the AI lifecycle and addressing emerging risks through its Generative AI Profile [25]. However, the literature remains fragmented in connecting these normative principles with legal accountability, risk-based compliance, transparency, and organizational governance in digital business. Existing approaches tend to emphasize ethical principles, regulatory requirements, or technical risk management separately, whereas digital businesses require an integrated governance structure that connects these dimensions throughout the AI lifecycle [26]. This study addresses this gap by positioning

responsible AI governance as a techno-legal framework in which legal obligations are translated into organizational processes and technical safeguards through four interconnected dimensions: Legal Accountability, Transparency and Explainability, Risk-Based Compliance, and Human-Centric Oversight. The integration of these dimensions provides a conceptual basis for aligning AI-driven innovation with legal certainty, fundamental rights, organizational accountability, and sustainable digital business development.

Table 1. Comparison of Contemporary Responsible AI Governance Frameworks

Framework	Year	Main Orientation	Key Governance Principles	Relevance to Digital Business
OECD AI Principles	2024	International AI governance	Human oversight, transparency, safety, accountability, traceability, and risk management	Supports responsible AI adoption and cross-border governance
NIST AI RMF	2023	Organizational risk management	Trustworthiness, risk identification, measurement, management, and governance	Provides practical mechanisms for managing AI risks
NIST Generative AI Profile	2024	Generative AI risk governance	Lifecycle risk management, testing, monitoring, and mitigation	Addresses emerging risks from generative AI applications
UNESCO AI Ethics Framework	2022/2023	Human-rights-centered governance	Human dignity, fairness, privacy, transparency, accountability, and human oversight	Establishes normative safeguards for human-centered AI
EU AI Act	2024	Binding risk-based regulation	Risk classification, transparency, obligations, governance, and enforcement	Provides enforceable compliance requirements for AI providers and deployers

Table 1 demonstrates that contemporary AI governance frameworks share fundamental principles, particularly accountability, transparency, human oversight, safety, and risk management, but differ in their regulatory status and implementation functions. The OECD and UNESCO frameworks primarily provide normative principles for trustworthy and human-centered AI, while NIST provides operational mechanisms for organizational risk management, and the EU AI Act establishes legally enforceable, risk-based requirements [27]. This comparison indicates that no single framework fully connects legal obligations with the organizational and operational requirements of digital businesses. The literature therefore supports an integrated approach that combines legal accountability, transparency and explainability, risk-based compliance, and human-centric oversight throughout the AI lifecycle [28]. This integration constitutes the conceptual basis of the present study and distinguishes the proposed framework from approaches that address responsible AI primarily from an ethical, technical, or regulatory perspective.

3. RESEARCH METHOD

3.1. Research Design

This study employs a normative juridical research method with a qualitative and conceptual approach to examine legal frameworks for responsible AI in digital business [29]. The normative juridical approach focuses on legal norms, regulatory principles, governance standards, and institutional responsibilities rather than collecting primary empirical data from organizations or respondents. The study examines how existing legal and governance instruments address accountability, transparency, risk management, human oversight, and the protection of fundamental rights in AI-enabled business environments. A comparative legal approach is also applied to identify similarities, differences, strengths, limitations, and regulatory gaps among contemporary AI governance frameworks [30]. The analysis then synthesizes these findings into an integrated conceptual framework that connects legal requirements with organizational governance mechanisms throughout the AI lifecycle. Accordingly, the study provides a normative and conceptual basis for responsible AI governance

rather than an empirical assessment of organizational compliance or the practical effectiveness of the proposed framework.

Figure 2. Methodological Framework for Developing an Integrated Legal Framework for Responsible AI

Figure 2 illustrates the methodological sequence used to develop the integrated legal framework for responsible AI in digital business. The research begins by identifying legal and governance problems associated with AI adoption, followed by a normative literature review, regulatory mapping, and comparative legal analysis. The findings are then synthesized into four core governance dimensions: Legal Accountability, Transparency and Explainability, Risk-Based Compliance, and Human-Centric Oversight [31]. The final stage assesses the conceptual consistency and potential practical relevance of these dimensions to develop an integrated framework that connects responsible AI principles with legal and organizational governance requirements throughout the AI lifecycle.

3.2. Research Materials and Data Sources

The research relies primarily on secondary legal and academic materials, categorized into primary legal materials, secondary legal materials, and supporting materials [32]. Primary legal materials consist of formal regulations, international legal instruments, and authoritative AI governance frameworks used to identify applicable legal principles and regulatory requirements. Secondary materials include peer-reviewed journal articles, academic books, conference papers, and scholarly studies addressing responsible AI, AI governance, digital business, algorithmic accountability, and technology regulation [33]. Supporting materials comprise institutional reports, policy documents, and relevant technical governance publications that provide additional context on regulatory developments and implementation challenges. Literature published primarily between 2023 and 2026 is prioritized to reflect recent developments in AI regulation and governance while maintaining relevance to the study's normative and comparative analysis. These materials are systematically synthesized to identify regulatory gaps and establish the legal and conceptual foundations for the proposed integrated framework for responsible AI governance in digital business.

Table 2 presents the categories of materials used to construct the legal and conceptual analysis. Primary legal materials provide the formal regulatory foundation, while international AI governance frameworks provide principles and standards for responsible AI governance. Academic literature supports the development of theoretical arguments and the identification of research gaps, while policy reports and other supporting materials provide contemporary context for AI governance and digital business [34]. The combination of these

Table 2. Research Materials and Analytical Sources

Category	Research Materials	Main Purpose
Primary Legal Materials	EU AI Act, data protection regulations, and relevant AI-related legal instruments	Identify legal obligations and regulatory requirements
International Governance Frameworks	OECD AI Principles, UNESCO AI Ethics Recommendation, and NIST AI RMF	Identify responsible AI governance principles
Academic Literature	Peer-reviewed journals, conference proceedings, and academic books	Establish theoretical and conceptual foundations
Policy and Institutional Reports	Reports from international organizations and regulatory institutions	Identify emerging policy developments and implementation challenges
Supporting Materials	Legal commentaries and relevant digital governance studies	Strengthen interpretation and contextual analysis

materials enables the study to examine responsible AI from complementary legal, conceptual, and organizational perspectives. The materials are analyzed comparatively to identify common principles, regulatory differences, and governance requirements relevant to responsible AI in digital business. This comparative assessment supports the synthesis of legal obligations and governance principles into the four dimensions of the proposed framework: Legal Accountability, Transparency and Explainability, Risk-Based Compliance, and Human-Centric Oversight. The resulting synthesis provides a structured basis for examining how these dimensions can be applied across the AI lifecycle and translated into organizational governance mechanisms.

3.3. Data Collection Procedure

Data collection is conducted through structured document analysis and a literature review. Relevant materials are identified using predetermined keywords, including responsible, AI legal framework, AI governance, AI accountability, algorithmic transparency, AI risk management, human oversight, and digital business regulation [35]. The collected materials are screened based on relevance, publication period, academic credibility, and their direct relationship to the research objectives. Regulatory and governance documents are examined to identify provisions and principles concerning AI risk classification, transparency, accountability, human oversight, data protection, and enforcement, while academic sources are reviewed to examine how these concepts have been interpreted and operationalized in previous research [36]. The selected materials are then organized into thematic categories to support systematic comparison, identification of regulatory gaps, and synthesis of the four governance dimensions developed in the study: Legal Accountability, Transparency and Explainability, Risk-Based Compliance, and Human-Centric Oversight.

3.4. Legal and Comparative Analysis

The analytical process combines qualitative normative analysis with comparative legal analysis. First, the study interprets the legal principles and governance requirements contained in selected regulatory instruments and authoritative AI governance frameworks [37]. Second, these requirements are compared across key analytical dimensions, including accountability, transparency and explainability, risk management, human oversight, data protection, fairness, and enforcement. Third, similarities and differences among the selected frameworks are identified to determine areas of regulatory convergence and divergence. Finally, regulatory and governance gaps are examined to assess where existing approaches may be insufficient to address the characteristics and risks of AI-enabled digital business [38]. This process moves the analysis beyond a descriptive legal review toward the conceptual synthesis of an integrated AI governance framework.

3.5. Framework Development

The framework development stage synthesizes the findings from the normative and comparative analyses into four interconnected dimensions: Legal Accountability, Transparency and Explainability, Risk-Based Compliance, and Human-Centric Oversight [39]. Legal accountability defines responsibilities among AI developers, providers, deployers, and business organizations, while transparency and explainability establish requirements for documenting and communicating AI-supported decisions. Risk-based compliance connects

governance and regulatory obligations with the potential impact and level of risk associated with AI systems, while human-centric oversight ensures meaningful human control over consequential AI-supported decisions and appropriate opportunities for review and redress [40]. These dimensions are integrated throughout the AI lifecycle to provide a coherent conceptual framework that connects legal requirements with organizational governance mechanisms for responsible AI adoption in digital business.

3.6. Research Quality and Conceptual Assessment

To strengthen the quality of the conceptual framework, the research applies source triangulation and consistency analysis. Source triangulation is conducted by comparing legal instruments, international AI governance frameworks, and peer-reviewed academic literature rather than relying on a single source or regulatory approach. Consistency analysis examines whether the proposed framework aligns with established principles of accountability, transparency, risk management, human rights, and human oversight [41]. The framework is further assessed in terms of its legal relevance, conceptual consistency, and potential practical applicability to AI-enabled digital business. This process helps identify areas of convergence and differences among existing legal and governance approaches and supports the integration of complementary principles into a coherent framework. It also ensures that each proposed governance dimension is connected to relevant legal responsibilities and organizational mechanisms throughout the AI lifecycle. However, the assessment remains conceptual and does not establish empirical effectiveness, which should be examined through future organizational and sector-specific studies. This assessment strengthens the coherence of the proposed framework while recognizing that its effectiveness in organizational practice requires further empirical examination.

4. RESULTS AND DISCUSSION

4.1. Existing Legal and Governance Frameworks for Responsible AI

The analysis indicates that contemporary responsible AI governance is shaped by several complementary frameworks, particularly the EU AI Act, OECD AI Principles, UNESCO AI Ethics Recommendation, and NIST AI Risk Management Framework [42]. Across these frameworks, the analysis identifies recurring principles of accountability, transparency, risk management, human oversight, fairness, privacy, and security, although their legal status, institutional scope, and implementation mechanisms differ. The EU AI Act provides a binding, risk-based regulatory structure, while the OECD and UNESCO frameworks establish broader normative principles for trustworthy and human-centered AI, and NIST provides operational mechanisms for organizational risk management [43]. The comparison therefore indicates that these frameworks are complementary but do not provide a single integrated structure connecting enforceable legal responsibilities with organizational and operational controls throughout the AI lifecycle. This finding supports the development of an integrated governance framework that combines Legal Accountability, Transparency and Explainability, Risk-Based Compliance, and Human-Centric Oversight for responsible AI adoption in digital business.

4.2. Legal Accountability, Transparency, and Human Oversight

The findings identify Legal Accountability, Transparency and Explainability, and Human-Centric Oversight as interconnected requirements for responsible AI in digital business. Accountability should be allocated according to the roles, responsibilities, and degree of control exercised by developers, providers, deployers, and business users rather than assigned to a single actor [44]. It operates across three stages: preventive measures through responsibility allocation, risk assessment, and documentation; monitoring measures through ongoing oversight, traceability, and performance review; and corrective measures through human intervention, system modification or discontinuation, complaint mechanisms, and appropriate redress. Transparency and explainability should provide stakeholders with meaningful information about the purpose, data, limitations, and role of AI in decision-making, particularly when automated decisions may significantly affect individuals. Human oversight should ensure that authorized personnel can review, intervene in, override, or discontinue AI-supported decisions when necessary [45]. These requirements should be integrated into organizational policies and governance procedures throughout the AI lifecycle, from system design and development to deployment, monitoring, evaluation, and remediation. Their integration can also strengthen the alignment between legal obligations, internal controls, and operational decision-making, particularly in digital businesses that rely on complex or high-impact AI systems. This integrated approach enables organizations to respond to emerging AI risks while maintaining accountability, transparency, and meaningful human control. These findings indicate that responsible AI governance requires interconnected responsibility structures, meaningful transparency,

and continuous human oversight to reduce the legal, ethical, and operational risks associated with automated decision-making.

Table 3. Findings from the Comparative Legal Analysis

Governance Dimension	Main Finding	Governance Response
Legal Accountability	Responsibility is distributed among AI actors	Define roles and responsibilities
Transparency & Explainability	AI decisions may be difficult to understand	Documentation and meaningful disclosure
Risk-Based Compliance	AI systems have different levels of risk	Apply proportional regulatory controls
Human Oversight	Automated decisions may create accountability gaps	Human review and intervention
Data Protection & Fairness	AI may create privacy and discrimination risks	Data governance and bias monitoring
Enforcement & Redress	Harmful AI decisions require remedies	Complaint, review, and remediation mechanisms

Table 3 summarizes the main findings of the comparative legal analysis and demonstrates that responsible AI requires interconnected governance mechanisms throughout the AI lifecycle. Legal accountability establishes the allocation of responsibilities, transparency and explainability support understanding and traceability, risk-based compliance determines proportionate governance controls, and human-centric oversight provides mechanisms for review, intervention, and correction [46]. Data protection, fairness, enforcement, and redress further strengthen the protection of individuals affected by AI-supported decisions. Together, these mechanisms provide the legal and organizational foundation for responsible AI governance in digital business. Their integration enables organizations to translate general legal and ethical principles into concrete governance practices, including responsibility allocation, risk assessment, documentation, monitoring, and corrective action. The comparative findings also show that these mechanisms should be applied proportionately according to the potential risks and impacts of different AI applications. This integrated approach can strengthen accountability and stakeholder protection while allowing digital businesses to pursue technological innovation within appropriate legal and organizational safeguards.

4.3. Integrated Legal Framework for Responsible AI in Digital Business

Based on the normative and comparative analyses, this study develops an Integrated Legal Framework for Responsible AI in Digital Business consisting of four interconnected pillars: Legal Accountability, Transparency and Explainability, Risk-Based Compliance, and Human-Centric Oversight. Legal Accountability establishes clear responsibilities among AI developers, providers, deployers, and business users throughout the AI lifecycle, while Transparency and Explainability support documentation, traceability, and meaningful understanding of AI-supported processes [47]. Risk-Based Compliance links regulatory and organizational controls to the potential level and severity of AI-related harm, enabling proportionate governance requirements, while Human-Centric Oversight ensures that authorized personnel retain meaningful authority to review, intervene in, override, or discontinue consequential AI-supported decisions. These pillars operate from design and development through deployment, monitoring, evaluation, and remediation, thereby connecting preventive, monitoring, and corrective governance mechanisms [48]. Collectively, the framework provides a conceptual basis for translating responsible AI principles into legal and organizational controls that support fairness, privacy, safety, accountability, trust, and sustainable digital business development.

Figure 3. Integrated Legal Framework for Responsible AI in Digital Business

Figure 3 illustrates the integrated framework developed from the research findings. The four pillars Legal Accountability, Transparency and Explainability, Risk-Based Compliance, and Human-Centric Oversight operate together throughout the AI lifecycle, connecting responsibility allocation, transparency and traceability, proportionate risk controls, and meaningful human intervention. The framework incorporates preventive, monitoring, and corrective governance mechanisms across the AI lifecycle, from AI design and development through deployment, evaluation, and remediation [49]. Their integration provides a structured conceptual foundation for promoting fair, safe, transparent, trustworthy, and legally compliant AI applications while supporting responsible and sustainable digital business development. The framework also enables organizations to align legal obligations with internal governance processes, ensuring that responsibility and oversight remain clearly defined throughout the AI lifecycle. By integrating these pillars into organizational policies and operational controls, digital businesses can strengthen risk management, stakeholder protection, and accountability while maintaining opportunities for responsible innovation.

4.4. Implications of the Proposed Framework

The findings indicate that the proposed framework can bridge the gap between AI regulation and practical digital business governance by translating responsible AI principles into organizational responsibilities, compliance procedures, and operational controls. Digital businesses can apply the framework by allocating responsibilities among relevant AI actors, conducting risk and impact assessments, establishing documentation and transparency procedures, implementing human review and intervention mechanisms, and developing processes for monitoring, incident response, correction, and redress [50]. The risk-based structure enables governance requirements to remain proportionate to the potential impact of different AI applications, thereby avoiding a uniform compliance approach that could unnecessarily constrain lower-risk innovation while maintaining stronger safeguards for higher-risk systems. At the institutional level, regulators can use the framework to support proportional oversight and accountability, while organizations and AI developers can incorporate its principles into internal policies, risk management procedures, and lifecycle governance. Overall, the framework provides a conceptual basis for AI governance that is accountable, transparent, risk-sensitive, human-centered, and applicable throughout the AI lifecycle, thereby supporting responsible technological innovation while maintaining legal certainty, stakeholder protection, and sustainable digital business development.

5. MANAGERIAL IMPLICATIONS

The findings provide important managerial implications for digital businesses adopting AI. Managers should integrate responsible AI governance into existing corporate risk management, compliance, data governance, and decision-making processes rather than treating AI regulation as a separate technical issue. Organizations should clearly allocate responsibilities among AI developers, technology providers, deployers, business users, and decision-makers while establishing procedures for risk assessment, documentation, transparency, human review, continuous monitoring, incident response, and corrective action. A risk-based approach should be applied so that higher-impact AI applications receive stronger controls, auditing, and human oversight, while lower-risk applications are subject to proportionate requirements that do not unnecessarily constrain innovation. Organizations should also establish AI governance policies and provide regular employee training to ensure that personnel understand legal obligations, algorithmic risks, privacy requirements, and appropriate intervention procedures. By embedding these mechanisms throughout the AI lifecycle, digital businesses can strengthen accountability and stakeholder trust, reduce legal and operational risks, and support responsible innovation in AI-enabled business processes.

6. CONCLUSION

This study concludes that responsible AI in digital business requires an integrated legal governance approach that connects technological innovation with accountability, transparency, risk management, and human oversight. Based on normative juridical and comparative legal analysis, the study identifies four interconnected dimensions. Legal Accountability, Transparency and Explainability, Risk-Based Compliance, and Human-Centric Oversight. The comparative findings indicate that existing regulatory and governance instruments provide important but differentiated foundations, while differences in their legal status and implementation mechanisms create challenges for organizations operating across digital and regulatory environments. The proposed framework addresses this gap by connecting legal responsibilities with organizational controls throughout the AI lifecycle, including risk assessment, documentation, monitoring, human intervention, and corrective mechanisms. Accordingly, the framework provides a conceptual basis for responsible and sustainable digital business governance while supporting the protection of fundamental rights, legal certainty, accountability, and stakeholder trust.

The study answers the research question by demonstrating that an effective legal framework for responsible AI should allocate clear responsibilities among AI developers, providers, deployers, business users, and other relevant stakeholders; establish meaningful transparency and explainability; apply proportionate compliance requirements according to the potential risks and impacts of AI systems; and maintain meaningful human oversight over consequential AI-supported decisions. These interconnected mechanisms provide a governance structure for addressing risks involving privacy, discrimination, algorithmic opacity, accountability gaps, and harmful automated decisions while ensuring that regulatory controls remain proportionate to technological risks. The framework therefore contributes to AI governance by connecting normative legal principles with organizational and lifecycle-based governance mechanisms rather than treating responsible AI solely as an ethical, technical, or compliance issue.

This study is subject to several limitations. As a normative and conceptual study, it does not empirically test the proposed framework within specific digital businesses or measure its effectiveness using organizational or user-level data. In addition, its comparative analysis cannot fully capture the institutional and sector-specific differences across all jurisdictions. The rapid development of emerging AI technologies may also require continued refinement of the proposed governance dimensions as new risks and regulatory requirements emerge. Future research should therefore empirically examine the framework through case studies, expert interviews, surveys, or organizational assessments involving digital businesses in different operational and regulatory contexts. Further research may compare implementation across jurisdictions, develop measurable indicators for the four framework dimensions, and investigate how responsible AI governance influences organizational compliance, innovation, stakeholder trust, and sustainable digital transformation, particularly in relation to emerging technologies such as generative and autonomous AI systems.

7. DECLARATIONS

7.1. About Authors

Adam Faturahman (AF) https://orcid.org/0000-0001-9727-9092

Sherli Triandari (ST) https://orcid.org/0009-0007-9323-4373

Ramzi Zainum Ikhsan (RI) https://orcid.org/0009-0005-2253-6476

Aswadi Jaya (AJ) https://orcid.org/0000-0001-5706-0977

Emilyani (EE) https://orcid.org/0009-0001-3860-3814

7.2. Author Contributions

Conceptualization: AF; Methodology: ST; Software: RI; Validation: AJ, EE ; Formal Analysis: AF and ST; Investigation: RI; Resources: AJ; Data Curation: EE and AF; Writing Original Draft Preparation: AF and ST; Writing Review and Editing: RI, AJ and EE; Visualization: AF; All authors, AF, ST, RI, AJ, and EE, have read and agreed to the published version of the manuscript.

7.3. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

7.4. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

7.5. Institutional Review Board Statement

Not applicable.

7.6. Informed Consent Statement

Not applicable.

7.7. Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

[1] C. Novelli, M. Taddeo, and L. Floridi, "Accountability in artificial intelligence: what it is and how it works," *Ai & Society*, vol. 39, no. 4, pp. 1871–1882, 2024.

[2] K. M. Richmond, S. M. Muddamsetty, T. Gammeltoft-Hansen, H. P. Olsen, and T. B. Moeslund, "Explainable ai and law: An evidential survey," *Digital Society*, vol. 3, no. 1, p. 1, 2024.

[3] O. Ferli, N. A. Achsani, T. Andati, and Z. Asikin, "Sustainable business innovation in indonesian firms esg disclosure profitability and greenwashing," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 8, no. 2, pp. 405–419, 2026.

[4] L. d. B. Aranda, C. Custis, O. J. Erdélyi, L. C. C. Galindo, and R. Rozenberg, "Advancing accountability in ai: Governing and managing risks throughout the lifecycle for trustworthy ai," *OECD Digital Economy Papers, No. 349*, 2023.

[5] E. Tabassi, "Artificial intelligence risk management framework (ai rmf 1.0). nist ai 100-1. gaithersburg, md: National institute of standards and technology," 2023.

[6] U. Rahardja, M. T. D. S. Putri, N. Septiani, F. Amelia, A. Avandi, and R. Evans, "Human centered legal governance for autonomous ai in digital societies," *Legal Autonomous Web-based Governance (LAW)*, vol. 1, no. 1, pp. 29–41, 2026.

[7] F. Filippucci, P. Gal, K. Laengle, and M. Schief, "Macroeconomic productivity gains from artificial intelligence in g7 economies," *OECD Artificial Intelligence Papers*, 2025.

[8] M. A. T. Makki, "Artificial intelligence between education, law, and ethics: A foresight study in emerging societies," , vol. 6, no. 1, pp. 211–221, 2026.

[9] C. Lukita, A. K. Chandra, R. Fahrudin, N. M. Agatha, and D. P. Suci, "Maturity level measurement model of msmes for sustainable economic growth," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 8, no. 2, pp. 434–442, 2026.

[10] Y. Mochizuki, E. Bruillard, and A. Bryan, "The ethics of ai or techno-solutionism? unesco's policy guidance on ai in education," *British Journal of Sociology of Education*, pp. 1–22, 2025.
[11] M. Lognoul, "Regulation (eu) 2024/1689 laying down harmonised rules on artificial intelligence (artificial intelligence act–ai act)," *Revue du Droit des Technologies de l'information*, no. 3-4, pp. 145–189, 2025.
[12] A. Rizky, U. Rahardja, M. Muhtarom, D. N. Ramadhan, S. Triandari, and R. F. Terizla, "Responsible ai governance in decentralized web systems," *Legal Autonomous Web-based Governance (LAW)*, vol. 1, no. 1, pp. 123–133, 2026.
[13] E. Santoso *et al.*, "Opportunities and challenges: e-commerce in indonesia from a legal perspective," *Jurnal Penelitian Hukum De Jure*, vol. 22, no. 3, pp. 395–410, 2022.
[14] E. Commission, "Ai act enters into force," *European Commission*, 2024.
[15] S. D. Retnandari, K. Khaeroman, A. T. Winarni, and W. Busse, "Digital innovation and technology driven evaluation of maritime safety systems performance in indonesia," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 8, no. 2, pp. 551–564, 2026.
[16] D. B. D. Badruzaman, "Legal review of consumer protection in e-commerce transactions in indonesia," *Equality: Journal of Law and Justice*, vol. 2, no. 1, pp. 89–102, 2025.
[17] N. AI, "Artificial intelligence risk management framework: Generative artificial intelligence profile," *NIST Trustworthy and Responsible AI Gaithersburg, MD, USA*, 2024.
[18] U. Rahardja and Q. Aini, "Enhancing blockchain security through smart contract vulnerability classification using bilstm and attention mechanism," *Journal of Current Research in Blockchain*, vol. 3, no. 1, pp. 28–45, 2026.
[19] M. S. Mansyah *et al.*, "Legal protection for victims of fraud in online buying and selling transactions from the perspective of islamic law," *Justice Law Review*, vol. 1, no. 1, pp. 37–65, 2025.
[20] S. Widhaningroem and Y. Widowaty, "Juridical study on investigation of fraud crime cases in e-commerce in indonesia," *LAW & PASS: International Journal of Law, Public Administration and Social Studies*, vol. 1, no. 2, pp. 150–161, 2024.
[21] A. Ruangkanjanases, A. Khan, O. Sivarak, U. Rahardja, and S.-C. Chen, "Modeling the consumers' flow experience in e-commerce: The integration of ecm and tam with the antecedents of flow experience," *Sage Open*, vol. 14, no. 2, p. 21582440241258595, 2024.
[22] R. S. Sari, L. Ferdiles, and A. M. Rusdi, "Model of legal protection in e-commerce transactions to improve the community economy in indonesia," *Jurnal Hukum Indonesia*, vol. 3, no. 2, pp. 87–95, 2024.
[23] A. Z. A. Shami, M. Saleem, and J. Ashraf, "Cybercrime and digital evidence: Investigating the challenges and opportunities in prosecuting cybercrime and handling digital evidence," *Research Consortium Archive*, vol. 3, no. 2, pp. 401–411, 2025.
[24] I. Haryanto, Y. Yunadin, W. Setiawan, F. Agrimiandra, and D. Alam, "Legal governance of technology driven cybercrime in digital society," *Legal Autonomous Web-based Governance (LAW)*, vol. 1, no. 2, pp. 141–154, 2026.
[25] A. Batool, D. Zowghi, and M. Bano, "Ai governance: a systematic literature review," *AI and Ethics*, vol. 5, no. 3, pp. 3265–3279, 2025.
[26] E. M. Ali, F. Dirgantara, and D. Darmawan, "Legal protection of consumers in online transactions: A case study of online fraud in indonesia," *International Journal of Service Science, Management, Engineering, and Technology*, vol. 6, no. 3, pp. 27–38, 2024.
[27] M. Nurkanti, U. Rahardja, M. Lubis, and A. Shukri, "Deep learning-based biology learning with ethnopedagogy and local wisdom to support sustainable development goals," *Jurnal Pendidikan IPA Indonesia*, vol. 15, no. 1, pp. 103–111, 2026.
[28] E. Saragih, M. A. Sahlepi, and M. A. Siregar, "Implementation of the law against fraud crimes in e-commerce-based electronic transactions," in *Proceedings of International Conference on Islamic Community Studies*, 2025, pp. 360–370.
[29] E. Papagiannidis, P. Mikalef, and K. Conboy, "Responsible artificial intelligence governance: A review and research framework," *The Journal of Strategic Information Systems*, vol. 34, no. 2, p. 101885, 2025.
[30] A. H. Rambe, I. Kumalasari *et al.*, "Juridical analysis of legal protection for consumers in e-commerce transactions in indonesia," *IJECK (International Journal Of Economy, Computer, Law, Management And Communication)*, vol. 2, no. 2, pp. 34–42, 2024.
[31] U. Rahardja, M. L. Daeli, S. A. Anjani, L. Pasha, A. Asri, and H. Zainarthu, "Enhancing trust and efficiency in e-commerce transactions through blockchain ai synergy," *ADI Journal on Recent Innovation*,

vol. 7, no. 1, pp. 25–37, 2025.

[32] R. Hanifiyah, "Law enforcement of online business fraud crimes according to positive law and islamic law (study on court decision number 975/pid. sus/2018/pn mks)," B.S. thesis, Fakultas Syariah dan Hukum Universitas Islam Negeri Syarif Hidayatullah Jakarta, 2022.

[33] A. Haidar, "An integrative theoretical framework for responsible artificial intelligence," *International Journal of Digital Strategy, Governance, and Business Transformation (IJDSGBT)*, vol. 13, no. 1, pp. 1–23, 2024.

[34] N. Lutfiani, M. A. Komara, S. A. Anjani, S. Solahudin, N. Rangi, and A. C. Kiboy, "Juridical analysis of legal protection against e-commerce fraud in indonesia," *Legal Autonomous Web-based Governance (LAW)*, vol. 1, no. 1, pp. 109–122, 2026.

[35] I. D. Kurniawan, P. Suwadi, and J. G. S. Soehartono, "An analysis of economic criminal actions of e-money theft case in e-commerce in indonesia," in *1st INTERNATIONAL CONFERENCE ON LAW, BUSINESS, AND GOOD GOVERNANCE 2024*, 2024, p. 1134.

[36] S. D. Andini and R. Nilasari, "Juridical analysis of legal protection against disadvantaged sellers in e-commerce transactions on the tokopedia online shopping site," *Proceedings Series on Social Sciences & Humanities*, vol. 14, pp. 284–289, 2023.

[37] L.-F. Spulbar, "Legal frameworks for ai-driven markets and their challenges and opportunities in the digital economy," *Revista de Ştiinţe Politice. Revue des Sciences Politiques*, no. 86, pp. 288–304, 2025.

[38] S. Widada, S. T. S. Alfian *et al.*, "Utilizing blockchain for electronic wellbeing records," *Blockchain Frontier Technology*, vol. 1, no. 2, pp. 11–22, 2022.

[39] J. Kaur, "Responsible artificial intelligence (ai) governance: ethical frameworks for business decision-making," in *Ethical quandaries in business practices: exploring morality and social responsibility*. IGI Global Scientific Publishing, 2024, pp. 337–368.

[40] T. Hudima, A. Soshnykov, and V. Dovhan, "Law into code: Eu regulation of digital accountability mechanisms for responsible business conduct," *European Journal of Sustainable Development*, vol. 15, no. 1, pp. 844–844, 2026.

[41] F. Agrimiandra, M. A. Mahdafiqia, D. P. A. Sakti, and D. Alam, "Legal governance of state financial losses in corruption cases," *Legal Autonomous Web-based Governance (LAW)*, vol. 1, no. 2, pp. 155–168, 2026.

[42] D. Marsela, Y. Yudhistira, and B. Fawaid, "Legal protection of consumers in online business: a criminal law perspective in handling fraud and identity theft," *Research Horizon*, vol. 4, no. 3, pp. 99–106, 2024.

[43] N. Vanu, M. Hasan, S. Akter, and M. Faruque, "Legal and ethical frameworks for regulating artificial intelligence in business," *Journal of Business Venturing, AI and Data Analytics*, vol. 1, no. 10.63471, 2024.

[44] J. Bahar, M. A. Prayoga, A. Alamsyah, and D. Alam, "Justice based consumer dispute mediation in the digital economy," *Legal Autonomous Web-based Governance (LAW)*, vol. 1, no. 2, pp. 169–181, 2026.

[45] Z. Tóth and M. Blut, "Ethical compass: The need for corporate digital responsibility in the use of artificial intelligence in financial services," *Organizational Dynamics*, vol. 53, no. 2, p. 101041, 2024.

[46] T. S. Hudima and A. O. Soshnykov, "Social responsibility of business in the context of digitalization and artificial intelligence: The legal dimension," *JE Eur. L.*, p. 7, 2025.

[47] P. Paroli, M. Muhtarom, M. M. Siahaan, D. Derlina, K. Moyo *et al.*, "Smart contract based data strategy for startup growth in digital business systems," *Journal of Computer Science and Technology Application*, vol. 3, no. 2, pp. 117–129, 2026.

[48] A. Haidar, "Responsible artificial intelligence: designing frameworks for ethical, sustainable, and risk-aware practices," Ph.D. dissertation, Université Paris-Saclay, 2024.

[49] N. U. H. Wani, N. Hamza, and B. Saboori, "Legal and ethical frameworks for ai in financial services: Balancing the innovation with responsibility and effective protection," in *Green Horizons: Role of AI in Sustainable Finance*. Springer, 2025, pp. 177–196.

[50] OECD, *Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions*. Paris: OECD Publishing, 2025. [Online]. Available: https://doi.org/10.1787/795de142-en