El mohtaref journal of sports Science. Social And Human Science

Vol (11) N° 01(2026)

P 377-389

Search information

Received 24/02/2026
Accepted 24/03/2026

Printed ISSN: 2352-989X
Online ISSN: 2602-6856

Governing Artificial Intelligence in Economic Institutions: An Integrated Approach

HAMMOUDI Dalel[1*]

DJENANE Abdelhak[2]

ZAGHEZ Sara[3]

[1] mohamed khider university of BISKRA;

d.hammoudi@univ-biskra.dz

[2] mohamed khider university of BISKRA;

abdelhak_djenane@univ-biskra.dz

[3] mohamed khider university of BISKRA;

Zaghez.sara@univ-biskra.dz

ABSTRACT

This article proposes an integrated AI governance framework for economic institutions to manage the ethical, operational, and regulatory compliance risks associated with the rapid deployment of AI systems. The framework embeds responsible AI principles within existing governance, risk management, and Governance, Risk, and Compliance structures, enabling effective oversight across the AI lifecycle while addressing cross-border regulatory complexity. By offering practical tools for risk assessment, audit ability, performance monitoring, and continuous improvement, the study provides a scalable roadmap that helps institutions balance innovation, trust, and regulatory accountability in a dynamic AI environment.

Keywords; AI Governance; Economic Institutions; Responsible and Ethical AI; Operational Risk; Regulatory Compliance; GRC Frameworks; Data and Model Risk; Trustworthy AI

[*] *Corresponding author*

1. INTRODUCTION

Economic institutions play a vital role in facilitating algorithms at scale yet are exposed to potential risks arising from their deployment. Regulatory and governance frameworks around AI in economic institutions have remained limited but require urgent development. Directed by responsible AI, holistic governance frameworks for economic institutions encompass ethical, operational, and regulatory compliance considerations, as economic agents face a rapid influx of new models and data sets and remain at heightened risk from AI-related incidents.

Economic agents extensively leverage AI-based products and services across a wide array of use cases—spanning cybersecurity, accounting, recruitment, money laundering, and credit risk. The unrivalled capacity of generative AI to generate text, audio, images, and videos at unmatched speed and scale ignites commercial interest across multiple sectors, including gaming, media, and publishing. Increasing reliance on AI systems heightens exposure to operational and regulatory compliance hazards on account of the black-box nature of many models.

Governance frameworks target novel threats that need to be comprehensively addressed in parallel with ethical principles guiding the responsible deployment of AI technologies throughout the economic environment (Choung et al., 2023). Economic institutions hospitals bear significant reputational, operational, financial, and legal risks linked to multiple internal and external repositories of protected and sensitive information (Kurshan et al., 2020).

Economic institutions confront regulatory frameworks governing AI deployments and potential/already-issued regulations prohibiting discrimination, protecting individual privacy and data sovereignty, securing consumers, ensuring fairness in commercial engagements, and safeguarding fiscal stakeholders. An integrated AI governance framework empowers economic actors to remain agile and adaptive at the nexus of AI technology and economics, centring ethic, operational, and regulatory compliance considerations.

2. The Rationale for AI Governance in Economic Institutions

The need for sound governance for the use of artificial intelligence (AI) in the economic domain has grown considerably over the past few years. Economic institutions, in particular, are being challenged to devise an appropriate governance framework to oversee AI innovation in their respective markets. Governments across the world are adopting policies, laws, and regulations that require businesses to govern the use of AI systems to minimize or eliminate associated risks (Choung et al., 2023). Financial authorities, including the Bank of England, the Financial Stability Board, and the International Monetary Fund, have begun to regulate AI use in financial institutions

because a lack of governance can compromise an institution's safety and soundness, the stability of the financial system, and the treatment of customers. Regulators from sectors including education, health, and consumer products are also drawing up regulations to support safe and responsible AI deployment.

Governments and regulators do not impose these requirements lightly; the economic aftermath of the 2008 financial crisis and the current implementation of digital currencies demonstrate that unregulated innovation entails significant risks to society at large. Consequently, institutions are compelled to examine governance mechanisms for the following principal reasons. First, unregulated innovation in economic markets can adversely impact the markets. Second, scrutiny from governments and regulators tends to be more stringent for economic institutions than for those in other sectors. Third, the engagement of economic institutions generally gives rise to market-wide discussions, while AI-related commentary, exploration, and experimentation often remain proprietary and inward-looking (Kurshan et al., 2020). Such barriers to the exchange of knowledge can induce both reputational and financial harm.

Governance considerations apply to three fundamental dimensions—operational, ethical, and regulatory compliance—that collectively shape risk management. Beyond the legal and regulatory requirements that institutions are mandated to uphold, stakeholders such as boards of directors, internal audit, and corporate compliance officers exert considerable pressure. Stakeholders are thus the primary audience for an integrated framework governing economic institutions. However, institutions should also heed the need to fulfill their corresponding multilateral responsibilities.

3. Core Principles of Integrated AI Governance

AI governance encompasses the mechanisms, processes, and principles that together inform the application of AI and enforcement of associated ethical guidelines. These mechanisms are as varied as governing bodies and represent a formal and an informal agenda. Beyond formal governance by designated committees and boards within economic institutions, an informed, inter-dependent and interactive societal debate shapes regulation that sets parameters for use of AI technologies and tools. Stakeholders in economic institutions—governance bodies, leadership, middle management, front-line employees, and external overseers—seek assurance that AI usage is both consistent with applicable norms and guided by and contributes to the institution's aspirations. Aligned with and extending beyond operational risk management frameworks, governance serves to identify and address ethical issues and related operational risks arising in conjunction with extensive AI use. Given the pervasive nature of AI throughout the operating model and operating environment of economic institutions, an integrated governance framework facilitates oversight of ethical, operational, and

regulatory compliance risks across departments, lines of business, and geographical regions (Gill et al., 2022).

In the absence of robust governance frameworks and oversight systems, entrepreneurial opportunities can decline. Responsible AI management encompasses three primary forms—ethical considerations, operational risk management, and regulatory requirements—often pursued independently within organisations. Rigorous governance frameworks for responsible use and related risk mitigation are therefore essential. A uniform set of AI governance principles—accountability, fairness, transparency, robustness, privacy, and sustainability—establishes prerequisites for economic institutions to engage in responsible AI management and indicates possible avenues for such engagement (Kurshan et al., 2020).

4. Ethical Considerations and Responsible AI

To deploy AI responsibly, relevant ethical considerations must be integrated within institutions. Ethical considerations refer to beliefs about what is right and wrong that determine conduct. Values describe what is important and may include compliance, sustainability, responsibility, and others, depending on institutional strategy. Ethical guardrails establish a framework for institutions to take ethical considerations into account while operationalizing AI.

A common approach to ethical guardrails is to classify them according to ethical frameworks: deontological, consequentialist, and virtue-based. Deontology centers on adherence to rules, such as avoiding harmful applications of AI. Consequentialism emphasizes the impact of actions, such as the quality of models or inclusivity of data. In practice, most institutions conform to a deontological framework, while some consider a consequentialist perspective. A more specific classification may also prove useful in practice, with common dimensions characterized by fairness, accountability, privacy, freedom of choice, and others.

Specific processes facilitate the integration of ethical considerations into the AI lifecycle. Deploying a rigorous bias-mitigation process to detect and correct bias in training data demonstrates a commitment to fairness, while a human-centered design approach that prioritizes user needs aligns with values of responsibility and user empowerment. Systematically engaging stakeholders, including external actors, throughout the development and deployment process may further enhance ethical evaluations. Clearly defined criteria for assessing alignment with ethical guardrails enable proactive consideration and evaluation of responses to ethical risks (Choung et al., 2023).

5. Operational Risk Management in AI Systems

AI systems are adopted in operational processes to drive efficiency, cost-effectiveness, and innovation. Operational risk is defined as the risk of losses from inadequate or failed internal processes, people, or systems, or from external events (Kurshan et al., 2020). Within economic institutions, operational risks applicable to a model machine-learning system include model drift, data quality, integration within surrounding systems, manner in which the model may fail, and the potential of adversarial risk evasion attacks.

Several operational risk events concern an unacceptable change to the model behavior—model drift, corruption of the data source from which the model derives its information and continued stable integration into surrounding systems. When model drift is detected, corrective action may include retraining with most-recent and relevant historical data, extending the training set either horizontally or vertically, implementing data augmentation, using another model covering the same problem, enabling explainable-ML capabilities to uncover what influences the model, revalidating critical variables if risk exposure nudges product suitability, reverting to the previous model, or terminating the initiative. For data-corruption events, a subset of the pattern-recognition procedure (e.g., a data-visualisation tool) remains functional on time. The model accommodates only a portion of the source, yet the remainder is subject to another model. Adverse effects and changes to integrity are checked. Supplementary visualisation gauges the interdependencies between the model outputs and surrounding conditions. Tools display coverage-missing events. Surrogate models covering various product spaces deliver predictions with sufficient coverage.

Once functionality is functioning in production, enhanced monitoring identifies superposed patterns that are disruptive and liable to breach risk limits. Global monitoring graphs capture activities, usage, and dispersion. Deltas from contemporaneous time are plotted against distance measures and elapsed times. Documentation of alert-triggering specifications is undertaken to explain the activity.

A second category of operational-risk concerns relates to risk evasion. Once positioned in production, support for adversarial risk-evasion attacks remains critical. Because these models operate at their core without an understanding of the surrounding conditions, dedicated testing tools unveil potential avenues for corruption. Simulation capability at various layers provides additional coverage. Capability to conduct simulation both before and after transpose remains important. (Yan et al., 2025)

Formal, Governance, Risk and Compliance (GRC) frameworks for continuous monitoring and alerting specify oversight at the appropriate granularity for awareness and assurance. Economic institutions adopt GRC controls as part of their wider Risk and Compliance framework. The rules associated with any such GRC layer comprise either a superlayer or supergroup or remain distributed across independent components. Key

decisions require either a change to the supervisory circuitry or secure access. Ability to document alteration effected on the GRC front—across Governance, Risk and Compliance in parallel—remains important.

An extensive, monitored enterprise operates under strict control for any material or fundamental changes. Changes undergo influence assessments, security clearance and full tracing of origin, destination, and nature of consequence. GRC changes do not require initiation at an equivalent level. Operationally repeated changes demand merely supervisory designation. Governance modules remain generic and are separately reusable across the enterprise.

During both implementation and adoption of the AI model, appropriate controls are established throughout the entire lifecycle (Piorkowski et al., 2022). Institutional standards address key considerations for the AI supply-chain through multiple dimensions applicable on top of functional capabilities. The criticality of preparation and formalisation of implementation procedures, encompassing all rollouts, is underscored.

6. Regulatory Compliance and Legal Alignments

Automated AI systems deployed in regulated sectors such as banking, securities, and payments must align with extensive regulations governing financial services, consumer protection, and data management. Regulatory adherence encompasses a comprehensive array of obligations that institutions must integrate into their deployment practices. Mapping these obligations to corresponding processes fosters an integrated compliance approach, facilitating the management of operational and regulatory risks originating from the use of such systems. Transparency and procedural documentation enhance compliance accountability throughout the organization, contributing to formal AI governance portfolios. (Jain et al.2024)

A specialized governance committee dedicated to regulatory compliance oversees AI systems deployed in economic institutions. This body establishes direction and monitors adherence as part of an integrated governance framework. Reporting frequency to this committee is regulated across platforms and technologies, ensuring that emerging operational or regulatory risks are promptly communicated. Cross-border implementation of AI capabilities in the financial sector necessitates consideration of international material legislation. Many obligations or prohibitions may exhibit global replication across various jurisdictions, permitting the addressing of multiple governance ratios, risks, and controls through an integrated universal analysis. Nonetheless, the potential for notable divergences in standards or obligations also exists, warranting dual-tracked compliance scrutiny when both sets of regulations apply (Kurshan et al., 2020).

7. Data Governance, Privacy, and Security

Data governance encompasses the management of the availability, integrity, and security of the data used by an organisation. Critical aspects of data governance for economic institutions include stewardship, quality, lineage, and adequate access controls. These institutions are required to maintain the privacy of their clients, especially in light of regulatory mandates like the GDPR. Enhanced data collection measures must be regulated accordingly, covering privacy by design, retention minimisation, and other principles articulated in privacy legislation. Security considerations, including defence against adversarial ML attacks and requirements stemming from financial regulations, must also be satisfactorily addressed (Schneider et al., 2020).

A security policy for data used in AI systems must take account of the potential impact of data breaches, classification of data sets according to security risk, and prioritisation of protection for data considered critical. Provisions for the response to data incidents, both at the operational level and in relation to external parties, must also be specified (Korobenko et al., 2024).

8. Accountability, Auditability, and Transparency

Making AI systems within economic institutions auditable and accountable is key to managing ethical, operational, and regulatory compliance risks. The AI Act includes provisions on data governance, data management, documentation, record-keeping, traceability, and information sharing that are relevant for auditability, accountability, and transparency. Similar obligations are enshrined in legislation and soft-law guidance governing the financial and consumer protection sectors.

The agenda comprised actively addressing AI compliance; designing model-risk governance, surveillance, and control frameworks; laying out rules for transaction monitoring, fraud detection, risk assessment, and customer engagement; defining criteria for consumer engagement; specifying rules on personnel onboarding, training, and learning; and establishing AI governance processes, conformance methodologies, and competence development relating to compliance and fraud (Díaz-Rodríguez et al., 2023).

9. Governance Architecture: Roles, Bodies, and Processes

The governance architecture for AI systems consists of governance bodies with specific roles and clearly defined responsibilities. Governance bodies are accountable for approving specific activities and controlling the associated risks. Governance arrangements must be appropriate to the size, nature, and complexity of an economic institution and should be tailored to those specific characteristics. The governance architecture formalizes the chain of accountability regarding AI systems. Ultimately, it clearly specifies the roles and responsibilities along the three AI governance objectives

of ethical alignment, operational risk management, and regulatory compliance (Schneider et al., 2020). Elaboration of workflows, policies, standard operating procedures, and training ecosystems associated with the governance architecture further supports the achievement of broader strategic objectives, such as fostering responsible innovation activities or ensuring prudent risk-taking.

The governance framework should articulate specific governance bodies, roles, and responsibilities across the economic institution. Its precise configuration will be institution-specific, taking into account other governance arrangements. Financial-sector economic institutions typically maintain governance architectures with a Board of Directors; Board Committees; Executive Committees; Control Functions such as Internal Audit, Risk Management and Compliance; Policy Owner Functions and Business Lines; and Control-Function Resilience (Gill et al., 2022). Additional bodies with resources dedicated to addressing specific governance objectives may be established if needed.

10. Risk Assessment and Mitigation Frameworks

Risks related to AI-based services in economic institutions can be categorized into ethical, operational, and reputational risks (Kurshan et al., 2020). Ethical risks further segment into three aspects: (i) unintended harm caused through what the system produces, (ii) harm resulting when the system fails to deliver what its user has legitimately anticipated, and (iii) the behaviour of modelling systems capable of participating in standard discussions of fair, ethical, or socially responsible behaviour. Operational risks stem from the nature of the process and the nature of the model, thereby segregating into four categories: °contextual drift° and °model drift°, risks related to the quality of the data going into the model, data integration and interaction between existing and new models, and the range of possible failure modes in the model itself. In turn, reputational risks stem from the existence of, or association with, an imperfect model.

While some organisations employ formal taxonomies to assess the risks of existing AI models, Economic Institutions face the dilemma of ensuring that new modelling systems comply with existing policy without having knowledge of the construction of the model itself (Piorkowski et al., 2022). Consequently, a risk prioritisation framework with a unified scoring scheme, score-to-risk colour maps suitable for visualisation on dashboards, and plans for risk mitigation accordingly, based on detection and control for emerging operational risks.

11. Performance Measurement and Continuous Improvement

Effective risk governance requires systematic performance measurement. To monitor the effectiveness of governance arrangements and the associated safety and compliance levels, a set of key performance indicators (KPIs) is essential. These KPIs should be

benchmarked against industry standards or internal targets, which can be established by performing a comprehensive assessment of ecosystem maturity and exposure (Kurshan et al., 2020).

A periodic governance evaluation cycle allows for the identification of necessary adjustments and improvements. Establishing feedback loops fosters continuous enhancement, enabling all participants to learn progressively from previous experiences. Information regarding safety, compliance, and the effectiveness of governance arrangements should be communicated to stakeholders regularly, ensuring a shared understanding of the current state and required improvements. (D'Brot & Brandt, 2024)

12. International and Cross-Border Considerations

Rapid advancements in artificial intelligence (AI) present economies with opportunities to enhance productivity, spur growth, and strengthen resilience (Choung et al., 2023). The pace of development, however, also generates a multitude of economic and societal risks. Risk landscapes are evolving, and many economic institutions acknowledge the need to address both AI-related opportunities and AI-induced risks. AI governance enables institutions to manage these risks while ensuring that AI systems remain aligned with organizational objectives and national or international priorities (Kurshan et al., 2020).

Economic institutions are complex and produce undesirable outcomes if AI systems are not governed adequately. These institutions rely on multi-level interactions between diverse entities that possess varying objectives, capabilities, and levels of knowledge. The governance of systems increases with the system's complexity and number of interconnections. Economic institutions in particular are complex systems similar in form and function to banking, payments, securities, and asset management systems, which typically establish AI governance frameworks. Within an economic institution, AI can contribute to running the institution, can support other functions of the institution, or can assist in monitoring the institution. The integration of economic institutions with financial-economic bureaucracies that modify governance structures raises pedagogy and methodology to the national level. (Goforth et al.2022)

AI governance encompasses diverse characteristics and corresponding AI systems, and institutional governance, regulatory reporting, product guidance, and emphasis on oversight differ considerably across economic institutions. Numerous factors drive distinct governance characteristics, including operational models, product offerings, cross-border activity, and compliance with physical space specifications. Compliance with legal and regulatory requirements is an objective of significant importance across all economic institutions, but the scope of applicable laws and regulations exhibits extreme variability, with some institutions concentrating solely on compliance while others adhere to multiple requirements. (Efunniyi et al.2024)

13. Case Studies: Applications in Banking, Securities, and Payments

Banks and other financial institutions—including broker-dealers, investment advisors, hedge funds, and cryptocurrency exchanges—are increasingly using AI, machine learning (ML), and statistical modelling. AI governance in banks therefore focuses on managing both model risk and compliance risk. Banks must formulate an AI governance framework aligned with existing model risk management (MRM) and compliance risk frameworks. Such a framework may be more robustly integrated into banking operations than similar frameworks at broker-dealers where relatively fewer models produce a narrower data and technology footprint, or at firms where financial engineering, rather than customer segmentation, is foundational to a client-product assignment (Kurshan et al., 2020).

Securities firms have adopted an AI governance framework based on the industry's overall governance model for machine learning, natural language processing (NLP), statistical modelling, and generative AI. A more widely accepted approach exists than in payments. Payments firms have undertaken broader institutional initiatives around data governance and privacy; collecting data is a condition for gaining insights from generative AI, and financial service participants' initiatives still trail the rapid emergence of these technologies. As a result, generative AI is arguably still governed through an experimental paradigm with modest controls, reporting, and other management. (Adekunle & Chukwuma-Eke…, 2023)

14. Implementation Roadmap for Economic Institutions

Governance enables organisations to take action: it places artificial intelligence systems in a policy framework that helps guard data, safeguard fairness, and ensure compliance with ever-evolving rules and laws. These systems carry various risks, such as regulatory breaches, litigation without thoroughly tested data, ethical mishaps, and public backlash from altered performance. To govern artificial intelligence systems, institutions must understand their objectives and vulnerabilities, as well as the proper risk frameworks and policies to support those decisions. By introducing appropriate principles and practices, organisations can safeguard machine learning operations at every stage, fulfilling fundamental obligations and encouraging compliance with external mandates (Choung et al., 2023).

The phased rollout plan allows institutions to implement governance gradually—from prioritising one or two policies to expanding to others—depending on the maturity of their artificial intelligence systems and risk appetite. Governance enablers illustrate how an institution can make rapid progress toward implementation by upfront investments in technology and infrastructure. Growth requirements suggest the resources necessary for completing various milestones along the roadmap, while accompanying commitments delineate what must be done before those milestones can be achieved.

Governance readiness clarifies the baseline state of governance an institution possesses at the outset of the journey, providing common reference points for progress measurement. Change management and stakeholder engagement support the preparation required to undertake the transformation and reinforce employee commitment and involvement thereafter; continuous monitoring and maintenance ensure safeguarding practices evolve alongside artificial intelligence systems and emerging types of scrutiny. (Ogedengbe et al., 2024)

15. Challenges, Limitations, and Future Directions

AI governance in economic settings is a timely but immature field; guidance lapses present an urgent need for governance standardization. Resources develop specific recommendations on governance, yet many fall short of outlining necessary structures. Empirical material substantiating argumentation is scarce; detailed elucidations of prerequisite structures, responsibilities, and processes remain limited. Demand for improvement of formal frameworks merits heightened attention, especially heightened-focus governance frameworks (Choung et al., 2023).

Uncertainties in procedure stem from sector-specific governance constraints, which vary significantly with institutional profile. Attention to banking regulation bolsters parallel governance structures addressing widely dispersed deposit-taking and lending; uneven facility sufficiency, sophistication, and risk assumptions compound implementation difficulty. Accord allows decentralization of monitoring engagement for institutionally feasible and sector-focused governance structures. Bifurcating the spheres of governance and funding further limits expense concerns (Kurshan et al., 2020).

16. Conclusion

AI’s rapid technological, societal, and regulatory evolution challenges economic institutions to govern models of adoption, design, and use. The stakes are high; segments of the financial system increasingly regard proactively governing risks as non-negotiable for maintaining societal trust and pursuing business opportunities. Yet no integrated frameworks exist to manage AI’s ethical, operational, and compliance risks holistically across economic institutions. To fill the gap, this work proposes an emerging governance framework that aligns with economic motivations and regulatory developments. The framework provides a structured overview of the integrated governance model and its economic underpinnings, its specific dimensions for managing AI’s ethical, operational, and compliance risks, and the choices guiding its configuration. The analysis draws on inputs from interviews with over twenty organizations across the financial ecosystem and public consultations with a broad array of private and public stakeholders, guiding the framework’s continued refinement to address emerging needs.

The framework serves as a starting point for dialogue and design. The AI ecosystem and the regulatory landscape are fast evolving; the framework will continue to adapt and develop as the dialogue unfolds and as institutions across sectors and jurisdictions deploy AI systems, gain experience, and improve their understanding of sound practices. The objective remains to strike a balance among rapid innovation, governance, trust, public welfare, and compliance that bolsters sectoral credibility and facilitates the process of responsibly negotiating both major opportunities and critical risks (Choung et al., 2023). Operationalizing the framework can simultaneously fulfil diverse objectives—mitigating risks anticipated by global and national policy makers, regulators and oversight bodies, and technology advisory organisations—while advancing sound economic activities (Kurshan et al., 2020).

References:

- ✓ Choung, H., David, P., & S. Seberger, J. (2023). A multilevel framework for AI governance.
- ✓ Kurshan, E., Shen, H., & Chen, J. (2020). Towards Self-Regulating AI: Challenges and Opportunities of AI Model Governance in Financial Services.
- ✓ Gill, N., Mathur, A., & V. Conde, M. (2022). A Brief Overview of AI Governance for Responsible Machine Learning Systems.
- ✓ Yan, Y., Sun, S., Zhang, Y., Yang, Z., Zhu, C., Xu, B., & Liu, M. (2025). SearchAttack: Red Teaming Search-augmented LLMs via Injecting the Multi-hop Information-seeking Tasks.
- ✓ Piorkowski, D., Hind, M., & Richards, J. (2022). Quantitative AI Risk Assessments: Opportunities and Challenges.
- ✓ Jain, V., Balakrishnan, A., Beeram, D., Najana, M., & Chintale, P. (2024). Leveraging artificial intelligence for enhancing regulatory compliance in the financial sector. Int. J. Comput. Trends Technol, 72(5), 124-140.
- ✓ Schneider, J., Abraham, R., Meske, C., & vom Brocke, J. (2020). AI Governance for Businesses.
- ✓ Korobenko, D., Nikiforova, A., & Sharma, R. (2024). Towards a Privacy and Security-Aware Framework for Ethical AI: Guiding the Development and Assessment of AI Systems.
- ✓ Díaz-Rodríguez, N., Del Ser, J., Coeckelbergh, M., López de Prado, M., Herrera-Viedma, E., & Herrera, F. (2023). Connecting the Dots in Trustworthy Artificial Intelligence: From AI Principles, Ethics, and Key Requirements to Responsible AI Systems and Regulation.
- ✓ D'Brot, J. & Brandt, W. C. (2024). Applying Continuous Improvement Principles: Implementing Evaluation Practices.. Region 5 Comprehensive Center.

- ✓ Goforth, E., Yosri, A., El-Dakhakhni, W., & Wiebe, L. (2022). Infrastructure asset management system optimized configuration: A genetic algorithm–complex network theoretic metamanagement approach. Journal of Infrastructure Systems, 28(4), 04022029.
- ✓ Efunniyi, C. P., Abhulimen, A. O., Obiki-Osafiele, A. N., Osundare, O. S., Agu, E. E., & Adeniran, I. A. (2024). Strengthening corporate governance and financial compliance: Enhancing accountability and transparency. Finance & Accounting Research Journal, 6(8), 1597-1616.
- ✓ Adekunle, B. I. & Chukwuma-Eke…, E. C. (2023). Integrating AI-driven risk assessment frameworks in financial operations: A model for enhanced corporate governance. … Journal of Scientific ….
- ✓ Ogedengbe, A. O., Jejeniwa, T. O., Friday, S. C., & Olatunji, H. (2024). Framework for Digitally Transforming Financial Management Systems in SME and Public Sector Organizations.