AI risk governance in Islamic digital finance

Darmawan Darmawan

Abstract

Purpose – *The rapid integration of artificial intelligence (AI) into digital financial systems has created opportunities for innovation while simultaneously generating complex governance challenges. Although AI improves efficiency and financial inclusion, it also introduces risks related to cybersecurity, data governance, institutional readiness and regulatory compliance. This study aims to identify and prioritize AI-related risks in digital financial systems and examine their implications for AI governance, particularly in the context of Islamic digital finance.*

Design/methodology/approach – *This study employs a quantitative approach based on a survey of 260 respondents to evaluate perceptions of AI-related risks in digital financial environments. The Failure Mode and Effects Analysis (FMEA) framework is used to assess risks across four dimensions: potential occurrence, frequency, impact and detection capability. Risk Priority Numbers are applied to rank and classify risks, complemented by multilevel analysis at both category and item levels.*

Findings – *The findings indicate that the most significant risks are primarily governance-related rather than technological. Risk management capacity, human capital constraints and Sharia compliance emerge as dominant dimensions shaping AI risk governance. The analysis also shows that AI risk structures are nonuniform. While aggregate-level analysis identifies governance-related risks as dominant, item-level analysis reveals concentrated vulnerabilities, particularly cybersecurity risks, that may remain obscured within broader classifications. The findings further suggest the presence of a governance execution gap, where institutional awareness of AI-related risks is not always followed by effective mitigation practices.*

Research limitations/implications – *This study relies on perception-based survey data, which reflects respondents' assessments of AI-related risks rather than direct observations of technological failures in real financial systems. Future research could extend the analysis by using case studies or institutional data from financial organizations that implement AI technologies.*

Practical implications – *The findings highlight the importance of strengthening institutional capacity through risk management frameworks, training and organizational readiness. Policymakers and financial institutions should adopt governance approaches that integrate technological safeguards with regulatory and ethical oversight, particularly within Islamic financial systems.*

Social implications – *Effective AI governance can strengthen public trust, support financial inclusion, and enhance the stability of digital financial systems. In Islamic financial contexts, alignment between AI systems and ethical as well as Sharia principles remains essential for maintaining institutional legitimacy and societal acceptance.*

Originality/value – *This study contributes to the literature by applying FMEA to AI risk governance in digital financial systems and by introducing a multilevel risk assessment perspective. The study further advances understanding of AI governance by identifying governance execution gaps and emphasizing the need to integrate technological and Sharia-based governance frameworks.*

Keywords *Artificial intelligence governance, Digital financial systems, AI risk management, Algorithmic governance, Failure mode and effects analysis, Islamic digital finance*

Paper type *Research paper*

Darmawan Darmawan is based at the Department of Islamic Finance Management, Universitas Islam Negeri Sunan Kalijaga, Yogyakarta, Indonesia.

1. Introduction

Artificial intelligence (AI)-driven financial systems operate through complex algorithmic processes that often function as opaque black-box models. These systems may generate unintended outcomes, including algorithmic bias, inaccurate predictions, cybersecurity vulnerabilities and

Received 11 March 2026
Revised 28 March 2026
10 May 2026
15 May 2026
22 May 2026
Accepted 24 May 2026

regulatory compliance challenges. Such risks raise concerns about transparency, accountability and institutional control, particularly in financial environments where automated decisions can affect financial stability and consumer protection (Varian, 2018; Dwivedi *et al.*, 2021; Hacker *et al.*, 2025).

In response to these challenges, AI governance has emerged as an important framework for managing risks associated with algorithmic decision-making in digital financial systems. In this study, AI governance refers to the institutional and regulatory mechanisms intended to ensure transparency, accountability and responsible AI deployment. Unlike broader digital governance, which addresses digital technologies more generally, AI governance focuses specifically on the oversight of automated decision-making systems and related risks, including explainability, bias and system reliability.

Despite the growing importance of AI governance, existing research remains fragmented and largely conceptual. Many studies focus on specific AI risks, such as algorithmic bias or cybersecurity threats, without systematically evaluating their relative importance within complex financial systems. Empirical studies prioritizing AI-related risks from a governance perspective also remain limited, particularly within digital financial ecosystems.

These challenges are further amplified in Islamic digital finance, where financial activities must comply with Shariah principles emphasizing fairness, transparency and ethical conduct. The integration of AI into Islamic financial services introduces additional governance complexities because algorithmic decision-making must align not only with regulatory requirements but also with Shariah compliance. Nevertheless, the intersection between AI governance and Islamic financial principles remains underexplored, particularly regarding the integration of Sharia governance into AI-driven decision-making systems (Khan, 2025; Wahab and Mahdiya, 2025).

To address these gaps, this study examines risks associated with the adoption of artificial intelligence in digital financial systems and identifies the most critical governance challenges affecting its implementation. The study employs the Failure Mode and Effects Analysis (FMEA) approach to evaluate AI-related risks across multiple dimensions, including potential occurrence, frequency, impact and detection capability.

This study contributes to the literature in several ways. First, it extends research on AI governance by applying the FMEA framework to systematically prioritize AI-related risks in digital financial systems (Stamatis, 2003; Liu *et al.*, 2013). Second, the study introduces a multilevel risk analysis combining category-level and item-level assessment to identify hidden risk concentrations that may not be visible through aggregate analysis alone. Third, the findings reveal a governance execution gap, where institutional awareness of AI-related risks does not always translate into effective mitigation capacity. Finally, the study contributes to the growing literature on AI governance in Islamic digital finance by integrating technological governance perspectives with Sharia-based governance considerations (Khan, 2025).

2. Literature review

2.1 Artificial intelligence in digital financial systems

AI has emerged as a transformative force in digital financial systems, enabling institutions to improve efficiency, automate decision-making and expand access to financial services. Advances in machine learning, big data analytics and algorithmic decision-making have reshaped financial operations, including credit scoring, fraud detection, algorithmic trading and regulatory compliance monitoring (Arner *et al.*, 2017; Jagtiani and Lemieux, 2019).

The integration of AI into financial infrastructure has accelerated the development of digital financial ecosystems, where services are delivered through interconnected platforms. These systems enable financial institutions to process large volumes of data, generate predictive insights, and improve service delivery. In emerging economies, AI-enabled

financial technologies have contributed to financial inclusion by extending financial services to underserved populations (Philippon, 2019; Demirgüç-Kunt *et al.*, 2022).

However, increasing reliance on AI has introduced significant governance challenges. AI systems often operate as complex black-box models, making it difficult to interpret how decisions are generated. This opacity raises concerns regarding transparency, accountability and regulatory oversight in financial decision-making (Dwivedi *et al.*, 2021). As a result, AI governance has become an increasingly important issue in digital financial systems, requiring institutional frameworks capable of managing emerging technological risks.

2.2 Artificial intelligence risks and algorithmic governance

Despite its potential benefits, the deployment of AI-driven systems in financial services introduces multiple layers of risk. These risks stem from the data-driven and predictive nature of AI, which relies heavily on historical data sets and complex modeling techniques.

One of the most prominent risks is algorithmic bias, where systems trained on biased or incomplete data may produce discriminatory outcomes. In financial services, such bias may affect credit allocation and financial access, potentially reinforcing inequality (Varian, 2018; Fuster *et al.*, 2022). In addition, AI systems may generate inaccurate predictions and unintended outcomes, leading to operational and systemic risks.

Cybersecurity risks also represent an important concern in AI-enabled financial systems. Increasing reliance on interconnected digital infrastructures exposes financial platforms to cyberattacks, data breaches and system manipulation. Broeders and Prenio (2018) note that digital financial systems expand the attack surface for cyber threats, requiring stronger cybersecurity governance and regulatory oversight.

Recent studies suggest that AI-driven digital platforms may create new forms of systemic risk because of interdependence among algorithmic infrastructures, data ecosystems and financial networks (Hacker *et al.*, 2025). In addition, trustworthy cyber threat intelligence and institutional cybersecurity readiness have become increasingly important in AI-enabled financial systems (Karaosman *et al.*, 2026).

In response to these challenges, algorithmic governance has gained increasing attention. Algorithmic governance refers to the institutional and regulatory mechanisms designed to oversee automated decision-making systems and ensure transparency, accountability, explainability and compliance with ethical and legal standards (Floridi *et al.*, 2018; Wirtz *et al.*, 2020).

2.3 Risk governance in digital financial ecosystems

Risk governance refers to the institutional processes through which risks are identified, assessed and managed within complex socio-technical systems (Renn, 2017). In digital financial ecosystems, risk governance must address challenges including technological failures, cybersecurity vulnerabilities, regulatory compliance and institutional capacity constraints. In digital financial ecosystems, risk governance must address challenges including technological failures, cybersecurity vulnerabilities, regulatory compliance and institutional capacity constraints.

The emergence of AI-driven financial systems has expanded the scope of risk governance beyond traditional financial risks, such as credit and market risks, to include risks related to data governance, algorithmic decision-making and technological infrastructure (Philippon, 2019; Thakor, 2020).

Effective risk governance in digital financial systems requires a multidimensional approach integrating regulatory oversight, technological safeguards and institutional capacity. Transparency and explainability are particularly important because AI systems frequently

operate as opaque models. Financial institutions must therefore develop mechanisms such as explainable AI and algorithm auditing to ensure accountability and regulatory compliance. (Floridi *et al.*, 2018).

2.4 Artificial intelligence governance in Islamic digital finance

The integration of artificial intelligence into Islamic digital finance introduces governance challenges extending beyond conventional financial risk considerations. Islamic financial systems are governed by Shariah principles emphasizing fairness (adl), transparency, and the prohibition of uncertainty (gharar) and unjust practices.

The use of AI in Islamic financial services raises important questions regarding the alignment of algorithmic decision-making with Shariah principles. For instance, algorithmic bias or opaque decision-making may conflict with the ethical and transparency requirements of Islamic finance. Ensuring Shariah compliance in AI-driven financial systems therefore requires integrating digital governance mechanisms with Shariah governance frameworks.

Recent studies highlight the need to develop AI governance frameworks that incorporate Islamic ethical principles and regulatory standards (Khan, 2025; Wahab and Mahdiya, 2025). These frameworks emphasize transparency, accountability and explainability in AI systems to ensure compliance with Shariah requirements in digital financial environments.

Nevertheless, empirical research examining AI-related risks within Islamic digital finance remains limited, indicating the need for further investigation into how AI governance frameworks can align with both technological and Shariah governance requirements.

2.5 Theoretical framework

This study is primarily grounded in Risk Governance Theory, which explains how institutions identify, assess, prioritize and manage complex risks within socio-technical systems (Renn, 2017; Aven and Renn, 2018). Risk governance theory is particularly relevant to AI because AI-related risks are characterized by uncertainty, interdependence and potentially systemic consequences within digital financial ecosystems. To complement this perspective, the study also draws selectively from the Technology Organisation Environment (TOE) framework and Institutional Theory to explain how organizational readiness, institutional capacity and regulatory environments shape the governance of AI-related risks in digital financial systems (Tornatzky *et al.*, 1990; Scott, 2013; Urbano *et al.*, 2019; Boateng, 2020). These perspectives help explain why AI governance challenges are shaped not only by technological capability but also by organizational preparedness, governance structures and external regulatory pressures.

Within this framework, AI governance is defined as the institutional, regulatory and organizational mechanisms designed to ensure that AI systems operate in a transparent, accountable, ethical and risk-controlled manner within digital financial systems. Unlike broader digital governance, AI governance specifically addresses risks arising from algorithmic decision-making, including explainability, accountability, bias, cybersecurity vulnerability and regulatory compliance (Floridi *et al.*, 2018; Wirtz *et al.*, 2020). From this theoretical perspective, AI-related risks are understood not merely as technological failures but as governance challenges shaped by the interaction between institutional capacity, organizational readiness, regulatory structures and algorithmic processes (Renn, 2017; Aven and Renn, 2018). By integrating risk governance and AI governance perspectives, the study conceptualizes AI governance as a multidimensional institutional process through which digital financial systems maintain operational reliability, ethical legitimacy and regulatory compliance in increasingly automated financial environments.

2.6 Research gap

Despite the growing literature on artificial intelligence and digital financial systems, several important gaps remain.

First, existing studies predominantly focus on conceptual discussions of AI governance, with limited empirical research systematically evaluating AI-related risks in digital financial systems. Second, prior research often examines specific AI risks in isolation, such as algorithmic bias or cybersecurity vulnerabilities, without considering interactions between multiple risk dimensions. Third, empirical studies prioritizing AI-related risks from a governance perspective remain limited, particularly within emerging digital financial ecosystems.

Moreover, the integration of AI governance with Islamic financial principles remains underexplored despite the increasing adoption of digital technologies in Islamic financial services. To address these gaps, this study applies the FMEA framework to identify and prioritize AI-related risks in digital financial systems empirically. As illustrated in Figure 1, the study proposes a conceptual framework categorizing AI-related risks into technological risks, data and cybersecurity risks and institutional governance risks, highlighting the need for an integrated governance approach.

3. Research methodology

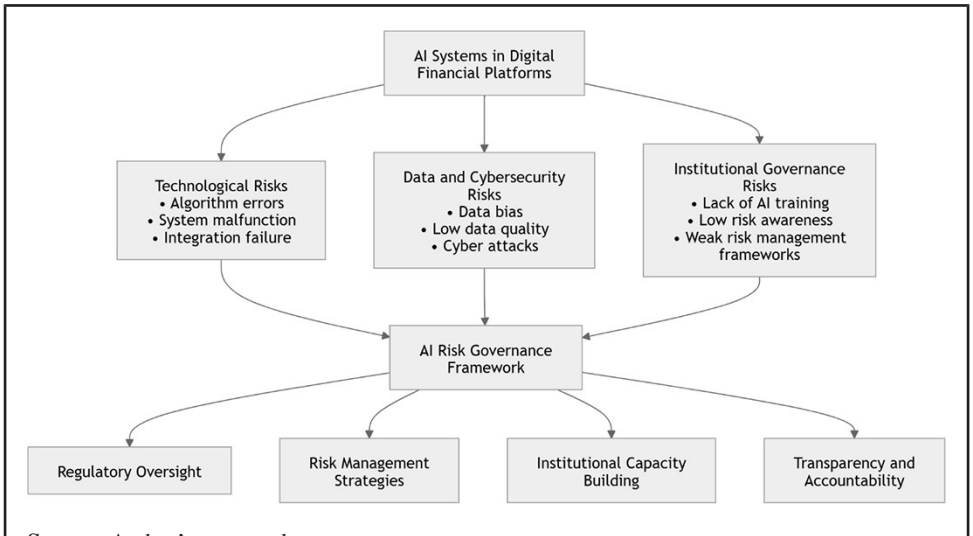
3.1 Research design

This study employs a quantitative research design to examine and prioritize risks associated with the adoption of AI in digital financial systems. The increasing integration of AI into financial services has created opportunities to improve operational efficiency and expand financial inclusion while also introducing new technological and governance risks (Arner *et al.*, 2017; Broeders and Prenio, 2018).

To evaluate these risks systematically, this study employs the FMEA framework. FMEA is a structured risk assessment method used to identify potential system failures, assess their consequences, and prioritize mitigation strategies (Stamatis, 2003). Although originally developed in engineering, FMEA has increasingly been applied in information systems and technology risk analysis because of its ability to assess risk severity across multiple dimensions (Liu *et al.*, 2013).

The selection of FMEA is based on its suitability for prioritizing multidimensional risks under conditions of uncertainty and interdependence. AI-related risks in digital financial

Figure 1 AI Risk Governance Framework for Digital Financial Systems



Source: Author's own work

systems involve technological, organizational, regulatory and ethical dimensions that interact simultaneously. Compared with conventional descriptive risk assessment approaches, FMEA enables a structured prioritization process by integrating severity, occurrence, impact and detection capability within a single analytical framework. This makes FMEA particularly suitable for identifying governance priorities in complex AI-driven financial environments.

3.2 Sample and data collection

Data were collected through an online survey designed to capture respondents' perceptions of AI-related risks in digital financial systems. Survey methods are appropriate for examining emerging technological risks because they allow researchers to gather insights from diverse stakeholders regarding perceived risks and governance challenges Hair *et al.* (2019).

A purposive sampling approach was employed to ensure that respondents had a minimum level of familiarity with digital financial services. The inclusion criteria required prior exposure to digital financial platforms or financial technology applications. The target population included students, academics, professionals and members of the general public with varying levels of experience in digital finance.

A total of 260 valid responses were collected and included in the final analysis. The sample reflects demographic diversity in terms of age, education and occupation. The relatively high proportion of respondents with tertiary education suggests an adequate understanding of digital financial systems, thereby improving response reliability.

The sample size is considered adequate for exploratory quantitative studies involving multidimensional risk assessment and FMEA-based analysis (Hair *et al.*, 2019). In FMEA-oriented research, analytical emphasis is placed on the consistency and relevance of stakeholder evaluations rather than on probabilistic population representation. Data collection was conducted in Indonesia between October 2025 and March 2026 through an online survey distributed to individuals familiar with digital financial services. Respondents were drawn from both urban and rural areas and represented diverse occupational backgrounds, including students, academics and professionals.

3.3 Operational definition of variables

The measurement instrument was developed to assess respondents' perceptions of risks associated with artificial intelligence in digital financial systems. The conceptualization of AI-related risks is derived from literature on digital financial governance, risk management and FMEA framework. This study identifies several categories of AI-related risks, including technological risk, cybersecurity risk, data quality risk, system integration risk, compliance risk and adoption risk. These categories represent different dimensions of vulnerability within AI-driven financial systems. In addition, the FMEA framework evaluates risk severity across four dimensions: potential (severity), frequency (occurrence), impact (consequence) and detection capability. These dimensions provide a structured basis for assessing and prioritizing AI-related risks.

All variables were measured using a five-point Likert scale ranging from 1 (very low) to 5 (very high), with higher scores indicating greater perceived risk severity.

The operational definitions of the study variables are presented in Table 1.

3.4 Risk assessment method

This study applies the FMEA approach to evaluate the relative importance of AI-related risks. FMEA enables a systematic assessment of potential failure modes by considering multiple dimensions of risk severity, including likelihood, impact and detection capability

Table 1 Operational definition of variables

Variable	*Indicators*	*Key references*
Technology risk	Risk of AI system malfunction, algorithmic errors, and inaccurate automated decision-making in financial services	Arner *et al.* (2017); Jagtiani and Lemieux (2019)
Cybersecurity risk	Risk of cyberattacks, data breaches, and unauthorized access affecting digital financial platforms	Broeders and Prenio (2018); Philippon (2019); Varian (2018); Dwivedi *et al.* (2021)
Data quality risk	Risk arising from incomplete, biased, or unstructured data used to train AI models	Dwivedi *et al.* (2021); Floridi *et al.* (2018)
System integration risk	Risk related to the integration of AI technologies with existing financial infrastructure and legacy systems	Arner *et al.* (2017); Vives (2019)
Compliance risk	Risk related to regulatory compliance, ethical standards, and governance requirements in AI-based financial services	Broeders and Prenio (2018); Zetzsche *et al.* (2020)
Adoption risk	Risk arising from limited digital literacy, lack of technical expertise, and resistance to AI adoption	Rogers (2003); Venkatesh *et al.* (2012)
Potential (severity)	Perceived possibility that a specific AI-related risk may occur	Stamatis (2003)
Frequency (occurrence)	Perceived frequency with which a risk may arise during AI operation	Liu *et al.* (2013)
Impact (consequence)	Severity of consequences if the risk occurs	Liu *et al.* (2013)
Detection	The ability of institutions to identify risks before they lead to significant failures	Stamatis (2003)

Source(s): Author's own work

(Stamatis, 2003; Liu *et al.*, 2013). By integrating survey-based perception data with the FMEA framework, the study translates qualitative assessments into quantifiable risk indicators. This approach enables structured comparison across risk categories and supports identification of priority areas for governance intervention.

3.5 Risk prioritization procedure

Risk prioritization is conducted using the Risk Priority Number (RPN), calculated by multiplying four risk dimensions:

$$RPN = Potential \times Frequency \times Impact \times Detection$$

Higher RPN values indicate greater perceived risk severity and identify areas requiring stronger governance attention. After calculating the RPN values for all identified risks, the risks are ranked from highest to lowest to determine the most critical AI-related risks in digital financial systems. This prioritization provides empirical insight into areas where regulatory oversight, institutional governance and technological safeguards are most needed.

4. Results

4.1 Respondent characteristics

A total of 260 valid responses were included in the analysis. The respondents reflect diverse demographic characteristics in terms of gender, age, education, occupation and residential location, as presented in Table 2.

The sample is dominated by respondents aged between 20 and 30 years (49.2%), with relatively high educational attainment, as more than 78% hold undergraduate or postgraduate degrees. This suggests adequate familiarity with digital technologies and financial systems. In addition, most respondents reside in urban areas (67.7%), reflecting the higher penetration of digital financial services in urban environments. These characteristics suggest that respondents are sufficiently familiar with digital financial systems to provide informed perceptions of AI-related risks.

Table 2 Demographic characteristics of respondents

Characteristic	*Category*	*Frequency*	*%*
Gender	Male	114	43.8
	Female	146	56.2
Age	< 20	36	13.8
	20–30	128	49.2
	31–40	56	21.5
	41–50	27	10.4
	50 <	13	5.0
Education	Secondary/Diploma	55	21.1
	Undergraduate	105	40.4
	Postgraduate	100	38.5
Occupation	Student	131	50.4
	Education sector	98	37.7
	Other professions	31	11.9
Residence	Urban	176	67.7
	Rural	84	32.3

Source(s): Author's own work

4.2 Descriptive statistics of artificial intelligence risk dimensions

Descriptive statistics were calculated for the four dimensions within the FMEA framework: potential, frequency, impact and detection. The results are presented in Table 3.

The mean values range from 3.48 to 3.67, indicating that respondents generally perceive AI-related risks as moderately high. Among these dimensions, impact (mean = 3.67) shows the highest value, suggesting that respondents consider the consequences of AI-related failures significant. Meanwhile, detection records slightly lower values, indicating moderate confidence in institutions' ability to identify risks before escalation. These findings suggest that AI-related risks are not only frequent but also potentially severe, reinforcing the importance of effective governance mechanisms.

4.3 Risk priority analysis and classification

The RPN was calculated for each identified risk using the FMEA framework. To improve interpretability, risks were classified into critical and noncritical categories based on the average RPN threshold value (149.72). Risks exceeding this threshold were categorized as critical. The classification results based on the RPN threshold are presented in Table 4.

At the aggregate level, governance-related risk categories (risk management failure, adoption and acceptance failure and Sharia compliance failure) are classified as critical. In contrast, technological, data and system integration risks fall below the threshold and are categorized as noncritical. These findings suggest that AI-related risks in digital financial systems are driven primarily by governance and institutional factors rather than technological limitations.

Table 3 Descriptive statistics of AI risk dimensions

Risk dimension	*Mean*	*SD*
Potential	3.63	0.72
Frequency	3.48	0.69
Impact	3.67	0.71
Detection	3.49	0.68

Source(s): Author's own work

Table 4 Classification of AI-related risks based on RPN threshold

Risk category	*Risk indicator*	*RPN*	*Classification*
AI technology failure	Inability of AI systems to process or analyze data accurately	132.36	Non-Critical
	Vulnerability to cyberattacks and data breaches	162.94	Critical
	Limited ability to process unstructured data	132.56	Non-Critical
Data failure	Lack of relevant and high-quality data	145.47	Non-Critical
	Dependence on biased historical data	148.31	Non-Critical
	Lack of context-specific data for islamic finance	146.75	Non-Critical
System integration failure	Difficulty integrating AI with existing systems	137.09	Non-Critical
	Misalignment with institutional requirements	135.83	Non-Critical
Sharia compliance failure	Noncompliance with sharia principles	160.16	Critical
	Limited ability to capture socio-cultural context	140.34	Non-Critical
	Difficulty accommodating sharia complexity	148.73	Non-Critical
Risk management failure	Lack of awareness of AI risks	165.25	Critical
	Failure to implement mitigation strategies	144.94	Non-Critical
	Need to strengthen AI risk management frameworks	171.81	Critical
Adoption and acceptance failure	Stakeholder resistance to AI adoption	155.32	Critical
	Lack of training and education	170.97	Critical
	General distrust toward AI	136.01	Non-Critical
	Lack of AI-related skills	160.17	Critical

Source(s): Author's own work

4.4 Item-Level analysis and key risk patterns

A more detailed item-level analysis reveals meaningful variations across risk categories. Within the risk management category, most items are classified as critical, particularly those related to risk awareness and the need to strengthen risk management strategies. However, the implementation of mitigation strategies is not classified as critical, suggesting a gap between awareness and execution. Within the adoption and acceptance category, risks related to training, skills and stakeholder resistance are classified as critical, whereas general distrust toward AI is not. This suggests that practical capability constraints represent a greater barrier to AI adoption than abstract perceptions of trust. Within the Sharia compliance category, only one item (noncompliance with Sharia principles) is classified as critical. Despite this, the category remains critical overall, highlighting the importance of ethical and regulatory alignment in AI-driven financial systems. An important anomaly is observed in the technological risk category. Although the category is classified as noncritical at the aggregate level, cybersecurity risk exceeds the critical threshold. This finding suggests that aggregate-level analysis may obscure critical risk hotspots.

4.5 Governance implications of the risk structure

The findings provide several implications for AI governance in digital financial systems. First, governance-related risks dominate the overall risk structure, suggesting that institutional capacity, regulatory frameworks and human capital are more influential than technological factors in managing AI adoption. Second, variation across risk categories suggests that governance strategies should be targeted rather than uniform. Policymakers and institutions should focus on specific high-risk areas rather than relying solely on aggregate assessments. Third, the prominence of human capital-related risks underscores the importance of training, education and digital literacy programs in supporting AI implementation. Effective AI governance therefore requires a multidimensional approach integrating technological safeguards, institutional capacity and regulatory oversight.

5. Discussion

5.1 Artificial intelligence risks in digital financial systems: beyond technological failures

The findings indicate that the most critical risks associated with AI in digital financial systems are primarily governance-related rather than purely technological. This finding aligns with studies suggesting that the rapid diffusion of AI in financial services has outpaced the institutional and regulatory capacities needed to govern emerging technological risks effectively (Arner *et al.*, 2017; Zetzsche *et al.*, 2020; Wirtz *et al.*, 2020). Recent discussions on AI governance similarly identify accountability, transparency and regulatory oversight as central concerns in increasingly algorithm-driven financial systems (Floridi *et al.*, 2018; Dwivedi *et al.*, 2021).

More specifically, the findings suggest that governance capacity, particularly risk management structures, organizational readiness and human capital, plays a more decisive role in shaping AI risk profiles than technological capability alone. This supports prior studies in fintech governance arguing that the effectiveness of AI deployment depends heavily on institutional readiness and organizational capability rather than technological sophistication alone (Gomber *et al.*, 2018; Philippon, 2019; Thakor, 2020). In this respect, AI-related risks are embedded within institutional contexts in which governance mechanisms shape how technological risks are interpreted, managed and mitigated.

The study extends the literature by showing that governance-related risks are not only conceptually important but also empirically dominant within a structured risk-prioritization framework. While previous studies often discuss AI governance challenges in general terms, the findings identify specific governance dimensions, including risk awareness, training and institutional risk management capacity, as consistently critical. This complements recent work on responsible AI and algorithmic governance that calls for translating governance principles into measurable and actionable mechanisms (Floridi *et al.*, 2018; Wirtz *et al.*, 2020; Batool *et al.*, 2023).

At the same time, the findings partially differ from studies emphasizing technological risks, such as algorithmic opacity and model uncertainty, as the primary challenges of AI implementation (Floridi *et al.*, 2018; Dwivedi *et al.*, 2021). Although these risks remain important, respondents perceive governance deficiencies, particularly those related to institutional capacity and implementation, as more immediate and consequential than technical limitations alone. These findings suggest a shift in AI risk governance from purely technical concerns toward institutional and implementation-related challenges.

An important contribution of the study is the identification of a governance execution gap. Item-level analysis shows that although awareness of AI-related risks and governance needs is consistently classified as critical, the implementation of mitigation strategies is not. This suggests that institutions may recognize AI-related risks but still face difficulties translating that awareness into effective governance practices. This finding resonates with recent research highlighting the persistent gap between formal AI governance frameworks and their operationalization within organizations (Schiff *et al.*, 2021; Krafft *et al.*, 2020). Overall, the findings suggest that the central challenge of AI adoption in digital financial systems lies not in the absence of technological solutions but in institutional capacity to implement and sustain them effectively.

5.2 Hidden risk patterns: the importance of item-level analysis

A key insight emerging from the findings is the presence of hidden risk patterns that become visible primarily through item-level analysis. While aggregate-level classification suggests that certain categories, such as technological risk, are relatively less critical, item-level analysis reveals that specific risks, particularly cybersecurity vulnerabilities, exceed the

critical threshold. This suggests that aggregate assessments may obscure concentrated risk nodes and therefore produce an incomplete understanding of overall risk structures. This finding is consistent with risk governance literature emphasizing that complex socio-technical systems often exhibit nonuniform risk distributions that cannot be fully captured through aggregated indicators (Aven, 2016; Renn, 2017). In digital financial systems, where risks emerge through interactions among technological infrastructures, data ecosystems and institutional processes, such heterogeneity becomes especially pronounced (Philippon, 2019; Thakor, 2020).

The findings also highlight the limitations of conventional single-level approaches in assessing AI-related risks. Existing studies frequently evaluate AI risks using aggregated constructs, such as operational, technological or governance risk, without examining variations at the indicator level (Floridi *et al.*, 2018; Dwivedi *et al.*, 2021). While these approaches remain useful for conceptual modeling, they may overlook critical risk concentrations requiring targeted intervention. By contrast, the multilevel approach adopted in the study enables a more nuanced identification of risk priorities.

A similar pattern appears in the adoption and acceptance dimension. Although the category itself is classified as critical, item-level analysis shows that risks related to training, skills and stakeholder capability are substantially more critical than general distrust toward AI. This finding aligns with the Unified Theory of Acceptance and Use of Technology (UTAUT), which emphasizes the importance of facilitating conditions and user capability in technology adoption (Venkatesh *et al.*, 2012). However, the findings extend this perspective by showing that capability constraints not only influence adoption outcomes but also shape the broader risk profile of AI systems. In this regard, insufficient human capital functions not only as a barrier to adoption but also as a source of systemic vulnerability.

The discrepancies between aggregate and item-level classifications suggest that AI-related risks exhibit characteristics of "emergent risk structures," in which risk significance is unevenly distributed across interconnected systems (Aven and Renn, 2018). This perspective is particularly relevant for AI-driven financial systems, where interdependencies among algorithms, data and institutional processes can amplify localized failures into broader systemic vulnerabilities (Hacker *et al.*, 2025). The findings therefore suggest that effective AI governance requires moving beyond aggregate risk metrics toward more granular and context-sensitive assessment frameworks capable of identifying both structural risk patterns and localized risk concentrations.

5.3 Cybersecurity, data governance and systemic risk

The identification of cybersecurity risk as a critical issue, despite belonging to a technological category classified as noncritical at the aggregate level, highlights the increasingly systemic nature of technological vulnerabilities in digital financial systems. This finding suggests that certain risks emerge not as isolated technical problems but as critical nodes within interconnected socio-technical systems. The findings therefore support the argument that cybersecurity risk represents a foundational layer of systemic risk in AI-driven financial ecosystems. Prior studies similarly note that the digitalization of financial services has expanded exposure to cyber threats as institutions become increasingly dependent on interconnected platforms and real-time data processing (Broeders and Prenio, 2018; Philippon, 2019). Recent studies also argue that AI systems may amplify these vulnerabilities by increasing complexity, opacity and interdependence across financial networks (Gomber *et al.*, 2018; Hacker *et al.*, 2025).

The findings further demonstrate that cybersecurity risk cannot be understood solely as a technical issue but must be viewed within broader governance and institutional contexts. Although cybersecurity is frequently framed as a technological challenge, effective cyber risk management depends heavily on organizational readiness, regulatory frameworks and

institutional coordination (Aven and Renn, 2018; Wirtz *et al.*, 2020; Karaosman *et al.*, 2026). The findings support this perspective by showing that cybersecurity emerges as critical because of its systemic implications rather than its categorical classification alone.

In addition to cybersecurity, the findings highlight the importance of data governance as a foundational component of AI risk governance. Although data-related risks are not classified as critical at the aggregate level, their association with algorithmic bias, model reliability and decision accuracy suggests that they significantly influence the integrity and trustworthiness of AI systems. This finding aligns with research demonstrating that poor data quality and biased data sets can distort algorithmic outputs and undermine the fairness and effectiveness of AI-driven decision-making (Floridi *et al.*, 2018; Dwivedi *et al.*, 2021).

The findings further suggest that data governance risks may function as latent systemic risks rather than immediately visible threats. While respondents may not perceive data-related issues as the most urgent concerns, these factors may still substantially influence the reliability of AI systems over time. This interpretation is consistent with research on systemic risk in digital platforms, which argues that certain vulnerabilities remain hidden until triggered by failures within interconnected systems (Hacker *et al.*, 2025). Overall, the findings suggest that cybersecurity and data governance should be understood as interdependent components of a broader systemic risk framework in AI-enabled financial systems. Effective AI governance therefore requires integrated approaches combining technological safeguards, institutional coordination and regulatory oversight.

5.4 Institutional readiness and human capital constraints

The findings highlight how institutional readiness and human capital constraints represent central challenges in the governance of AI-enabled digital financial systems. Risks related to insufficient training, limited technical skills, and low levels of risk awareness are consistently identified as critical, indicating that effective AI implementation depends more on organizational capability than on technological availability alone. This finding is consistent with established technology adoption theories, particularly the UTAUT, which emphasizes the role of facilitating conditions, user capability and organizational support in shaping technology adoption outcomes (Venkatesh *et al.*, 2012). Similarly, diffusion of innovation theory suggests that the adoption of complex technologies depends not only on functional advantages but also on the knowledge, skills and readiness of potential adopters (Rogers, 2003). The findings therefore support these perspectives by showing that capability-related factors, such as training and skill development, are more critical than attitudinal factors, including general trust in AI.

The study also extends existing theories by showing that human capital constraints not only affect AI adoption but also shape the broader risk structure associated with implementation. Unlike traditional technology adoption models primarily concerned with usage behavior, the findings suggest that insufficient organizational capability can amplify operational, governance and compliance risks in AI-driven systems. This aligns with research on digital transformation emphasizing that the benefits of advanced technologies depend heavily on complementary investments in workforce development and organizational capability (Verhoef *et al.*, 2021).

An important insight emerging from the findings is the discrepancy between risk awareness and mitigation capacity. Although respondents perceive awareness of AI-related risks as highly critical, mitigation strategies are not rated with the same urgency. This suggests that institutions may recognize the importance of AI governance but still face difficulties translating that awareness into effective operational practices. This finding resonates with the concept of capability gaps in organizational theory, in which knowledge does not necessarily translate into effective action because of resource constraints, coordination problems or institutional limitations (Teece, 2018).

The prominence of human capital-related risks also highlights the continuing importance of human oversight in AI-driven financial systems. Although AI technologies enable automation and data-driven decision-making, human expertise remains essential for interpreting algorithmic outputs, ensuring regulatory compliance, and managing exceptions in complex financial environments (Wirtz *et al.*, 2020; Dwivedi *et al.*, 2021). In this regard, AI should be viewed not as a substitute for human decision-making but as a complementary tool requiring strong institutional support and skilled human intervention. Overall, the findings suggest that institutional readiness and human capital development remain central components of effective AI governance. Without sustained investment in training, organizational learning and capacity building, even advanced AI systems may fail to deliver their intended benefits or may generate new governance risks within digital financial systems.

5.5 Artificial intelligence governance in the context of Islamic digital finance

The findings provide valuable insights into AI governance within Islamic digital financial systems. The identification of Sharia compliance risk as a critical category, despite only one item exceeding the threshold, highlights the asymmetric character of ethical risk in Islamic finance. Unlike conventional finance, certain risks in Islamic finance carry disproportionate significance because they directly affect institutional legitimacy and stakeholder trust. This observation aligns with Sharia governance literature emphasizing that compliance is not merely a regulatory requirement but a core element of institutional credibility and public trust (Rahman *et al.*, 2023; Minaryanti and Mihajat, 2024). Even isolated instances of noncompliance may undermine institutional legitimacy because financial transactions must adhere to principles such as the prohibition of riba (interest), gharar (uncertainty) and unethical practices (Kismawadi *et al.*, 2025).

Recent studies on AI implementation in Islamic finance further reinforce this concern. Although AI technologies can improve efficiency, risk management and Sharia compliance monitoring, they also introduce ethical and legal challenges related to algorithmic transparency, data bias and accountability (Sain and Adinugraha, 2025; Iqbal *et al.*, 2025). These challenges are particularly significant because decision-making in Islamic finance must be technically, ethically and legally justifiable. The findings therefore support emerging research advocating the integration of AI governance frameworks with Sharia governance principles. Recent studies propose lifecycle-based AI governance approaches that embed Sharia principles, including justice (adl), public interest (maslahah) and accountability, across data processing, model development and deployment (Zafar and Ali, 2025). This suggests that AI governance in Islamic finance extends beyond technical compliance toward broader ethical considerations.

The study also extends the literature by demonstrating that Sharia compliance risk may function as a high-impact, low-frequency risk. Although only one item is classified as critical, its elevated RPN score indicates that noncompliance in decision-making processes may carry substantial systemic implications. This finding resonates with discussions on maqasid al-Shariah-based AI ethics emphasizing that the objective of Islamic financial systems extends beyond regulatory compliance toward the preservation of justice, social welfare and economic stability (Sain and Adinugraha, 2025).

The findings also highlight the need to reconcile two parallel governance logics: technological governance and Sharia governance. While the former emphasizes efficiency, risk control and regulatory compliance, the latter focuses on ethical accountability and alignment with Islamic legal principles. Existing studies suggest that these frameworks often remain fragmented, with many institutions adopting AI technologies without fully integrating them into Sharia governance structures (Arsyad *et al.*, 2025; Kismawadi *et al.*, 2025). The findings suggest that effective AI governance in Islamic digital finance requires a hybrid model combining technological safeguards with Sharia-based ethical oversight. Such an approach would help institutions manage operational risks while ensuring alignment with Islamic values and

societal expectations. Overall, the findings suggest that AI governance in Islamic digital finance requires the integration of ethical, legal and technological dimensions within context-specific frameworks.

5.6 Toward a multidimensional artificial intelligence risk governance framework

AI-related risks in digital financial systems are layered and interconnected, making them difficult to capture through single-level analytical approaches. While aggregate-level analysis highlights the dominance of governance-related risks, item-level findings reveal concentrated risk nodes, such as cybersecurity vulnerabilities and Sharia compliance issues, that carry disproportionate systemic implications. This pattern reflects the broader complexity of AI-driven financial systems, where risks emerge through interactions among technological, organizational and regulatory domains. The findings support risk governance literature emphasizing interconnected risk structures that require integrated analytical frameworks (Renn, 2017; Aven and Renn, 2018). In digital finance, where AI systems operate within dynamic environments shaped by data flows, institutional practices and regulatory constraints, such complexity becomes particularly significant (Philippon, 2019; Thakor, 2020).

The findings also demonstrate that effective AI governance cannot be reduced to abstract principles or regulatory guidelines alone. Although transparency, accountability and fairness remain essential governance principles (Floridi *et al.*, 2018; Wirtz *et al.*, 2020), their effectiveness depends heavily on institutional capacity for implementation. The identification of governance execution gaps and capability constraints suggests that the challenge of AI governance lies not only in defining standards but also in ensuring their operationalization across organizational contexts. As demonstrated in Islamic digital finance, effective governance must simultaneously address operational risk, regulatory compliance and broader ethical considerations. This reinforces recent arguments that AI governance should be understood as a context-sensitive process that integrates technical, organizational and normative dimensions (Krafft *et al.*, 2020; Batool *et al.*, 2023).

In this regard, the study advances the literature by proposing a multidimensional perspective on AI risk governance in which risk assessment operates across multiple levels of analysis and governance is viewed as an evolving institutional process. Such a perspective enables more precise identification of priority risk areas, supports targeted governance interventions, and strengthens institutional capacity to respond to emerging risks. Overall, the findings suggest that AI governance in digital financial systems should be understood as an ongoing process of alignment among technological innovation, institutional capability, regulatory oversight and ethical expectations. This perspective underscores the importance of adaptive and integrative governance frameworks capable of responding to the evolving nature of AI-related risks.

5.7 Practical and policy implications

The findings provide several implications for policymakers, regulators and financial institutions involved in AI-driven financial systems. The identification of governance-related risks as the dominant source of vulnerability suggests that effective AI governance requires more than technological innovation alone. Institutional readiness, organizational capability and regulatory coordination remain critical for sustainable AI implementation within digital financial ecosystems (Wirtz *et al.*, 2020; Dwivedi *et al.*, 2021).

For policymakers and regulators, the findings highlight the need for integrated AI governance frameworks that combine technological oversight with institutional risk management mechanisms. The identification of cybersecurity vulnerabilities and governance execution gaps suggests that regulatory approaches should move beyond general digital governance principles toward more AI-oriented supervisory mechanisms. These mechanisms include AI governance audit systems, explainability requirements for AI-based decision-making,

periodic algorithmic review procedures, and institutional AI risk assessment standards to strengthen accountability and transparency in automated financial services (Floridi *et al.*, 2018; Zetzsche *et al.*, 2020). Regulatory authorities may also strengthen collaboration among financial regulators, cybersecurity agencies and digital governance institutions to address systemic AI-related risks. Sector-specific AI governance guidelines and supervisory escalation protocols may further improve institutional responsiveness to AI-related failures.

The findings also suggest that institutional capability and human capital development should become central priorities in AI governance strategies. Risks related to limited training, low risk awareness and organizational readiness indicate that many institutions may adopt AI technologies faster than their governance capacity can adapt. Financial institutions should invest in AI literacy programs, professional training and governance mechanisms capable of supporting continuous AI risk monitoring. Establishing dedicated AI governance units, AI ethics and compliance committees, or multidisciplinary oversight teams may improve coordination across technological, legal and operational dimensions of risk management (Rogers, 2003; Venkatesh *et al.*, 2012).

In the context of Islamic digital finance, the findings suggest that AI governance frameworks should address not only operational and regulatory concerns but also ethical and Sharia governance considerations. The identification of Sharia compliance risk highlights the importance of integrating Sharia supervisory functions into AI governance structures, particularly in automated decision-making, digital financing and AI-assisted financial screening processes (Khan, 2025). Institutions may also consider establishing Sharia-AI supervisory mechanisms to ensure that algorithmic decisions remain aligned with ethical and Sharia standards.

More broadly, the findings suggest that AI governance should be approached as a dynamic institutional process rather than a purely technical compliance exercise. The presence of hidden risk concentrations suggests that governance mechanisms must identify localized vulnerabilities before they evolve into systemic failures. In this regard, multilevel risk assessment approaches and institutional AI readiness assessments may provide more adaptive frameworks for managing AI-related risks in rapidly evolving digital financial environments.

6. Conclusion

This study demonstrates that AI governance challenges in digital financial systems extend beyond technological performance alone. The findings suggest that AI-related risks are predominantly governance-driven, with risk management capacity, human capital and Sharia compliance emerging as central dimensions of AI implementation. A central contribution of the study lies in demonstrating that AI risk structures are inherently nonuniform. While aggregate-level analysis identifies governance-related risks as dominant, item-level analysis reveals critical risk concentrations, such as cybersecurity vulnerabilities and Sharia compliance risks, that may be obscured in broader classifications. This finding highlights the importance of multilevel risk assessment for identifying both structural and localized risk hotspots.

The study contributes to the literature by bridging risk governance and AI governance through an empirically grounded framework. By integrating FMEA with multilevel analysis, the study advances existing approaches to AI risk assessment. The study also introduces the concept of a governance execution gap, where awareness of AI-related risks does not always translate into effective mitigation. From a practical perspective, the findings underscore the importance of strengthening institutional capacity as a central component of AI governance. Investments in training, skill development and organizational readiness remain essential for responsible AI implementation. The identification of cybersecurity and Sharia compliance risks further underscores the need for governance mechanisms that align technological systems with regulatory and ethical principles. In the context of Islamic digital finance, the findings further

suggest that AI governance requires a hybrid approach combining technological oversight with Sharia-based ethical governance. This reflects the need to align operational efficiency with normative and religious principles that underpin institutional legitimacy and public trust.

Despite these contributions, several limitations should be acknowledged. First, the use of perception-based survey data may introduce subjectivity into risk evaluations. Second, the analysis is limited to a specific institutional and geographical context, which may limit the generalizability of the findings. Future research could extend this work by incorporating objective performance data, conducting cross-country comparative analyses, or adopting longitudinal approaches to examine how AI-related risks evolve.

References

Arner, D.W., Barberis, J. and Buckley, R.P. (2017), "FinTech and RegTech in a nutshell, and the future in a sandbox", *SSRN Electronic Journal*, doi: 10.2139/ssrn.3088303.

Arsyad, I., Kharisma, D.B. and Wiwoho, J. (2025), "Artificial intelligence and islamic finance industry: problems and oversight", *International Journal of Law and Management*, doi: 10.1108/IJLMA-07-2024-0236.

Aven, T. (2016), "Risk assessment and risk management: review of recent advances on their foundation", *European Journal of Operational Research*, Vol. 253 No. 1, pp. 1-13, doi: 10.1016/j.ejor.2015.12.023.

Aven, T. and Renn, O. (2018), "Improving government policy on risk: eight key principles", *Reliability Engineering & System Safety*, Vol. 176, pp. 230-241, doi: 10.1016/j.ress.2018.04.018.

Batool, A., Zowghi, D. and Bano, M. (2023), "Responsible AI governance: a systematic literature review", arXiv Preprint arXiv:2401.10896, doi: 10.48550/arXiv.2401.10896.

Boateng, R. (2020), *Handbook of Research on Managing Information Systems in Developing Economies*, IGI Global, Hershey, PA.

Broeders, D. and Prenio, J. (2018), "Innovative technology in financial supervision (suptech): the experience of early users, No. 9 ed", Financial Stability Institute/Bank for International Settlements. FSI Insights on policy implementation No. 9, available at: www.bis.org/fsi/publ/insights9.pdf

Demirgüç-Kunt, A., Klapper, L., Singer, D. and Ansar, S. (2022), "The global findex database 2021: Financial inclusion", *Digital Payments, and Resilience in the Age of COVID-19*, World Bank Publications.

Dwivedi, Y.K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., . . . Kizgin, H. (2021), "Artificial intelligence (AI): multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy", *International Journal of Information Management*, Vol. 57, p. 101994, doi: 10.1016/j.ijinfomgt.2019.08.002.

Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., . . . Vayena, E. (2018), "An ethical framework for a good AI society: opportunities, risks, principles, and recommendations", *Minds & Machines*, Vol. 28 No. 4, pp. 689-707, doi: 10.1007/s11023-018-9482-5.

Fuster, A., Goldsmith-Pinkham, P., Ramadorai, T. and Walther, A. (2022), "Predictably unequal? The effects of machine learning on credit markets", *The Journal of Finance*, Vol. 77 No. 1, pp. 5-47, doi: 10.1111/jofi.13090.

Gomber, P., Kauffman, R.J., Parker, C. and Weber, B.W. (2018), "On the fintech revolution: interpreting the forces of innovation, disruption, and transformation in financial services", *Journal of Management Information Systems*, Vol. 35 No. 1, pp. 220-265, doi: 10.1080/07421222.2018.1440766.

Hacker, P., Kasirzadeh, A. and Edwards, L. (2025), "AI, digital platforms, and the new systemic risk", arXiv preprint arXiv:2509.17878, doi: 10.48550/arXiv.2509.17878.

Hair, J.F., Black, J.W., Babin, B.J. and Anderson, R.E. (2019), *Multivariate Data Analysis*, Pearson New International Edition, Harlow, Essex, England.

Iqbal, M.S., Sukamto, F.A., Norizan, S.N., Mahmood, S., Fatima, A. and Hashmi, F. (2025), "AI in islamic finance: global trends, ethical implications, and bibliometric insights", *Review of Islamic Social Finance and Entrepreneurship*, Vol. 4 No. 1, pp. 70-85, doi: 10.20885/RISFE.vol4.iss1.art6.

Jagtiani, J. and Lemieux, C. (2019), "The roles of alternative data and machine learning in fintech lending: evidence from the LendingClub consumer platform", *Financial Management*, Vol. 48 No. 4, pp. 1009-1029, doi: 10.1111/fima.12295.

Karaosman, E., Rizvani, A. and Pekaric, I. (2026), "Security barriers to trustworthy AI-Driven cyber threat intelligence in finance: evidence from practitioners", arXiv Preprint arXiv:2603.23304, doi: 10.48550/arXiv.2603.23304.

Khan, T. (2025), "AI governance for islamic Finance-A dynamic prescriptive approach", *Available at SSRN 5239754*, doi: 10.2139/ssrn.5239754.

Kismawadi, E.R., Irfan, M. and Harahap, I. (2025), "Integrating artificial intelligence in islamic financial management: Opportunities and challenges in maintaining shariah compliance", in Ghosal, I., Gupta, S., Rana, S. and Saha, D. *Indigenous Empowerment through Human-Machine Interactions: The Challenges and Strategies from Business Lenses*, Emerald, London, pp. 273-288, doi: 10.1108/978-1-83608-068-820251016.

Krafft, P.M., Young, M., Katell, M., Huang, K. and Bugingo, G. (2020), "Defining AI in policy versus practice", *AAAI/ACM Conference on AI, Ethics, and Society*, pp. 72-78, 10.1145/3375627.3375835.

Liu, H.C., Liu, L. and Liu, N. (2013), "Risk evaluation approaches in failure mode and effects analysis: a literature review", *Expert Systems with Applications*, Vol. 40 No. 2, pp. 828-838, doi: 10.1016/j.eswa.2012.08.010.

Minaryanti, A.A. and Mihajat, M.I. (2024), "A systematic literature review on the role of sharia governance in improving financial performance in sharia banking", *Journal of Islamic Accounting and Business Research*, Vol. 15 No. 4, pp. 553-568, doi: 10.1108/JIABR-08-2022-0192.

Philippon, T. (2019), "On fintech and financial inclusion, (No. w26330)", National Bureau of Economic Research, doi: 10.3386/w26330.

Rahman, M., Ming, T.H., Baigh, T.A. and Sarker, M. (2023), "Adoption of artificial intelligence in banking services: an empirical analysis", *International Journal of Emerging Markets*, Vol. 18 No. 10, pp. 4270-4300, doi: 10.1108/IJOEM-06-2020-0724.

Renn, O. (2017), *Risk Governance: coping with Uncertainty in a Complex World*, Routledge, London.

Rogers, E. (2003), *Diffusion of Innovations*, 5th Ed. Free Press, New York, NY.

Sain, Z. and Adinugraha, H.H. (2025), "Artificial intelligence and islamic finance: enhancing sharia compliance and social impact in banking 4.0", *Journal of Business Management and Islamic Banking*, Vol. 4 No. 1, pp. 25-46, doi: 10.14421/jbmib.2025.0401-03.

Schiff, D., Borenstein, J., Biddle, J. and Laas, K. (2021), "AI ethics in the public, private, and NGO sectors: a review of a global document collection", *IEEE Transactions on Technology and Society*, Vol. 2 No. 1, pp. 31-42, doi: 10.1109/TTS.2021.3052127.

Scott, W.R. (2013), *Institutions and Organizations: Ideas, Interests, and Identities*, Sage publications, Thousand Oaks, CA.

Stamatis, D.H. (2003), *Failure Mode and Effect Analysis*, Quality Press, Milwaukee, WI.

Teece, D.J. (2018), "Business models and dynamic capabilities", *Long Range Planning*, Vol. 51 No. 1, pp. 40-49, doi: 10.1016/j.lrp.2017.06.007.

Thakor, A.V. (2020), "Fintech and banking: what do we know?", *Journal of Financial Intermediation*, Vol. 41, p. 100833, doi: 10.1016/j.jfi.2019.100833.

Tornatzky, L.G., Fleischer, M., and Chakrabarti, A.K. (1990), *The Processes of Technological Innovation*, Lexington Books, Lexington, MA.

Urbano, D., Aparicio, S., and Audretsch, D.B. (2019), *Institutions, Entrepreneurship, and Economic Performance*, Springer International Publishing, doi: 10.1007/978-3-030-13373-3_1.

Varian, H. (2018), "Artificial intelligence, economics, and industrial organization", in *The Economics of Artificial Intelligence: An Agenda*, University of Chicago Press, Chicago, IL, pp. 399-419, doi: 10.7208/chicago/9780226613475.003.0016.

Venkatesh, V., Thong, J.Y. and Xu, X. (2012), "Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology", *MIS Quarterly*, Vol. 36 No. 1, pp. 157-178, doi: 10.2307/41410412.

Verhoef, P.C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Dong, J.Q., Fabian, N. and Haenlein, M. (2021), "Digital transformation: a multidisciplinary reflection and research agenda", *Journal of Business Research*, Vol. 122, pp. 889-901, doi: 10.1016/j.jbusres.2019.09.022.

Vives, X. (2019), "Digital disruption in banking", AnnualReview of Financial Economics, Vol. 11 No. 1, pp. 243-272, doi: 10.1146/annurev-financial-100719-120854.

Wahab, A.W. and Mahdiya, I. (2025), "Digital shariah governance and the future of islamic finance: a framework for AI-driven shariah compliance in a global regulatory environment", *International Journal of Islamic Finance*, Vol. 3 No. 2, pp. 19-31, doi: 10.14421/ijif.v3i2.2777.

Wirtz, B.W., Weyerer, J.C. and Sturm, B.J. (2020), "The dark sides of artificial intelligence: an integrated AI governance framework for public administration", *International Journal of Public Administration*, Vol. 43 No. 9, pp. 818-829, doi: 10.1080/01900692.2020.1749851.

Zafar, M.B. and Ali, H. (2025), "Shariah governance standard on generative AI for islamic financial institutions", *SSRN*, Vol. 5143165, doi: 10.2139/ssrn.5143165.

Zetzsche, D.A., Arner, D.W. and Buckley, R.P. (2020), "Decentralized finance", *Journal of Financial Regulation*, Vol. 6 No. 2, pp. 172-203, doi: 10.1093/jfr/fjaa010.

Further reading

Gomber, P., Koch, J.A. and Siering, M. (2017), "Digital finance and FinTech: current research and future research directions", *Journal of Business Economics*, Vol. 87 No. 5, pp. 537-580, doi: 10.1007/s11573-017-0852-x.

Liu, H.-C., Chen, X.-Q., Duan, C.-Y. and Wang, Y.-M. (2019), "Failure mode and effect analysis using multi-criteria decision making methods: a systematic literature review", *Computers & Industrial Engineering*, Vol. 135, pp. 881-897, doi: 10.1016/j.cie.2019.06.055.

Corresponding author

Darmawan Darmawan can be contacted at: Darmawan@uin-suka.ac.id