AI-ENABLED FRAMEWORKS FOR STRATEGIC RISK MANAGEMENT: A SYSTEMATIC REVIEW AND MODEL FOR ORGANISATIONAL RESILIENCE AND DECISION-MAKING SUPPORT

By

Ayomide Oluwatobiloba Adesemowo
Southern University College of Business
Harding Blvd, Baton Rouge, Louisiana,
USA 70807 Louisiana, USA

ABSTRACT

With the emergence of a new digital world in the context of the contemporary era of digital transformation and systemic volatility, traditional concepts of strategic risk management have come under increasing challenge due to the inherent complexities of the modern business world. To address these challenges in a volatile world, a new framework has been developed based on concepts from artificial intelligence. The framework has been developed based on a systematic review of the contemporary literature in accordance with the PRISMA 2020 guidelines. A systematic review has been undertaken to examine the contemporary literature on artificial intelligence-based risk management in response to these challenges in a volatile world. The framework has been developed by integrating concepts of artificial intelligence-based analytics, modelling, and adaptive governance in accordance with the organisation's strategic objectives. The framework is grounded in the theoretical foundations of dynamic capabilities and decision support systems. The framework has the potential to address the challenges faced by small and medium-sized enterprises and can be applicable in different sectors of the economy. However, the effectiveness of the framework depends on the availability of high-quality data and the implementation of responsible artificial intelligence principles in a digital world. The framework has addressed the gap between theory and practice, developing a robust approach to responding to these challenges in a volatile world. The framework has the potential to benefit technology and governance leaders in developing artificial intelligence-based organisational resilience capabilities in a digital world and to offer sustainable strategic benefits across developed and emerging economies.

KEYWORDS: Artificial Intelligence (AI); Strategic risk management; Organisational resilience; Decision support system (DSS); Corporate governance; Dynamic capabilities; Volatile, uncertain, complex, and ambiguous (VUCA) world)

INTRODUCTION

In the present world, where volatility is on the rise, digital transformation is changing the way businesses operate, and the world is becoming increasingly interconnected, risk management is key to the success and resilience of businesses and organisations. This is because traditional approaches to risk management, which are often reactive and judgment-based, are failing to address the complexities of risks such as cybersecurity, supply chain, and market volatility [1, 2]. In the present world, technological shifts are occurring at an incredible rate, and the business environment is constantly changing, further emphasising the need for innovative tools that support strategic decision-making while ensuring corporate governance [3, 4].

In this context, AI, with its ability to process vast amounts of data, recognise emerging trends, and support adaptive learning, is poised to revolutionise the way risk management is perceived while ensuring alignment with organisational objectives [5, 6]. This is because AI-based approaches to risk management can reduce decision biases, enable real-time risk identification, and improve accuracy in the face of volatility, uncertainty, complexity, and ambiguity [7]. Despite the potential benefits of AI in strategic risk management, challenges related to algorithmic transparency, bias, and ethics underscore the need for frameworks that support the effective integration of AI while ensuring corporate governance [8, 9].

In this context, this study proposes an innovative AI-based strategic risk management framework to ensure organisational resilience while supporting strategic decision-making. This study is also aimed at contributing to the broader fields of corporate governance, DSS, dynamic capabilities, organisational resilience, AI, strategic risk management, and decision support systems.

https://doi.org/10.56578/jimd040304

governance, and technology management. The framework presented in this work differs from other sector-based studies [10, 11] in that it offers a scalable solution applicable across sectors, particularly for SMEs and high-risk industries [4, 12]. The present work's results highlight the benefits of this framework in improving strategic alignment, anticipating future risks through predictive analytics, and promoting resilience, thus offering useful insights for organisations operating in today's complex business environment.

Literature Review AI in Strategic Risk Management

The application of AI in strategic risk management has revolutionised the ability of firms to thrive in VUCA environments. AI has improved firms' resilience, decision-making, and governance. This systematic literature review (SLR) examines scholarly publications and industry reports from 2019 to 2024 to explore the application, challenges, and gaps of AI in strategic risk management. The review identifies the potential of AI to transcend the limitations of conventional risk management and the need to develop a comprehensive, governance-based model.

Conceptual Frameworks for AI-Driven Risk Management

Several researchers have proposed conceptual models for incorporating AI into strategic risk management, emphasising data-driven decision-making and strategic alignment.

Carayannis et al. [4] proposed a framework for small and medium-sized enterprises (SMEs), which combined AI-based predictive analytics and strategic foresight to build resilience. The framework, however, fails to incorporate ERM systems. Zigiene˘ et al. [13] proposed a framework for managing supply chain risks in SMEs, which relies on analytics to mitigate external risks. The proposed model fails to incorporate governance. Bussmann et al. [1] proposed an XAI-based framework for fintech companies to improve decision-making, but the proposed models lack universal application. Lopez-Sol´ ´ıs et al. [7] proposed the application of generative AI in scenario planning, but the proposed model fails to consider AI risks like bias. Biloslavo et al. [3] proposed applying AI to strategic planning in VUCA environments, but their model lacks an integrated governance approach.

The proposed models highlight the potential of AI for strategic risk management, but their lack of integration underscores the need for an integrated model.

Practical Applications of AI in Strategic Risk Management

Further, the applied studies demonstrate the potential of AI for decision-making and resilience-building across different sectors. Javaid [6] discusses the potential of predictive analytics in real-time risk identification in the financial sector, but the algorithmic risks are not addressed. Adeoye et al. [10] discuss the application of AI in the oil and gas sector's HSE system, where risks are mitigated but governance is not addressed. Kalisetty et al. [2] and Kassa et al. [12] discuss the role of AI in building supply chain resilience, but their studies are limited to the sectoral level. Milojevic and Redzepagic [´ 14] discuss the assessment of the role of AI in building banking compliance, but the potential is not addressed from the perspective of SMEs. Bi and Bao [11] discuss the potential of AI in financial risk management, but this potential is not addressed from the enterprise perspective.

In the above studies, the potential of AI is examined across different sectors, and the absence of standardised frameworks is noted.

Organisational and Implementation Challenges

The potential of AI is also associated with certain organizational and implementation challenges, especially from the perspective of governance, the availability of resources, and transparency. Habbal et al. [8] introduced the AI TRiSM framework to address the algorithmic risks, but the strategic potential is not addressed. Novelli et al. [15] discussed regulatory ambiguity, particularly regarding the EU AI Act, where strong governance is required. Stahl et al. [9] discussed transparency challenges in the impact assessment of AI, which are important from the perspective of stakeholders. Maghfirah and Eni [16] discussed the potential organisational challenges, particularly regarding resource availability, especially in SMEs.

These challenges underscore the absence of a practical, governance-based framework that balances AI's analytical capabilities with scalability and ethical considerations [17].

Gaps in the Current Literature

The literature identifies several gaps that underscore the need for a comprehensive framework. First, very few studies have empirically validated the long-term effectiveness of AI-based risk models, which are largely theoretical and sector-specific [10, 11]. Second, despite the significance of SMEs in the economy, very little research has explored the challenges and opportunities of implementing AI-based solutions in these sectors [13, 16]. Third, most existing frameworks are not aligned with ERM standards such as ISO 31000 [1]. Finally, the debate over ethical trade-offs, such as transparency, bias, and AI-related risks, is also limited [8, 18].

Synthesis

The synthesis of the literature confirms AI's potential to transform strategic risk management and decision-making. Although several frameworks and applications have shown promise in enhancing decision-making and governance, their fragmented, sector-specific nature has limited adoption and scalability. The challenges of implementing these solutions are also significant and include bias, resource constraints, and changing regulations. The absence of empirical validation of these solutions, solutions for SMEs, and their alignment with existing ERM standards underscores the need for a robust, governance-based framework that is scalable and practical. Such a framework will bridge the gap between AI innovation and practical organisational application.

Methodology

This SLR utilises the SLR methodology to search for existing literature on the application of AI in strategic risk management. An original conceptual framework will be developed to support organisational resilience and enhance corporate governance.

Research Questions

This SLR is informed by four research questions:

- **RQ_1.** How does AI transform the traditional risk management function to support strategic decision-making?
- **RQ_2.** What are the main frameworks for the application of AI in strategic risk management?
- **RQ_3.** What challenges are encountered in the application of AI in strategic risk management?
- **RQ_4.** What are the main implications for the application of AI in strategic decision-making?

This SLR is informed by the PRISMA 2020 guidelines to ensure methodological rigour and transparency in the search, selection, and synthesis of the included literature [9].

Data

To ensure the SLR is exhaustive, the data sources included relevant and credible sources such as Scopus, Web of Science, IEEE Xplore, and ACM Digital Library. High-quality grey literature sources, such as OECD and NIST reports, were also included [8].

To ensure the SLR is exhaustive, the search strings included relevant keywords such as "artificial intelligence," "machine learning," "predictive analytics," "risk management," and "strategic resilience," among others [7].

In this SLR, the eligibility criteria included:

- Only sources published in the English language between 2019 and 2024;
- Peer-reviewed journal articles, conference papers, book chapters, and credible industry reports;
- Only sources focusing on the application of AI in strategic organisational risk management.

In this SLR, the exclusion criteria included:

- Non-empirical sources such as editorials and opinions;
- Technical sources focusing on the application of AI;
- Inaccessible sources.

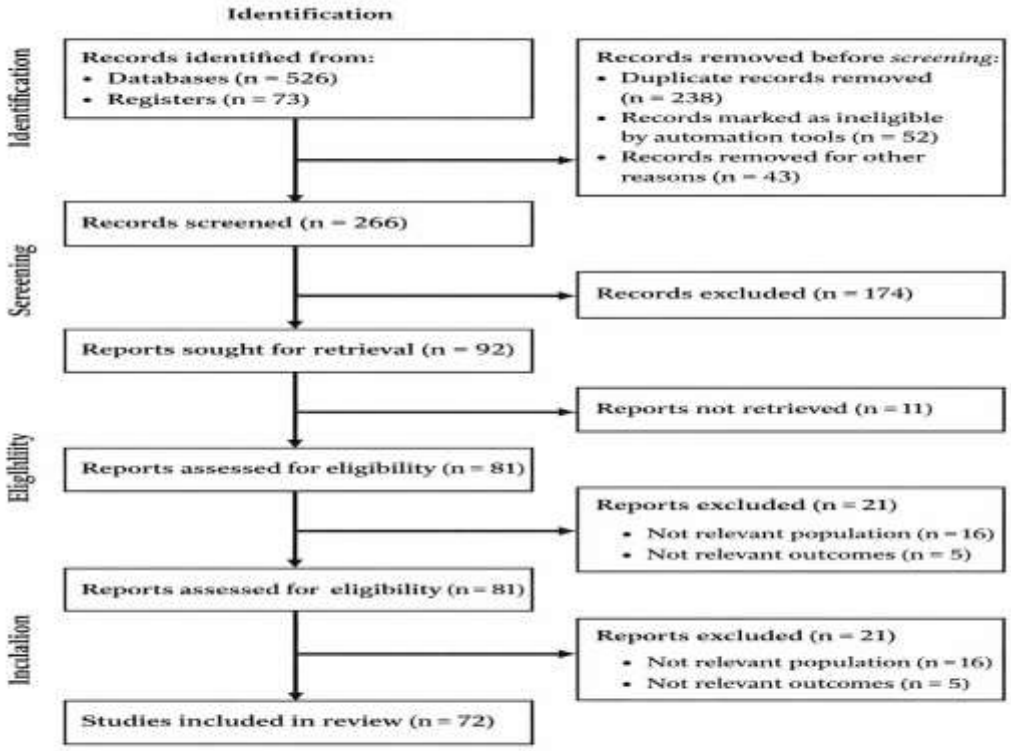

Figure 1. PRISMA 2020 flow diagram
Source: Based on PRISMA 2020 guidelines

This selection process was carried out using Zotero for reference management. Discrepancies were addressed through discussions among the researchers to ensure objectivity [1].

Methodological rigour is ensured using tools such as the CASP checklist for qualitative studies, bias assessment for quantitative studies, and the AMSTAR-2 tool for systematic reviews [19].

A detailed overview of the systematic selection process is illustrated in Figure 1 using the PRISMA 2020 flow diagram.

Results

This section presents the findings of the SLR on the application of AI in strategic risk management, with particular emphasis on its transformative role in enhancing organizational resilience and decision support within the context of corporate governance. The SLR, which synthesises 72 studies published between 2019 and 2024, seeks to address four research questions on the transformative role of AI in the following areas: the role of AI in transforming traditional risk management, the role of AI in

transforming primary frameworks, the challenges associated with the adoption of AI, and the role of AI in strategic decision-making. The findings are presented under four themes: trends in AI risk management studies; the distribution of AI applications across sectors and risk domains; the capabilities of AI approaches; and the challenges with the preliminary framework components. These findings lay the groundwork for the development of the novel AI-based strategic risk management framework.

Trends in AI Risk Management Research

SLR highlights a steady increase in research on the application of AI in risk management from 2019 to 2024. This is a growing trend as there is a rising academic and industry interest in applying AI in risk management in terms of strategic resilience, governance, and decision-making [4]. Most of these research papers focus on research related to predictive analytics, AI-based governance tools, and applications related to volatility and complexity in today's business world [15, 20].

To better illustrate the trend in AI risk management research in a visual format, Figure 2 illustrates the trend in terms of types of research papers and a steady increase in peer-reviewed journal articles, conference papers, and high-quality industry reports.

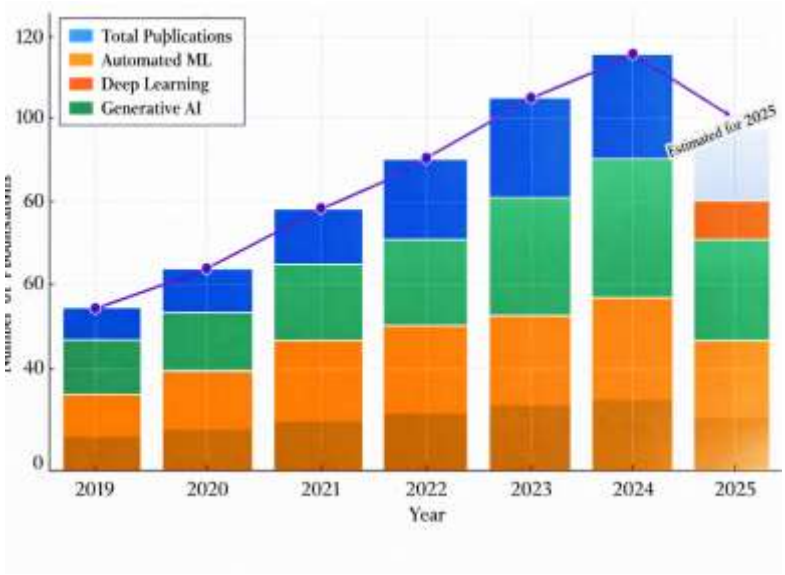

Figure 2. Publication trends in AI and risk management (2019–2024) by publication type
Source: Developed by the authors using illustrative data

This increasing body of work only serves to highlight the need for a unified and practical AI framework that can help to integrate these disparate approaches.

Distribution of AI Applications across Sectors and Risk Domains

The distribution of AI application across sectors and risk domains varies. The financial services industry leads, with a focus on cybersecurity and financial risk management, driven by data-rich environments and regulatory needs, respectively. The energy industry follows, with emerging interest in sustainability and operational risks. Supply chain management and healthcare are other areas with increasing application, albeit constrained by resource availability in smaller sectors like manufacturing and retail. Cybersecurity and financial risks dominate, but strategic risk management remains an under-explored area, indicating an unmet need in the area of integrated enterprise-wide AI application.

Comparative Capabilities of AI Approaches

The review identifies and compares the capabilities of three main AI approaches: traditional machine learning, deep learning, and generative AI, in terms of their ability to deliver core strategic risk management capabilities.

- Traditional machine learning is strong in explainability and system integration, which are critical in compliance-driven activities [1].
- Deep learning is strong in terms of predictive accuracy, which is critical in risk monitoring activities, thanks to its superior pattern recognition capabilities [6].
- Generative AI is strong in adaptability, which is critical in decision support activities, but its weakness in explainability may hinder its adoption in highly regulated environments [5, 8].

The unique advantages of these three AI technologies suggest that no single technology is adequate in dealing with strategic risks in isolation from other technologies. Rather, a unified framework where these technologies are integrated would provide a more holistic solution to meet the complex needs of risk management leaders who seek a balance of accuracy, agility, transparency, and governance.

Figure 3 visually corroborates this analysis through a comparative analysis of how these three AI technologies individually perform in terms of eight critical dimensions in strategic risk management activities, as depicted in a radar chart below:

Figure 3. Comparative capabilities of AI approaches for risk management
Source: Developed by the authors based on SLR

Preliminary Framework Components Identified in the Literature

SLR identifies five key components which are generally regarded as integral to supporting the adoption of AI in strategic risk management. Even though these components are identified in different industries, they are generally implemented individually without a holistic framework. This synthesis will provide a foundation for a more universal and integrated framework.

(1) Strategic Governance: This involves developing guidelines, ethics, and governance structures to align AI with organizational objectives and regulatory guidelines [15].

(2) Dynamic Risk Assessment: This concept is associated with processes for recognizing and evaluating risks using AI-based predictive analytics and modeling techniques [6].

(3) Technical Controls: This concept is associated with processes for validating, auditing, and detecting biases in data to ensure system reliability, accuracy, and trust [8].

(4) Human Oversight: This concept emphasizes human judgment, training, and ethics in relation to using AI automation while ensuring accountability [19].

(5) Continuous Improvement: This concept emphasizes using feedback mechanisms and adaptive learning to enhance AI tools and governance processes over time [4].

Even though these concepts are generally identified in the literature, they are generally not implemented in a holistic framework, which is critical in supporting organizations, especially those with limited resources, in realizing the full potential of AI in managing strategic risks.

Figure 4 below represents how these five interrelated components are integrated, according to literature findings.

Figure 4: Five Interrelated Components of Strategic Risk Management with AI

Figure 4. Proposed AI-based strategic risk management framework (synthesis from SLR)
Source: Developed by the authors based on SLR

Persistent Challenges In AI-Driven Risk Management

Despite the potential of the suggested framework, there are some challenges that persist in the implementation of the framework in risk management, particularly for SMEs and resource-constrained industries.

(1) Data Quality and Availability: Most organizations have issues related to data availability. Lack of data availability can impact the accuracy of the risk prediction carried out by AI [13, 16].

(2) Regulatory Compliance: New regulations, such as the EU AI Act, have raised issues of updating the risk management governance. Most organizations are not equipped to handle such issues [15].

(3) Explainability and Transparency: Most of the advanced techniques in risk management, such as deep learning or generative AI, are not transparent. Lack of transparency in risk management has raised issues in terms of approval from concerned authorities [1].

(4) Shortage of Technical Expertise: Most organizations lack the required expertise in risk management. Lack of expertise in risk management has raised issues of engaging external experts for risk management [19].

(5) Security Vulnerabilities: Most of the techniques in risk management, such as AI, have raised security issues. Most of the security issues in risk management have raised concerns related to data poisoning [8].

These challenges have highlighted that, despite the identification of essential components of risk management in the literature, there is a need for a more integrated approach in risk management, which is lacking in the current literature.

As such, Table 1 has been presented to highlight the major risk types along with the mitigation strategies:

Table 1. AI risk types and mitigation strategies

Risk Type	Mitigation Strategy	Source
Data Quality Issues	Implement robust data validation protocols	Zigiene et al. (2022) [13]
Regulatory Non-Compliance	Develop adaptive governance policies	Novelli et al. (2023) [15]
Lack of Explainability	Use explainable AI models for critical tasks	Bussmann et al. (2020) [1]
Expertise Shortage	Invest in workforce training and partnerships	Ferrara (2024) [19]
Security Vulnerabilities	Apply encryption and secure model deployment	Habbal et al. (2024) [8]

Source: Developed by the authors

Summary of Key Findings

This SLR demonstrates that there is a clear increase in research on using AI in strategic risk management, which is a significant indicator of its importance in risk management and governance, especially in a VUCA environment [4].

The key findings of this SLR are:

(1) Rising Research Interest: There has been a steady increase in research on using AI in risk management from 2019 to 2024, which indicates its importance in risk management and governance, especially in a VUCA environment [4].

(2) Narrow Sector Focus: There is a narrow focus on using AI in risk management in the finance and cybersecurity sectors, while there is little research on using AI in other sectors, especially in SMEs, which are highly vulnerable to risks and have a lack of AI resources [6].

(3) Isolated Use of AI Capabilities: There are many types of AI, such as machine learning, deep learning, and generative AI, which have unique capabilities, such as accuracy, explainability, and flexibility, respectively. However, these capabilities are rarely integrated with other capabilities in a holistic manner [5].

(4) Persistent Adoption Barriers: There are still many barriers to using AI in risk management, such as data quality, regulatory issues, transparency, a lack of skills, and increased security issues, which are still obstacles to using AI in risk management, especially in SMEs, which have a lack of resources [13, 15].

(5) Scattered Framework Components: There are many studies on using AI in risk management, which discuss key components such as governance, risk assessment, and human oversight, but they are rarely integrated under a single framework applicable to many sectors [8].

These insights collectively highlight the need for a framework that brings these aspects together in a single strategy, particularly for SMEs. The framework presented in the next section addresses this need by presenting a more pragmatic solution that bridges theory and implementation.

Discussion

This systematic review has validated that although the transformative potential of AI in SRM is becoming more widely accepted, current applications are fragmented and predominantly concentrated

in industries such as finance and cybersecurity [6, 14]. The lack of sectoral diversity in current SRM has resulted in a considerable gap in the development of a more holistic, intersectoral approach that brings AI into SRM in a strategic management context, particularly for organizations operating in a VUCA environment.

To address this shortfall in current SRM, the current study proposes an original framework for AI-Driven Strategic Risk Management that brings disparate insights from the literature together in a single framework. Unlike most other SRM models that are predominantly technical in nature, sector-specific, or limited to risk compliance, such as the NIST framework for AI Risk Management or the finance-focused framework by Bi and Bao [11], the framework presented in this paper brings predictive, explanatory, and generative capabilities of AI together in a single framework that is focused on governance. Ayomide Oluwatobiloba Adesemowo

Figure 5. Proposed AI-driven strategic risk management framework
Source: Developed by the authors

Figure 5 displays the proposed framework with its six interdependent components: Strategic Governance, Dynamic Risk Assessment, Technical Controls, Human Oversight, Continuous Improvement, and Stakeholder Engagement. As depicted, the components work together to create a cohesive framework that supports real-time risk identification, ethical oversight, and improvement. As discussed, the main function of the Strategic Governance is to set the direction and scope for the application of AI. It enables the identification of risks in advance through Dynamic Risk Assessment. Technical Controls ensure the integrity of the technology, while Human Oversight ensures transparency and accountability. Continuous Improvement utilises feedback loops to adapt to the evolving landscape of threats and technology, and Stakeholder Engagement is essential to fostering trust through openness and inclusivity (Adesemowo, 2022).

Table 2 is included to further clarify the strategic role played by each component in the proposed framework. It is included to ensure the reader understands the model's application in aligning the adoption and application of AI with organisational objectives, evolving regulatory requirements, and the requirements of key stakeholders.

Table 2. Framework components and strategic contributions

Component	Description	Strategic Contribution	Key References
Strategic Governance	Establishes policies and guidelines that align AI adoption with organisational goals, compliance requirements, and ethical standards	Promotes strategic fit, legal compliance, and responsible AI deployment	Novelli et al. (2024); Milojevic and Redzepagic (2021)
Dynamic Risk Assessment	Uses AI-driven systems to identify, monitor, and predict risks in real time	Improves early warning capacity, proactive risk management, and scenario planning	Javaid (2024); Adeoye et al. (2024)
Technical Controls	Involves data validation, bias detection, model testing, and audit mechanisms	Strengthens the accuracy, reliability, and trustworthiness of AI systems	Habbal et al. (2024)
Human Oversight	Integrates human judgment, staff training, and ethical supervision into AI-supported processes	Ensures accountability, balances automation with human reasoning, and reduces misuse	Ferrara (2024)
Continuous Improvement	Applies feedback loops, monitoring, and adaptive learning to refine AI models over time	Supports long-term resilience, efficiency, and system refinement	Carayannis et al. (2024)
Stakeholder Engagement	Encourages transparent communication, accountability, and participation of key stakeholders in AI use	Builds stakeholder trust, legitimacy, and reputational protection	Bussmann et al. (2020)

Source: Developed by the authors based on synthesis of reviewed studies

Originality of the Framework

This research is original in the sense that it provides a new framework for strategic risk management using AI techniques. It is original because it incorporates the following innovations:

- Integrated Approach: Unlike other studies, which focus on one aspect of the field, this research provides a unified model. It incorporates governance, technology, and human factors.
- Balanced AI Capabilities: It incorporates the advantages of machine learning, deep learning, and generative AI. These techniques can be combined to achieve the benefits of prediction, flexibility, and explainability.
- Practical and Scalable: It is applicable to both large companies and SMEs.

Implications

Theoretical Implications

This research extends several theoretical approaches to strategic management and organizational theory:

- Decision-Making Theory: It shows how AI can reduce the negative effects of human cognitive biases and improve strategic sense-making in uncertain environments.
- Resource-Based View: It shows how AI can be considered not only as a resource but also as a dynamic data-driven resource, which can support sustainable competitive advantage.
- Dynamic Capabilities Theory: It shows how AI can support the organization's ability to sense, seize, and transform in the context of emerging threats.

Practical Implications

This research provides a clear roadmap to the practical application of the framework. It is useful to both practitioners and companies. It provides the following steps for the application of the framework:

- Each part of the framework is discussed with particular advice for SMEs.
- Metrics to measure the success of the application.
- Strategic Governance: Organizations must develop strategies that govern the alignment of AI with organisational objectives and regulatory requirements, such as the EU AI Act or OECD AI Principles. SMEs can use open-source governance tools such as OpenGov or work with compliance consultants to develop such strategies. Key Performance Indicator (KPI): Percentage of AI initiatives compliant with regulatory standards (100% compliance desired).
- Dynamic Risk Assessment: Organizations must assess risks through the use of predictive analytics tools. SMEs can utilize cloud-based tools such as Google Cloud AI or Amazon SageMaker, which are cost-effective. Key Performance Indicator (KPI): Reduction in time taken to detect critical risks (e.g., from weeks to mere hours).
- Technical Controls: Organizations must develop technical controls to ensure the reliability of AI systems. SMEs can utilize open-source tools such as TensorFlow Model Analysis to assess bias in predictive models. Key Performance Indicator (KPI): Percentage of AI models audited for bias and accuracy (100% quarterly desired).
- Human Oversight: Organizations must develop strategies to ensure that AI is aligned with organizational objectives through the use of human oversight. SMEs can utilize free online courses such as Coursera's AI Ethics to develop basic knowledge about AI. Key Performance Indicator (KPI): Number of employees who undergo training in AI ethics annually (at least 80% desired).
- Continuous Improvement: Organizations must develop strategies to continuously improve AI tools as risks evolve. SMEs can start with basic feedback mechanisms such as reviewing AI predictions against actual outcomes on a monthly basis. Key Performance Indicator (KPI): Number of AI model updates through the use of feedback mechanisms (at least one update desired every quarter).
- Stakeholder Engagement: Communicate AI strategies transparently to gain trust from customers, regulators, and employees. SMEs can achieve this through frequent updates or a public dashboard showing progress in risk management. KPI: Stakeholder Trust Score, measured through surveys to achieve 75% positive feedback.

Practical Guidance for SMEs: Implementing the AI-Based Strategic Risk Management Framework

To guide SMEs in implementing the proposed AI-Based Strategic Risk Management Framework, this section includes a set of steps to follow in implementing the framework, specifically designed for a resource-constrained environment. Although SMEs might not have the luxury of advanced technical infrastructure and human capital in AI, they can still benefit from the availability of free or low-cost tools and incremental implementation strategies.

Table 3 offers specific actions to take, free or low-cost tools to consider, and related KPIs for each of the six components of the proposed AI-Based Strategic Risk Management Framework.

Table 3. Step-by-step implementation overview for SMEs

Framework Dimension	Practical Actions for SMEs	Affordable Tools and Resources	Performance Indicators
Strategic Governance	Develop a simple AI use policy that supports business objectives and complies with basic legal and ethical	OECD AI guidance, NIST AI Risk	Percentage of AI activities meeting legal and ethical requirements

	requirements	Management Framework	
Dynamic Risk Assessment	Identify major business risks and use predictive tools to monitor likely threats using existing business data	Google Cloud AI, Microsoft Azure AI, Amazon SageMaker	Reduction in time taken to identify and respond to major risks
Technical Controls	Prepare and clean data, test models for bias, and routinely validate outputs for accuracy and reliability	OpenRefine, Fairlearn, TensorFlow Model Analysis	Percentage of AI models reviewed for bias, security, and reliability each quarter
Human Oversight	Train responsible staff in AI basics and assign clear roles for reviewing AI-supported decisions	Google AI learning resources, Coursera AI Ethics courses	Percentage of key staff trained in AI governance and oversight
Continuous Improvement	Conduct regular monthly reviews and refine AI systems based on feedback and performance outcomes	Google Data Studio, Power BI, SageMaker retraining tools	Frequency of model updates and measurable improvement in model performance
Stakeholder Engagement	Maintain transparent communication about AI use with customers, employees, and other stakeholders	Google Forms, Slack, Mailchimp	Stakeholder trust and satisfaction scores from periodic feedback surveys

Source: Author

Limitations and Directions for Future Research

Despite the theoretical depth and integrative innovation of the proposed framework, some limitations have also been identified that will serve as directions for future research and practical refinement:

(1) Sectoral Concentration

The current review relies heavily on the finance and cybersecurity domains because AI risk management applications in these fields are highly mature. This may affect the applicability of the framework in other sectors such as manufacturing, public services, and healthcare. Future research directions include applying and validating the framework in these relatively unexplored sectors through comparative case studies to assess its applicability and effectiveness across different operational contexts.

(2) Emerging AI Developments

The literature review is based on studies published through 2024 and may not have captured the latest developments in hybrid intelligent systems and other advanced generative AI tools. Given the rapid pace of development in AI and intelligent systems, future research directions include updating the framework to incorporate the latest developments in these fields, thereby maintaining its relevance and practical value for organisational strategies and decision-making.

(3) Lack of Empirical Validation

The proposed framework is based on a comprehensive synthesis of existing literature and is conceptual in nature. While this provides a strong theoretical foundation for the framework, it is essential to take the next step and validate it through empirical research. Future research directions include piloting the framework in different organisational contexts, especially in high-risk industries and SMEs. The methodologies for such studies may include a combination of qualitative and quantitative research approaches and analysis of performance metrics for effectiveness and efficiency in reducing risk exposure, enhancing the effectiveness of scenario planning and risk detection tools, and so forth.

Future research will thus empirically validate this framework in less-researched areas, such as public administration, sustainability risks, and SME governance, while further advancing the investigation of other ethical issues, such as bias mitigation and algorithmic accountability, to encourage responsible AI adoption.

CONCLUSIONS

This research offers a novel AI-based strategic risk management framework, which was developed through a thorough SLR methodology on existing literature from 2019 to 2024. The proposed framework combines six interrelated elements: Strategic Governance, Dynamic Risk Assessment, Technical Controls, Human Oversight, Continuous Improvement, and Stakeholder Engagement, which are designed to support proactive, data-driven decision-making in VUCA environments.

The framework offers a number of advantages over other risk management frameworks that are either industry-specific or technology-centric, as it is universally applicable, especially for SMEs, which are often not in a position to implement cutting-edge AI governance systems. By bridging these fragmented approaches and aligning AI capabilities with enterprise-level objectives, this framework responds to a growing call for a more holistic and responsible integration of AI in risk governance.

This research contributes to the development of strategic management theory by extending decision-making theory through AI-based bias reduction, extending the RBT through a dynamic capability perspective on AI, and extending DCT through its support for organisations to sense, seize, and adapt to new risks.

The research, although conceptually robust, has several limitations, including its focus on existing literature in the finance sector and its failure to empirically validate its framework. However, this research provides a solid foundation for future research.

Future studies will seek to extend this framework through empirical validation across a range of industries, regions, and regulatory environments, with a particular focus on SMEs and ethical AI governance.

Ultimately, this framework can provide helpful recommendations for organisations that wish to utilise the transformative potential of AI to build strategic resilience, make better decisions, and cultivate stakeholder trust, creating a foundation for more flexible, resilient, and ethical risk management in an ever-more complex world.

REFERENCES

[1] Khandani, A. E., Kim, A. J., & Lo, A. W. (2010). Consumer credit-risk models via machine-learning algorithms. *Journal of Banking & Finance, 34*(11), 2767–2787.

[2] Lessmann, S., Baesens, B., Seow, H.-V., & Thomas, L. C. (2015). Benchmarking state-of-the-art classification algorithms for credit scoring: An update of research. *European Journal of Operational Research, 247*(1), 124–136.

[3] Arsić, V. B. (2021). Challenges of financial risk management: AI applications. *Management: Journal of Sustainable Business and Management Solutions in Emerging Economies, 26*(3), 1–10.

[4] Fritz-Morgenthal, S., Hein, B., & Papenbrock, J. (2022). Financial risk management and explainable, trustworthy, responsible AI. *Frontiers in Artificial Intelligence, 5*, 779799.

[5] Barredo Arrieta, A., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., ... Herrera, F. (2020). Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion, 58*, 82–115.

[6] Rai, A. (2020). Explainable AI: From black box to glass box. *Journal of the Academy of Marketing Science, 48*(1), 137–141.

[7] Rudin, C. (2019). Stop explaining black box machine learning models for high-stakes decisions and use interpretable models instead. *Nature Machine Intelligence, 1*(5), 206–215.

[8] Leo, M., Sharma, S., & Maddulety, K. (2019). Machine learning in banking risk management: A literature review. *Risks, 7*(1), 29.

[9] Min, H. (2010). Artificial intelligence in supply chain management: Theory and applications. *The International Journal of Logistics Research and Applications, 13*(1), 13–39.

[10] Baryannis, G., Validi, S., Dani, S., & Antoniou, G. (2019). Supply chain risk management and artificial intelligence: State of the art and future research directions. *International Journal of Production Research, 57*(7), 2179–2202.

[11] Ivanov, D., & Dolgui, A. (2020). Viability of intertwined supply networks: Extending the supply chain resilience angles towards survivability. *International Journal of Production Research, 58*(10), 2904–2915.

[12] Shrestha, Y. R., Ben-Menahem, S. M., & von Krogh, G. (2019). Organizational decision-making structures in the age of artificial intelligence. *California Management Review, 61*(4), 66–83.

[13] Dwivedi, Y. K., Kshetri, N., Hughes, L., Slade, E. L., Jeyaraj, A., Kar, A. K., ... Wright, R. (2023). "So what if ChatGPT wrote it?" Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI for research, practice and policy. *International Journal of Information Management, 71*, 102642.

[14] Raji, I. D., Smart, A., White, R. N., Mitchell, M., Gebru, T., Hutchinson, B., ... Barnes, P. (2020). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. In *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* (pp. 33–44).

[15] Veale, M., & Borgesius, F. Z. (2021). Demystifying the draft EU Artificial Intelligence Act. *Computer Law Review International, 22*(4), 97–112.

[16] Brynjolfsson, E., Li, D., & Raymond, L. R. (2023). Generative AI at work. *National Bureau of Economic Research Working Paper* No. 31161.

[17] Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems, 50*(3), 559–569.

[18] Glikson, E., & Woolley, A. W. (2020). Human trust in artificial intelligence: Review of empirical research. *Academy of Management Annals, 14*(2), 627–660.

[19] Mehrabi, N., Morstatter, F., Saxena, N., Lerman, K., & Galstyan, A. (2021). A survey on bias and fairness in machine learning. *ACM Computing Surveys, 54*(6), 115.

[20] Varshney, K. R. (2019). Trustworthy machine learning and artificial intelligence. *XRDS: Crossroads, The ACM Magazine for Students, 25*(3), 26–29.

[21] Adesemowo, A.O. (2022). Investment in the health sector and macroeconomic performance in the US: an empirical investigation. 1990-2022. Southern University and A&M College of Business. and TIJANI, Nureni Abayomi.