Journal of Intelligent Management Decision
https://www.acadlore.com/journals/JIMD

AI–Driven Frameworks for Strategic Risk Management: A Systematic Review and Model for Organizational Resilience and Decision Support

Khalid Zeriouh[1*], Mehdi Amara[2]

[1] Department of Management and Entrepreneurship, Higher National School of Management, 42003 Kolea, Algeria
[2] Laboratory of Research and Economic Studies, Mohamed Cherif Messaadia University, 41043 Souk Ahras, Algeria

* Correspondence: Khalid Zeriouh (zeriouhkhalid@gmail.com)

Received: 06-20-2025 **Revised:** 07-27-2025 **Accepted:** 08-05-2025

Citation: K. Zeriouh and M. Amara, "AI–driven frameworks for strategic risk management: A systematic review and model for organizational resilience and decision support," *J. Intell Manag. Decis.*, vol. 4, no. 3, pp. 224–234, 2025. https://doi.org/10.56578/jimd040304.

Abstract: In an era defined by digital transformation and systemic volatility, conventional approaches to strategic risk management have been increasingly challenged by the complexity and unpredictability of modern operational environments. To address these limitations, a novel artificial intelligence (AI)–driven framework has been developed to enhance organizational resilience and optimize strategic decision-making. Constructed through a systematic review conducted in accordance with PRISMA 2020 guidelines, this study synthesizes current academic literature and industry publications to identify critical enablers, practical gaps, and methodological advancements in AI-enabled risk governance. The proposed framework integrates real-time analytics, predictive modelling, and adaptive governance mechanisms, aligning them with enterprise-wide strategic objectives to support decision-making under volatile, uncertain, complex, and ambiguous (VUCA) conditions. Anchored in dynamic capabilities theory and decision support systems (DSS) literature, the framework is designed to facilitate proactive risk anticipation, reduce cognitive and algorithmic biases in decision-making, and foster strategic alignment in rapidly evolving contexts. Its adaptability to small and medium-sized enterprises (SMEs), as well as its cross-sectoral relevance, underscores its scalability and practical utility. Nonetheless, the effectiveness of the framework is contingent upon the availability of high-quality data, the level of digital maturity within organizations, and the implementation of responsible AI principles. By bridging the gap between theoretical innovation and real-world applicability, this study contributes a robust foundation for future empirical validation and sector-specific customization. The framework is expected to inform governance and technology leaders aiming to institutionalize AI-based resilience capabilities, thereby supporting sustainable strategic outcomes in both developed and emerging markets.

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

1 Introduction

In an era of escalating volatility, digital disruption, and growing global interconnectedness, effective risk management has become pivotal to ensuring organizational success and resilience across industries. Yet, traditional approaches, often reactive and reliant on subjective judgment, increasingly struggle to address complex, interconnected risks such as cybersecurity threats, supply chain disruptions, and market uncertainties [1, 2]. The rapid pace of technological change and dynamic business environments further underscore the urgent need for innovative tools that strengthen strategic decision-making and corporate governance [3, 4].

AI, with its capacity to process vast amounts of data, identify emerging patterns, and enable adaptive learning, holds transformative potential to redefine risk management and align it with broader enterprise objectives [5, 6]. Unlike conventional risk frameworks, AI-driven approaches can reduce decision biases, enable real-time risk detection, and enhance precision in VUCA contexts [7]. However, challenges such as algorithmic opacity, data bias, and ethical concerns highlight the need for robust frameworks that guide responsible and transparent AI integration [8, 9].

Addressing this gap, this study proposes an original AI-based strategic risk management framework designed to enhance organizational resilience and support informed decision-making, while contributing to the fields of corporate

governance and technology management. Unlike existing sector-specific studies [10, 11], the proposed framework provides a scalable, cross-sectoral solution, with particular relevance for SMEs and high-risk industries [4, 12]. The findings demonstrate how this approach improves strategic alignment, anticipates emerging risks through predictive analytics, and fosters resilience, thereby offering actionable insights for organizations navigating today's complex business landscape.

2 Literature Review

AI in Strategic Risk Management

The integration of AI into strategic risk management is transforming how organizations navigate VUCA environments. AI enhances resilience, improves decision-making, and strengthens corporate governance. This systematic literature review (SLR) synthesizes peer-reviewed studies and industry reports (2019–2025), examining conceptual frameworks, practical applications, implementation challenges, and current gaps. It highlights AI's potential to overcome traditional risk management limitations while identifying the need for a unified, governance-oriented framework.

Conceptual Frameworks for AI-Driven Risk Management

Several recent studies propose conceptual models that integrate AI into strategic risk management, with a shared emphasis on data-driven decision-making and strategic alignment.

Carayannis et al. [4] offer a framework for SMEs that merges AI-driven predictive analytics with strategic foresight to enhance resilience, though it lacks integration with enterprise risk management (ERM) systems. Žigiene et al. [13] focus on supply chain risk for SMEs using analytics to manage external threats but omit governance elements. Bussmann et al. [1] introduce explainable AI (XAI) frameworks for fintech to improve transparency, yet these lack applicability across sectors. López-Solís et al. [7] explore generative AI in scenario planning but overlook AI-specific risks such as bias. Biloslavo et al. [3] advocate for AI in strategic planning within VUCA environments, although their model requires more explicit governance integration.

Together, these frameworks reflect AI's transformative potential but remain fragmented, reinforcing the need for a more integrated model that aligns AI use with governance and strategic objectives.

Practical Applications of AI in Strategic Risk Management

Applied studies further demonstrate AI's ability to improve decision-making and resilience across various industries. Javaid [6] shows how predictive analytics enable real-time risk identification in finance, though without addressing algorithmic risks. Adeoye et al. [10] apply AI in oil and gas HSE systems, mitigating operational risks, but highlight the need for structured governance. Kalisetty et al. [2] and Kassa et al. [12] examine AI's role in enhancing supply chain resilience, but their findings are limited by sectoral focus. Milojević and Redzepagic [14] assess AI's use in banking compliance, yet provide limited insight into SME adoption. Bi and Bao [11] demonstrate the value of AI in financial risk management, enhancing data-driven insights, though without extending to enterprise-wide integration.

These applications confirm AI's potential but also reveal the absence of standardized, cross-sectoral frameworks to guide responsible and scalable implementation [5].

Organizational and Implementation Challenges

Despite its potential, integrating AI into strategic risk management presents several challenges, particularly around governance, resource availability, and transparency. Habbal et al. [8] introduce the AI Trust, Risk, and Security Management (AI TRiSM) framework to address algorithmic bias, data quality, and human oversight, yet it lacks strategic application. Novelli et al. [15] highlight regulatory ambiguity, such as the EU AI Act, requiring robust governance structures. Stahl et al. [9] underscore transparency challenges in AI impact assessments, which are critical for stakeholder trust. Maghfirah and Eni [16] point to common resource constraints, especially for SMEs, such as limited data infrastructure and technical capacity.

These barriers highlight the absence of a practical, governance-based framework that balances AI's analytical strengths with scalability and ethical responsibility [17].

Gaps in the Current Literature

The literature reveals several critical gaps that underscore the need for a comprehensive framework. First, few studies empirically validate the long-term effectiveness of AI-based risk models, as many remain theoretical or sector-specific [10, 11]. Second, while SMEs are central to many economies, their unique constraints and adoption contexts remain underexplored [13, 16]. Third, most frameworks lack alignment with established ERM standards such as ISO 31000, limiting practical utility [1]. Lastly, discussions on ethical trade-offs such as transparency, bias, and AI-related vulnerabilities are still limited [8, 18].

These gaps signal the need for a scalable, cross-sectoral AI framework that integrates strategic governance, operational feasibility, and responsible AI principles.

Synthesis

This review affirms AI's transformative potential for strategic risk management, enhancing decision support, resilience, and governance. While several frameworks and applications show promise, their fragmented and sector-

specific nature limits broader adoption. Implementation challenges such as bias, resource limitations, and evolving regulations further complicate integration. The lack of empirical validation, SME-focused solutions, and standardized ERM alignment emphasizes the need for a robust, governance-oriented framework that is both scalable and practical. Such a model can bridge the gap between AI innovation and responsible organizational implementation, contributing meaningfully to both academic literature and professional practice.

3 Methodology

This study employs an SLR to identify and synthesize existing research on the integration of AI into strategic risk management. The goal is to develop an original conceptual framework that supports organizational resilience and strengthens corporate governance.

3.1 Research Questions

The review is guided by four research questions:

- RQ1. How does AI transform traditional risk management to support strategic decision-making?
- RQ2. What are the primary frameworks for integrating AI into strategic risk management?
- RQ3. What challenges arise in adopting AI for strategic risk management?
- RQ4. What practical implications do AI-driven approaches offer for strategic decision-makers?

The review process follows the PRISMA 2020 guidelines, ensuring methodological rigor and transparency in identifying, screening, and synthesizing relevant literature [9]. Both descriptive and thematic analyses were conducted to interpret the findings, with particular emphasis on practical frameworks, technological enablers, governance challenges, and directions for future research [4].

3.2 Data

To ensure comprehensive coverage, data were collected from multiple reputable sources, including Scopus, Web of Science, IEEE Xplore, and ACM Digital Library, and supplemented by high-quality gray literature such as OECD and NIST reports [8]. Search strings combined keywords such as "artificial intelligence," "machine learning," "predictive analytics," "risk management," and "strategic resilience," adapted using Boolean operators and database-specific syntax [7].

Inclusion criteria were:

- English-language publications from 2019 to 2025;
- Peer-reviewed journal articles, conference proceedings, book chapters, and reputable industry reports;
- Studies addressing AI in strategic or organizational risk management contexts.

Exclusion criteria included:

- Non-empirical opinion pieces and editorials;
- Technical AI studies without managerial relevance;
- Inaccessible full texts.

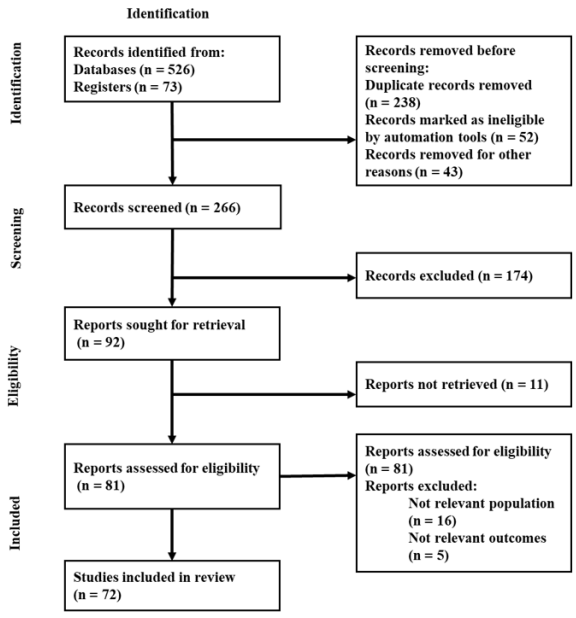

Figure 1. PRISMA 2020 flow diagram
Source: Based on PRISMA 2020 guidelines

The selection process was managed using Zotero for reference management, with discrepancies resolved through discussion among the researchers to ensure objectivity [1]. Methodological rigor was assessed using tools such as the CASP checklist for qualitative studies, bias assessments for quantitative research, and AMSTAR-2 for existing reviews [19].

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

4 Results

This section presents findings from an SLR examining AI in strategic risk management, focusing on its transformative role in enhancing organizational resilience and decision support within corporate governance frameworks. The SLR, synthesizing 72 studies from 2019 to 2025, addresses four research questions: how AI transforms traditional risk management, primary frameworks, adoption challenges, and practical implications for strategic decision-makers. Findings are organized into four themes: trends in AI risk management research, distribution of AI applications across sectors and risk domains, comparative capabilities of AI approaches, and challenges with preliminary framework components. These findings highlight gaps and opportunities, laying the foundation for a novel AI-based strategic risk management framework.

Trends in AI Risk Management Research

SLR highlights a steady rise in research on the use of AI in risk management between 2019 and 2025. This growing trend reflects increasing academic and industry interest in using AI to enhance strategic resilience, governance, and decision-making [4]. Many of these studies focus on predictive analytics, AI-based governance tools, and applications that address volatility and complexity in today's business environment [15, 20].

To visually capture this evolution, Figure 2 presents the publication trends by type, showing a notable increase in peer-reviewed journal articles, conference papers, and high-quality industry reports. The figure supports the textual analysis by illustrating the shift from technical AI discussions to more strategic, governance-oriented studies.

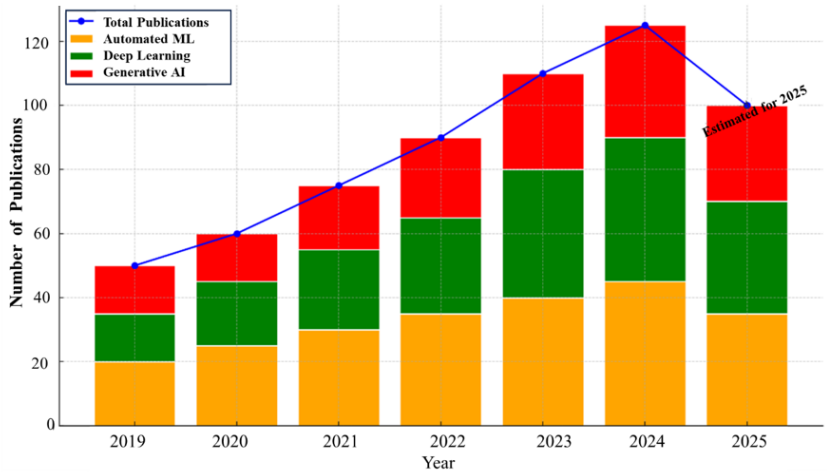

Figure 2. Publication trends in AI and risk management (2019–2025) by publication type

Source: Developed by the authors using illustrative data

This growing body of work reinforces the need for a unified and practical AI framework that can connect fragmented approaches and guide implementation across sectors.

Distribution of AI Applications Across Sectors and Risk Domains

AI applications vary across sectors and risk domains. Financial services lead, with a focus on cybersecurity and financial risk management, driven by data-rich environments and regulatory demands [6, 14]. The energy sector shows emerging interest in sustainability and operational risks [10], while supply chain management and healthcare are growing, though limited by resource constraints in smaller sectors like manufacturing and retail [2, 16]. Cybersecurity and financial risks dominate, but strategic risk management remains underexplored, highlighting a gap in enterprise-wide AI applications [1, 8].

Comparative Capabilities of AI Approaches

The review compares three major AI approaches - traditional machine learning, deep learning, and generative AI- across core strategic risk management capabilities: predictive accuracy, risk assessment, monitoring, explainability, adaptability, and decision support.

• Traditional machine learning performs well in explainability and system integration, making it ideal for compliance-driven tasks and regulated environments [1].

• Deep learning excels in predictive accuracy and complex risk monitoring due to its advanced pattern recognition capabilities [6].

• Generative AI offers strong adaptability and decision support, particularly in scenario planning and simulation. However, it poses challenges in explainability, which may limit its use in highly regulated sectors [5, 8].

These distinct yet complementary strengths suggest that no single AI approach is sufficient for managing strategic risks in isolation. Instead, an integrative framework that combines these technologies can better address the diverse needs of risk leaders balancing accuracy, agility, transparency, and governance.

Figure 3 visually supports this analysis by comparing how each AI method performs across eight key dimensions relevant to strategic risk management. The radar chart demonstrates their individual strengths and highlights areas where they can be most effectively applied or combined.

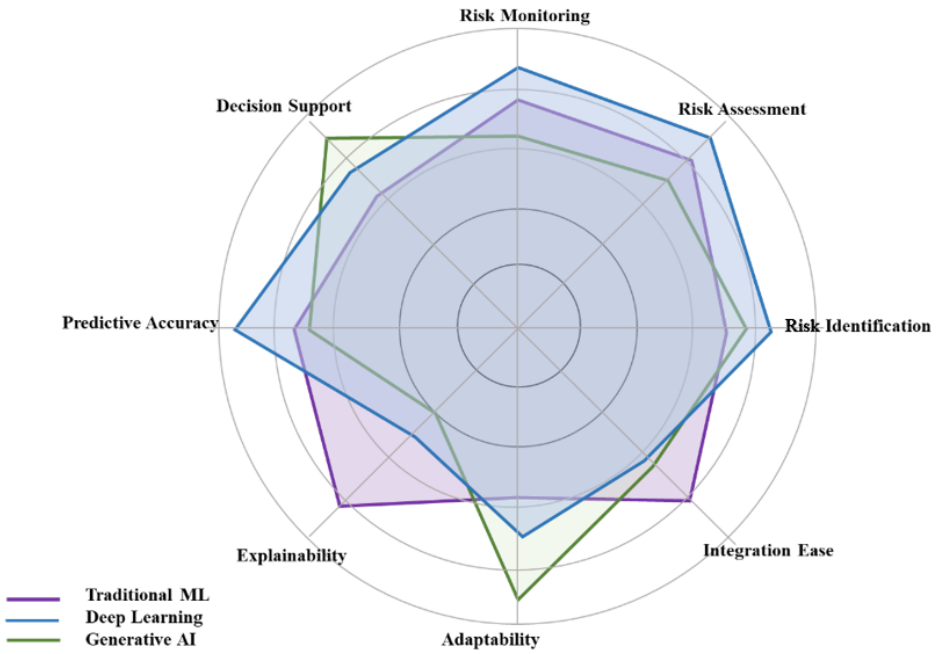

Figure 3. Comparative capabilities of AI approaches for risk management

Source: Developed by the authors based on SLR

Preliminary Framework Components Identified in the Literature

SLR identifies five core components commonly proposed to support AI adoption in strategic risk management. Although these elements emerge across various sectors, they are often applied in isolation, without integration into a holistic framework. This synthesis lays the groundwork for a more scalable and unified approach.

(1) **Strategic Governance**: Involves defining clear policies, ethical guidelines, and oversight structures to align AI initiatives with organizational goals and regulatory standards [15].

(2) **Dynamic Risk Assessment**: Refers to systematic processes for identifying and evaluating emerging risks using AI-powered predictive analytics and scenario modelling [6].

(3) **Technical Controls**: Focuses on data validation, model auditing, and bias detection to ensure system reliability, accuracy, and trust [8].

(4) **Human Oversight**: Stresses the role of human judgment, training, and ethical awareness to complement AI automation and maintain accountability [19].

(5) **Continuous Improvement**: Encourages the use of feedback loops and adaptive learning to refine AI tools and governance practices over time [4].

Although widely acknowledged, these components are rarely combined into a strategic, cross-sectoral model. Integrating them cohesively is essential for organizations, especially those with limited resources, to fully realize AI's potential in managing strategic risks.

Figure 4 illustrates how these five interdependent components interact, based on findings from the literature. The visual aid supports understanding by positioning the components in a connected system rather than isolated functions.

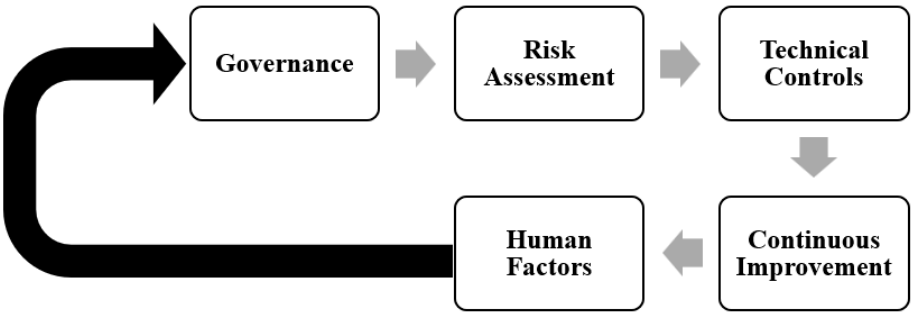

Figure 4. Proposed AI-based strategic risk management framework (synthesis from SLR)
Source: Developed by the authors based on SLR

Persistent Challenges in AI-Driven Risk Management

Despite the promise of the proposed framework, several persistent challenges still limit the effective use of AI in strategic risk management, particularly for SMEs and resource-constrained sectors.

(1) **Data Quality and Availability**: Many organizations struggle with incomplete, fragmented, or poorly governed data. This weakens the reliability and accuracy of AI predictions [13, 16].

(2) **Regulatory Compliance**: Changing regulations such as the EU AI Act require ongoing updates to governance practices. This poses difficulties for organizations without strong legal or compliance capacity [15].

(3) **Explainability and Transparency**: Advanced AI models like deep learning or generative AI often operate as "black boxes." Their lack of interpretability reduces stakeholder trust and makes regulatory approval more challenging [1].

(4) **Shortage of Technical Expertise**: Many firms lack the internal skills needed to design, maintain, and oversee AI systems, leading to a reliance on costly external consultants or technology partners [19].

(5) **Security Vulnerabilities**: AI systems face new security risks, including data poisoning or adversarial attacks, which require advanced safeguards not yet widely adopted [8].

These challenges show that while academic research has identified essential components, it still falls short of offering a fully integrated and actionable roadmap, especially for organizations across different sectors or with limited resources.

To address this gap, Table 1 summarizes the main risk types along with practical mitigation strategies proposed in the literature:

Table 1. AI risk types and mitigation strategies

Risk Type	Mitigation Strategy	Source
Data Quality Issues	Implement robust data validation protocols	Žigienė 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 shows that interest in using AI for strategic risk management has grown significantly. However, its real-world application is still uneven and fragmented. Key findings include:

(1) **Rising Research Interest**: From 2019 to 2025, there has been a steady increase in studies on AI in risk management, highlighting its importance for resilience and governance, especially in VUCA environments [4].

(2) **Narrow Sector Focus**: Most applications focus on finance and cybersecurity. Broader, cross-sector use, especially for SMEs, remains limited despite their high exposure to risk and lack of AI resources [6].

(3) **Isolated Use of AI Capabilities**: Different AI types (e.g., machine learning, deep learning, generative AI) offer unique strengths like accuracy, explainability, or adaptability. Yet, these are often used separately, not combined in an integrated way [5].

(4) **Persistent Adoption Barriers**: Poor data quality, regulatory uncertainty, lack of transparency, limited skills, and growing security risks continue to block effective use, especially in low-resource organizations like SMEs [13, 15].

(5) **Scattered Framework Components**: Many studies refer to core elements like governance, risk assessment, and human oversight. But they are rarely unified into one practical, cross-sectoral model [8].

Together, these insights show the need for a clear, scalable framework that combines these elements into a single strategy especially one suited to SMEs. The framework proposed in the next section responds to this gap by offering a more practical, integrated solution that connects theory with implementation.

5 Discussion

This systematic review confirms that although the transformative potential of AI in strategic risk management is increasingly recognized, existing applications remain fragmented and heavily concentrated in sectors such as finance and cybersecurity [6, 14]. This narrow sectoral focus has left a significant gap in enterprise-wide, cross-sectoral approaches that integrate AI within strategic governance, especially for organizations operating in VUCA environments.

To address this shortfall, the present study proposes an original AI-Driven Strategic Risk Management Framework that unifies disparate insights from the literature into a scalable, practical structure. Unlike traditional models that are primarily technical, sector-specific, or limited to compliance, such as the NIST AI Risk Management Framework or the finance-oriented model by Bi and Bao [11], this framework integrates predictive, explanatory, and generative AI capabilities into a governance-driven system. It is designed to be flexible and adaptable across industries and organizational sizes, including SMEs with limited digital resources.

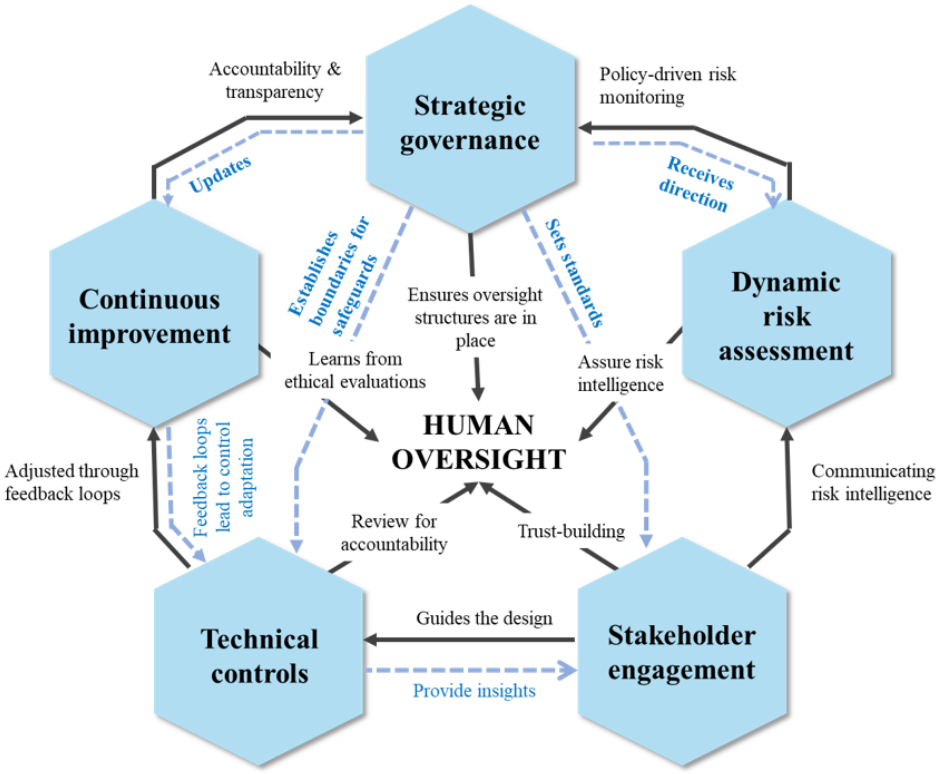

Figure 5. Proposed AI-driven strategic risk management framework

Source: Developed by the authors

Figure 5 presents the proposed framework and its six interdependent components: Strategic governance, dynamic risk assessment, technical controls, human oversight, continuous improvement, and stakeholder engagement. Together, these components form a cohesive system that supports real-time risk identification, ethical oversight, and iterative improvement. Strategic Governance sets direction and boundaries for AI use, enabling proactive risk identification through Dynamic Risk Assessment. Technical Controls safeguard system integrity, while Human Oversight ensures transparency and accountability. Continuous Improvement uses feedback loops to adapt to evolving threats and technologies, and Stakeholder Engagement builds trust through open communication and inclusivity.

Table 2 further clarifies the strategic contributions of each component, illustrating how they collectively align AI adoption with organizational objectives, evolving regulatory requirements, and the expectations of key stakeholders. By providing a concise mapping between framework components and their strategic functions, Table 2 enhances understanding of how this model bridges AI capabilities with enterprise-wide governance and resilience goals.

Table 2. Framework components and strategic contributions

Component	Description	Strategic Contribution	Key References
Strategic Governance	Policies aligning AI with objectives and compliance	Ensures regulatory alignment and strategic fit	Novelli et al. (2024) [15]; Milojević & Redzepagic (2021) [14]
Dynamic Risk Assessment	Real-time predictive risk identification	Supports proactive threat anticipation and scenario planning	Javaid (2024) [6]; Adeoye et al. (2024) [10]
Technical Controls	Data validation, bias detection, and model auditing	Enhances reliability and trustworthiness	Habbal et al. (2024) [8]
Human Oversight	Training, ethical guidelines, and human judgment integration	Balances automation with human insights and accountability	Ferrara (2024) [19]
Continuous Improvement	Feedback loops and adaptive learning mechanisms	Drives long-term resilience and refinement	Caravannis et al. (2025) [4]
Stakeholder Engagement	Transparent communication and accountability frameworks	Builds stakeholder trust and mitigates reputational risks	Bussmann et al. (2020) [1]

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

5.1 Originality of the Framework

This study presents a new AI-driven framework for strategic risk management with three key advances:

• Integrated Approach: The framework brings together governance, technology, and human factors into a single, unified model. While previous studies often focus on one aspect or a specific industry, this framework offers a more complete and cross-sectoral roadmap.

• Balanced AI Capabilities: It combines the strengths of traditional machine learning, deep learning, and generative AI. This allows for better prediction, greater flexibility, and improved explainability, key features often missing when only one method is used.

• Practical and Scalable: The framework is flexible enough for large corporations but also suitable for SMEs, which often face resource and expertise limitations.

5.2 Implications

5.2.1 Theoretical implications

This study extends several streams of strategic management and organizational theory:

• Decision-Making Theory: Demonstrates how AI mitigates human cognitive biases and enhances strategic sensemaking under high uncertainty.

• Resource-Based View: Positions AI not merely as a tool, but as a dynamic, data-driven capability that can reinforce sustained competitive advantage when embedded in robust governance and risk structures.

• Dynamic Capabilities Theory: Shows how AI strengthens an organization's capacity to sense, seize, and transform in response to emerging threats, creating adaptive resilience.

5.2.2 Practical implications

For practitioners, the framework offers a clear, actionable roadmap to deploy AI as a strategic enabler of resilience and decision-making. Below, we outline practical steps for each component, with specific guidance for SMEs and metrics to evaluate success.

• Strategic Governance: Organizations should establish policies aligning AI with business objectives and regulations like the EU AI Act or OECD AI Principles. For SMEs, this could involve adopting open-source governance templates or partnering with compliance consultants to ensure regulatory fit. Key Performance Indicator (KPI): Percentage of AI initiatives compliant with regulatory standards (target: 100% compliance).

• Dynamic Risk Assessment: Use predictive analytics to identify risks in real time, such as supply chain disruptions or cybersecurity threats. SMEs can leverage affordable cloud-based tools like Google Cloud AI or Amazon SageMaker to implement predictive models. KPI: Reduction in time to detect critical risks (e.g., from weeks to hours).

• Technical Controls: Implement data validation, bias detection, and model auditing to ensure AI reliability. For example, SMEs can use open-source tools like TensorFlow Model Analysis to monitor bias in predictive models. KPI: Percentage of AI models audited for bias and accuracy (target: 100% quarterly audits).

• Human Oversight: Train staff on AI ethics and integrate human judgment to balance automation. SMEs can access free online courses (e.g., Coursera's AI Ethics) to build basic AI literacy. KPI: Number of employees trained in AI ethics annually (target: at least 80% of relevant staff).

• Continuous Improvement: Use feedback loops to refine AI tools as risks evolve. SMEs can start with simple feedback mechanisms, like monthly reviews of AI predictions versus actual outcomes. KPI: Number of AI model updates based on feedback (target: at least one update per quarter).

• Stakeholder Engagement: Communicate AI strategies transparently to build trust with customers, regulators, and employees. SMEs can engage stakeholders through regular updates or public dashboards showing risk management progress. KPI: Stakeholder trust score, measured via surveys (target: 75% positive feedback).

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

To support SMEs in adopting the proposed AI-Based Strategic Risk Management Framework, this section offers a step-by-step implementation guide tailored to resource-constrained environments. While SMEs may lack extensive technical infrastructure or specialized AI teams, they can still benefit from lightweight, affordable tools and incremental adoption strategies.

Table 3 provides practical actions, suggested free or low-cost tools, and KPIs for each of the six framework components. This structured approach enables SMEs to translate the framework into operational steps that improve strategic decision-making, resilience, and regulatory compliance.

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

Framework Component	Key Actions for SMEs	Suggested Tools (Free/Low Cost)	SME KPIs
Strategic Governance	Draft a lightweight AI use policy aligned with business goals and basic regulations	OECD AI templates, NIST AI RMF	% of AI activities compliant with legal/ethical standards
Dynamic Risk Assessment	Identify key strategic risks and apply pre-built predictive models to existing data	Google Cloud AI, Azure AI, Amazon SageMaker	Time reduction in detecting critical risks
Technical Controls	Clean datasets, audit models for bias, and validate outputs regularly	OpenRefine, Fairlearn, TensorFlow Model Analysis	% of models audited for bias/security quarterly
Human Oversight	Train key staff on AI basics and assign decision-review responsibilities	Google's AI for Everyone, Coursera (AI Ethics)	% of relevant staff trained in AI oversight
Continuous Improvement	Establish monthly feedback reviews to refine AI tools based on outcomes	Google Data Studio, Power BI, SageMaker, retraining tools	Frequency of model updates and performance tuning
Stakeholder Engagement	Communicate AI-related practices to stakeholders through transparent channels	Google Forms, Slack, Mailchimp	Stakeholder trust score via periodic surveys

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

5.4 Limitations and Directions for Future Research

While the proposed framework offers theoretical depth and integrative innovation, several limitations suggest directions for future research and practical refinement:

(1) Sectoral Concentration

The current review draws heavily from finance and cybersecurity domains, where AI applications in risk management are most mature. This focus may limit the framework's immediate generalizability to other sectors such as manufacturing, public services, or healthcare. Future studies should apply and evaluate the framework in these underexplored sectors using comparative case studies to test its adaptability and effectiveness in diverse operational contexts.

(2) Emerging AI Developments

The review covers literature up to 2025, and may not fully capture the most recent advancements in hybrid intelligence systems or advanced generative AI tools. As AI technologies evolve rapidly, ongoing research should focus on updating the framework to reflect these technological shifts, ensuring its continued relevance and strategic value.

(3) Lack of Empirical Validation

While the proposed framework is grounded in a robust synthesis of the existing literature, it remains conceptual at this stage. To enhance its practical relevance and credibility, empirical validation is a necessary next step. Future

research should aim to pilot the framework in real-world organizational settings—particularly in high-risk industries and SMEs. Suitable methodologies may include mixed-method approaches, combining qualitative interviews with practitioners, quantitative surveys across diverse sectors, and performance metric analyses. Such evaluations could assess outcomes like reductions in risk exposure, improvements in scenario planning effectiveness, and faster detection of emerging threats. These validation efforts will be essential in translating the framework from a theoretical contribution into a practical tool for strategic decision-making and organizational resilience.

Future research should therefore empirically validate the framework in underexplored areas like public administration, sustainability risks, and SME governance, while also deepening the examination of ethical dimensions such as bias mitigation and algorithmic accountability to promote responsible AI adoption.

6 Conclusions

This study presents an original AI-based strategic risk management framework, developed through a rigorous SLR covering research published between 2019 and 2025. The proposed framework integrates six interdependent components - Strategic Governance, Dynamic Risk Assessment, Technical Controls, Human Oversight, Continuous Improvement, and Stakeholder Engagement - to support proactive, data-driven decision-making in VUCA environments.

Unlike existing sector-specific or technically focused models, this framework offers cross-sectoral relevance and practical scalability, particularly for SMEs that often lack the resources to implement advanced AI governance systems. By bridging fragmented approaches and aligning AI capabilities with enterprise-wide goals, the framework responds to growing demands for more holistic and responsible AI integration in risk governance.

The study also contributes to strategic management theory by enhancing decision-making theory through AI-enabled bias reduction, extending the resource-based view by framing AI as a dynamic capability, and reinforcing dynamic capabilities theory by enabling organizations to sense, seize, and adapt in response to emerging risks.

Despite its conceptual strength, the study acknowledges certain limitations, including a focus on finance-sector literature and the absence of empirical validation. Nonetheless, it lays a solid foundation for future research. Subsequent studies should empirically test and refine the framework across various industries, regions, and regulatory environments, with particular attention to SME adoption and ethical AI governance.

Ultimately, this framework offers actionable guidance for organizations aiming to harness AI's transformative power to strengthen strategic resilience, improve decision-making, and build stakeholder trust, laying the groundwork for more agile, robust, and ethically grounded risk management in an increasingly complex world.

Data Availability

The data used to support the research findings are available from the corresponding author upon request.

Conflicts of Interest

The authors declare no conflict of interest.

References

[1] N. Bussmann, P. Giudici, D. Marinelli, and J. Papenbrock, "Explainable AI in fintech risk management," *Front. Artif. Intell.*, vol. 3, p. 26, 2020. https://doi.org/10.3389/frai.2020.00026

[2] S. Kalisetty, C. Pandugula, and G. Mallesham, "Leveraging artificial intelligence to enhance supply chain resilience: A study of predictive analytics and risk mitigation strategies," *J. Artif. Intell. Big Data*, vol. 3, no. 1, pp. 29–45, 2023. https://doi.org/10.31586/jaibd.2023.1202

[3] R. Biloslavo, D. Edgar, E. Aydin, and C. Bulut, "Artificial intelligence (AI) and strategic planning process within VUCA environments: A research agenda and guidelines," *Manag. Decis.*, 2024. https://doi.org/10.1108/MD-10-2023-1944

[4] E. G. Carayannis, R. Dumitrescu, T. Falkowski, G. Papamichail, and N. R. Zota, "Enhancing SME resilience through artificial intelligence and strategic foresight: A framework for sustainable competitiveness," *Technol. Soc.*, vol. 81, p. 102835, 2025. https://doi.org/10.1016/j.techsoc.2025.102835

[5] S. Feuerriegel, J. Hartmann, C. Janiesch, and et al., "Generative AI," *Bus. Inf. Syst. Eng.*, vol. 66, pp. 111–126, 2024. https://doi.org/10.1007/s12599-023-00834-7

[6] H. A. Javaid, "AI-driven predictive analytics in finance: Transforming risk assessment and decision-making," *Adv. Comput. Sci.*, vol. 7, no. 1, p. 204, 2024.

[7] O. López-Solís, A. Luzuriaga-Jaramillo, M. Bedoya-Jara, J. Naranjo-Santamaría, D. Bonilla-Jurado, and P. Acosta-Vargas, "Effect of generative artificial intelligence on strategic decision-making in entrepreneurial business initiatives: A systematic literature review," *Adm. Sci.*, vol. 15, no. 2, p. 66, 2025. https://doi.org/10.3390/admsci15020066

[8] A. Habbal, M. K. Ali, and M. A. Abuzaraida, "Artificial intelligence trust, risk and security management (AI TRiSM): Frameworks, applications, challenges and future research directions," *Expert Syst. Appl.*, vol. 240, p. 122442, 2024. https://doi.org/10.1016/j.eswa.2023.122442

[9] B. C. Stahl, J. Antoniou, N. Bhalla, and et al., "A systematic review of artificial intelligence impact assessments," *Artif. Intell. Rev.*, vol. 56, pp. 12 799–12 831, 2023. https://doi.org/10.1007/s10462-023-10420-8

[10] T. A. Adeoye, H. C. Olisakwe, Y. A. Adebayo, and A. E. Esiri, "AI-driven HSE management systems for risk mitigation in the oil and gas industry," *Compr. Res. Rev. Eng. Technol.*, vol. 2, no. 1, pp. 1–22, 2024. https://doi.org/10.57219/crret.2024.2.1.0059

[11] S. Bi and W. Bao, "Innovative application of artificial intelligence technology in bank credit risk management," *Int. J. Glob. Econ. Manag.*, vol. 2, no. 3, pp. 76–81, 2024. https://doi.org/10.62051/ijgem.v2n3.08

[12] A. Kassa, D. Kitaw, U. Stache, B. Beshah, and G. Degefu, "Artificial intelligence techniques for enhancing supply chain resilience: A systematic literature review, holistic framework, and future research," *Comput. Ind. Eng.*, vol. 186, p. 109714, 2023. https://doi.org/10.1016/j.cie.2023.109714

[13] G. Žigienė, E. Rybakovas, R. Vaitkienė, and V. Gaidelys, "Setting the grounds for the transition from business analytics to artificial intelligence in solving supply chain risk," *Sustainability*, vol. 14, p. 11827, 2022. https://doi.org/10.3390/su141911827

[14] N. Milojević and S. Redzepagic, "Prospects of artificial intelligence and machine learning application in banking risk management," *J. Cent. Bank. Theory Pract.*, vol. 10, no. 3, pp. 41–57, 2021.

[15] C. Novelli, F. Casolari, A. Rotolo, M. Taddeo, and L. Floridi, "Taking AI risks seriously: A new assessment model for the AI act," *AI & Soc.*, vol. 39, no. 5, pp. 2493–2497, 2024.

[16] P. Maghfirah and Y. Eni, "The impact of artificial intelligence (AI) adoption on the productivity of small and medium enterprises (SMEs) industries in Indonesia: High cost, lack of knowledge, and inadequate infrastructure as mediation variables," *Int. J. Bus. Manag. Econ. Rev.*, vol. 7, pp. 128–145, 2024. https://doi.org/10.35409/ijbmer.2024.3584

[17] R. Kopperapu, "Harnessing AI and machine learning for enhanced fraud detection and risk management in financial services," *SSRN*, 2024. https://doi.org/10.2139/ssrn.5104927

[18] N. Montealegre-López, "Exploring the role of trust in AI-driven decision-making: A systematic literature review," *Manag. Rev. Q.*, 2025. https://doi.org/10.1007/s11301-025-00526-4

[19] E. Ferrara, "Fairness and bias in artificial intelligence: A brief survey of sources, impacts, and mitigation strategies," *Sci*, vol. 6, no. 1, p. 3, 2024. https://doi.org/10.3390/sci6010003

[20] P. Giudici, M. Centurelli, and S. Turchetta, "Artificial intelligence risk measurement," *Expert Syst. Appl.*, vol. 235, p. 121220, 2024. https://doi.org/10.1016/j.eswa.2023.121220