

Managing Emerging Artificial Intelligence Risks through Enterprise Risk Management, Risk Governance, and Risk Leadership: A Conceptual Framework for Health Insurance Organizations

Rafyanti Widyarini¹, Franciskus Antonius Alijoyo²

Master of Management Sekolah Tinggi Manajemen Asuransi Trisakti

¹rafyantiwidyarini@gmail.com, ²franciskus.antonius.alijoyo63@gmail.com

Abstract

The adoption of Artificial Intelligence (AI) in health insurance organizations has significantly transformed core operational processes such as underwriting, claims management, fraud detection, and customer analytics. While AI enhances efficiency and decision-making accuracy, it simultaneously introduces emerging risks that are complex, dynamic, and difficult to manage using traditional risk management approaches. These risks include algorithmic bias, lack of transparency, data privacy breaches, model drift, and increasing organizational dependency on automated decision systems. This study develops a conceptual framework for managing emerging AI risks in health insurance organizations through the integration of Enterprise Risk Management (ERM), risk governance, and risk leadership. The research employs a qualitative conceptual approach supported by a structured literature synthesis of Scopus-indexed journals and authoritative institutional reports. The theoretical foundation is grounded in COSO ERM (2017), ISO 31000:2018, and the NIST Artificial Intelligence Risk Management Framework (2023), complemented by recent literature on AI governance and risk leadership in high-stakes industries. The findings suggest that effective management of AI-related risks requires a multi-layered approach. Enterprise Risk Management provides a structured mechanism for risk identification, assessment, and mitigation. Risk governance ensures accountability, regulatory compliance, and ethical oversight in AI deployment. Meanwhile, risk leadership plays a critical role in shaping organizational culture, promoting ethical awareness, and ensuring cross-functional alignment in decision-making processes. The integration of these three dimensions forms a comprehensive framework that enhances organizational resilience in managing AI-driven uncertainties in the health insurance sector.

Keywords: Artificial Intelligence, Enterprise Risk Management, Risk Governance, Risk Leadership, Health Insurance, Emerging Risks.

1. Introduction

The rapid development of Artificial Intelligence (AI) has significantly transformed the global health insurance industry. AI is increasingly used in underwriting processes, claims automation, fraud detection, and customer risk profiling. These technologies improve operational efficiency, reduce processing time, and enhance decision-making accuracy in complex insurance environments.

However, despite these advantages, AI adoption introduces new categories of risk that are fundamentally different from traditional actuarial and operational risks. Unlike conventional models that rely on historical stability, AI systems are adaptive, data-driven, and continuously learning. This dynamic nature creates uncertainty in outputs and introduces systemic risks that evolve over time.

Key risks emerging from AI adoption in health insurance include algorithmic bias, lack of explainability (black-box systems), data privacy violations, and model drift. These risks are not only technical in nature but also organizational, ethical, and regulatory challenges that require a more integrated approach to risk management.

Although extensive literature has discussed AI risks from technical, ethical, and regulatory perspectives, existing studies remain fragmented in their approach. Most

research focuses separately on either Enterprise Risk Management (ERM), risk governance, or ethical AI frameworks without integrating these dimensions into a unified organizational model.

Furthermore, traditional ERM frameworks such as COSO (2017) and ISO 31000:2018 were not originally designed to address adaptive and non-linear risks generated by AI systems. Similarly, current governance models tend to emphasize compliance and oversight but lack behavioral and cultural integration through leadership mechanisms.

As a result, there is a clear gap in the literature regarding the absence of a holistic framework that integrates structural (ERM), institutional (governance), and behavioral (leadership) dimensions in managing AI-related risks within health insurance organizations.

The core problem addressed in this study is the inability of existing risk management frameworks to effectively manage emerging AI risks in health insurance organizations. Traditional ERM approaches are insufficient in handling dynamic, opaque, and evolving risks generated by AI systems. In addition, fragmented governance structures and underdeveloped risk leadership further weaken organizational capacity to respond to AI-related uncertainties. Therefore, there is a need for an integrated conceptual framework that aligns ERM, risk governance, and risk leadership to ensure effective management of AI-driven risks.

This study is guided by the following research questions:

- a. How do emerging AI technologies generate new forms of risk in health insurance organizations?
- b. Why are traditional Enterprise Risk Management frameworks insufficient in managing AI-driven risks?
- c. How does risk governance contribute to managing AI-related uncertainties in insurance organizations?
- d. What is the role of risk leadership in shaping organizational responses to AI risks?
- e. How can ERM, risk governance, and risk leadership be integrated into a unified conceptual framework for AI risk management?

This study provides several academic and practical contributions:

First, it extends the application of Enterprise Risk Management into the context of AI-driven risk environments, particularly within the health insurance industry.

Second, it contributes to the development of risk governance literature by linking institutional oversight mechanisms with emerging AI regulatory challenges.

Third, it highlights the importance of risk leadership as a critical enabler of ethical, adaptive, and cross-functional risk management practices.

Finally, it proposes an integrated conceptual framework that bridges structural, institutional, and behavioral dimensions of risk management.

From a practical perspective, this study provides insights for health insurance organizations in designing more resilient risk management systems in the era of AI adoption. The proposed framework can assist organizations in:

- a. Improving AI risk identification and mitigation processes
- b. Strengthening governance and compliance structures
- c. Enhancing ethical decision-making in AI deployment
- d. Building a risk-aware organizational culture
- e. Supporting strategic decision-making in digital transformation

This study also provides learning outcomes for academics and practitioners in the field of risk management and insurance, including:

- a. Understanding the complexity of AI-driven risks in health insurance
- b. Recognizing limitations of traditional ERM in dynamic technological environments
- c. Comprehending the role of governance and leadership in AI risk control
- d. Developing the ability to construct integrated conceptual risk frameworks
- e. Enhancing critical thinking in managing emerging risks in digital transformation contexts

2. Literature Review

Enterprise Risk Management (ERM) in Complex Organizations

Enterprise Risk Management (ERM) is a holistic approach that integrates risk management into organizational strategy and performance. COSO (2017) defines ERM as a framework that enables organizations to identify, assess, manage, and monitor risks in order to create, preserve, and realize value. ERM emphasizes a portfolio view of risk across the entire organization rather than isolated risk categories.

However, the applicability of traditional ERM becomes limited in environments characterized by high uncertainty and technological complexity. Kaplan and Mikes (2012) highlight that risk management frameworks must differentiate between preventable, strategic, and external risks. In the context of Artificial Intelligence (AI), risk does not always fit neatly into these categories because it is dynamic, adaptive, and system-generated.

In health insurance organizations, ERM plays a critical role in managing underwriting, claims, and financial risks. Nevertheless, its static and historically driven structure makes it less effective in addressing AI-specific risks such as model drift, algorithmic bias, and data dependency.

ISO 31000 and Limitations in AI-Driven Environments

ISO 31000:2018 provides internationally recognized principles for risk management, emphasizing integration, structured processes, customization, inclusiveness, and continual improvement. It is widely adopted across industries, including insurance, due to its flexibility and system-wide applicability.

However, ISO 31000 does not explicitly address risks arising from machine learning systems or algorithmic decision-making. AI systems introduce non-linear risk behaviors where outputs evolve continuously based on data inputs. This dynamic nature challenges the assumption of stability embedded in traditional risk frameworks.

Therefore, while ISO 31000 provides a foundational structure, it requires augmentation when applied to AI-driven environments such as health insurance underwriting systems.

Artificial Intelligence Risk and the NIST AI RMF Perspective

The NIST Artificial Intelligence Risk Management Framework (AI RMF, 2023) represents one of the most comprehensive approaches to AI risk governance. It defines AI risk as a combination of the likelihood of harm and the severity of impact, considering contextual factors.

The framework introduces four core functions: govern, map, measure, and manage. These functions emphasize that AI risk must be continuously monitored and adjusted rather than treated as a static condition.

Key dimensions of trustworthy AI include fairness, accountability, transparency, reliability, and safety. In health insurance contexts, these dimensions are particularly important due to the sensitivity of personal health data and the ethical implications of automated decision-making.

Risk Governance in High Stake Industries

Risk governance refers to the structures, policies, and processes that guide decision-making under uncertainty. Renn (2008) argues that risk governance is not only a technical process but also a socio-political system that integrates scientific evidence, institutional frameworks, and stakeholder values.

In the context of AI in health insurance, risk governance extends beyond regulatory compliance. It includes algorithmic accountability, ethical oversight, and continuous monitoring of AI systems. Governance mechanisms such as model validation committees, AI ethics boards, and compliance audits are increasingly being adopted to manage AI-related risks.

Sun and Medaglia (2019) emphasize that AI governance requires multi-level coordination between technical experts, regulators, and organizational leadership to ensure responsible system deployment.

Risk Leadership and Organizational Behavior

Risk leadership refers to the ability of organizational leaders to shape risk-aware culture and ensure alignment between strategy, ethics, and operational execution. Unlike governance, which focuses on structure, leadership focuses on behavior and cultural transformation.

Kaplan and Mikes (2012) argue that effective risk management requires leadership that understands the nature of different risk categories and adapts responses accordingly. In AI environments, leadership must go beyond compliance and actively engage in ethical decision-making and cross-functional coordination.

Deloitte (2023) highlights that organizations with strong AI leadership capabilities are more successful in implementing responsible AI systems, particularly in highly regulated industries such as insurance.

AI Risk in Health Insurance Organization

The application of AI in health insurance introduces several interrelated risk dimensions. First, algorithmic bias may result in unfair underwriting decisions due to biased training data. Second, lack of explainability reduces transparency in decision-making processes, making it difficult to justify outcomes to regulators and customers.

Third, data privacy risks are heightened due to the sensitive nature of health-related information. Fourth, model drift creates ongoing uncertainty as AI systems degrade over time when exposed to new data patterns.

According to the World Economic Forum (2024), AI-driven systemic risks are increasingly recognized as global threats due to their cross-sectoral and cascading effects across industries.

Synthesis and Research Positioning

The literature indicates that existing approaches to AI risk management are fragmented across three main domains: technical risk control (ERM and ISO 31000), institutional oversight (risk governance), and behavioral adaptation (risk leadership).

However, there is limited integration of these three dimensions into a unified conceptual framework, particularly in the context of health insurance organizations. This fragmentation creates gaps in organizational readiness to manage AI-driven uncertainties effectively.

Therefore, this study positions itself at the intersection of these three domains by proposing an integrated framework that combines Enterprise Risk Management, risk governance, and risk leadership to address emerging AI risks holistically.

3. Method

Research Design

This study adopts a qualitative conceptual research design aimed at developing an integrated framework for managing emerging Artificial Intelligence (AI) risks in health insurance organizations. Unlike empirical studies that rely on statistical testing, conceptual research focuses on theory synthesis and framework development by integrating existing literature into a coherent model.

The objective of this approach is to bridge fragmented perspectives from Enterprise Risk Management (ERM), risk governance, and risk leadership into a unified conceptual structure relevant to AI-driven risk environments.

Research Approach

The study employs a structured literature review (SLR) approach combined with conceptual synthesis. This approach allows systematic identification, evaluation, and interpretation of relevant academic and institutional literature related to AI risk management, ERM frameworks, governance mechanisms, and leadership theories.

The synthesis process emphasizes thematic integration rather than quantitative meta-analysis, considering the conceptual nature of the research problem.

Data Sources

The literature used in this study was obtained from reputable academic and institutional databases, including:

- a. Scopus-indexed journals
- b. ScienceDirect (Elsevier)
- c. SpringerLink
- d. IEEE Xplore
- e. Google Scholar (filtered for peer-reviewed sources)
- f. Institutional reports (NIST, OECD, World Economic Forum, ISO)

These sources were selected to ensure academic rigor and relevance to emerging AI risk discourse in insurance and financial services.

Inclusion and Exclusion Criteria

To ensure quality and relevance, the following criteria were applied:

Inclusion Criteria:

- a. Publications between 2019–2025 (to ensure recency)
- b. Peer-reviewed journal articles (Scopus/ISI indexed preferred)
- c. Studies focusing on:

- Artificial Intelligence risk
 - Enterprise Risk Management
 - Risk governance
 - Risk leadership
 - Insurance or financial services context
- d. English-language publications
- Exclusion Criteria:
- Non-peer-reviewed articles without academic validation
 - Studies unrelated to risk management or AI
 - Duplicate publications
 - Opinion-based articles without methodological foundation

Data Collection and Selection Process

The literature selection process resulted in 28 core studies that were deemed relevant to the research objectives. The selection process followed three stages:

- a. Identification Stage
- Initial search using keywords such as:
- AI risk in insurance
 - enterprise risk management AI
 - risk governance artificial intelligence”
 - AI leadership risk management”
- b. Screening Stage
- Titles and abstracts were screened to eliminate irrelevant studies.
- c. Eligibility Stage
- Full-text review was conducted to ensure alignment with research focus on ERM, governance, and leadership integration.

Data Analysis Technique

This study applies thematic analysis and conceptual synthesis. The process involves:

- a. Coding of Literature Themes
- AI risk dimensions (bias, privacy, transparency, drift)
 - ERM limitations
 - Governance mechanisms
 - Leadership roles
- b. Pattern Identification
- Identifying recurring relationships between risk categories and organizational response mechanisms.
- c. Conceptual Integration
- Synthesizing findings into a unified three-layer framework:
- Enterprise Risk Management (structural layer)
 - Risk Governance (control layer)
 - Risk Leadership (behavioral layer)

Conceptual Nature of the Study

This research is purely conceptual, meaning no primary data collection or statistical testing is conducted. Instead, the study relies on secondary data (published literature and institutional frameworks) to construct a theoretical model.

The conceptual nature is appropriate given the emerging and evolving characteristics of AI risk in health insurance, where empirical datasets are still limited and fragmented.

Validity and Reliability of the Conceptual Approach

To ensure academic rigor, the study applies:

- a. Source triangulation (journal articles + institutional reports)
- b. Theoretical triangulation (ERM + governance + leadership theories)
- c. Time-bound validation (recent literature 2019–2025)
- d. Database credibility filtering (Scopus and recognized publishers)

This strengthens the validity of the conceptual framework developed in this study.

4. Result and Discussion

Emerging Nature of Artificial Intelligence Risks in Health Insurance

The analysis of the selected literature indicates that Artificial Intelligence (AI) introduces a fundamentally new risk landscape in health insurance organizations. Unlike traditional actuarial risks that are largely stable and statistically predictable, AI-related risks are dynamic, adaptive, and continuously evolving based on data inputs and model learning processes.

Four dominant categories of AI risks emerge from the synthesis:

First, algorithmic bias, which occurs when machine learning models replicate or amplify historical inequalities embedded in training datasets. In health insurance, this may result in discriminatory underwriting decisions or unequal premium determination across demographic groups.

Second, lack of explainability, often referred to as the black-box problem, limits the ability of organizations to interpret how AI systems reach specific decisions. This creates accountability challenges, especially in regulated environments where justification of decisions is mandatory.

Third, data privacy and security risks, which are significantly heightened due to the sensitive nature of health-related personal data processed by insurance systems.

Fourth, model drift, where AI model performance deteriorates over time due to changes in population behavior, healthcare trends, or external environmental shifts.

These findings confirm that AI risk in health insurance is not static but systemic and continuously evolving, requiring adaptive risk management structures.

Limitations of Traditional Enterprise Risk Management (ERM)

The findings reveal that traditional Enterprise Risk Management frameworks, while structurally robust, are insufficient to fully address AI-driven risks.

ERM is primarily designed around stable and historical risk patterns, where risk events can be identified, quantified, and mitigated based on past data. However, AI systems introduce non-linear and emergent risks that cannot be fully predicted using historical probability distributions.

Kaplan and Mikes' (2012) risk categorization framework becomes less effective in AI contexts because AI risks simultaneously behave as:

- Strategic risks (related to innovation and competitive advantage),
- Operational risks (system performance and model errors), and
- Systemic risks (networked and cascading effects across systems).

This overlap creates ambiguity in risk classification and weakens the effectiveness of traditional ERM implementation. Therefore, ERM alone cannot function as a complete solution for AI risk governance in health insurance organizations.

Role of Risk Governance in Managing AI Uncertainty

Risk governance emerges as a critical mechanism for addressing the accountability and oversight gaps introduced by AI systems.

The synthesis shows that effective risk governance in AI-driven insurance organizations must include:

- Formal AI oversight committees responsible for model validation and approval
- Continuous algorithm auditing mechanisms to monitor fairness, accuracy, and drift
- Integration of ethical AI principles into organizational policies
- Alignment with regulatory frameworks such as ISO 31000:2018 and NIST AI RMF (2023)

Renn (2008) emphasizes that risk governance is not purely technical but also institutional and socio-political in nature. In the context of health insurance, this means that AI governance must balance technical performance with ethical responsibility and regulatory compliance.

The NIST AI RMF (2023) further strengthens this perspective by introducing a continuous lifecycle approach (govern–map–measure–manage), which ensures that AI risks are not treated as one-time assessments but as ongoing governance processes.

Risk Leadership and Organizational Adaptation

The findings highlight that risk leadership plays a decisive role in ensuring the successful implementation of ERM and governance structures.

While governance provides rules and mechanisms, leadership determines whether these mechanisms are effectively embedded into organizational behavior and culture.

In AI-driven health insurance organizations, risk leadership is required to:

- Foster cross-functional collaboration between IT, actuarial, compliance, and executive teams
- Promote ethical awareness in AI-based decision-making
- Ensure alignment between technological innovation and risk appetite
- Build a risk-intelligent organizational culture

Kaplan and Mikes (2012) argue that risk management effectiveness depends not only on systems but also on leadership capability to interpret and respond to uncertainty. In AI environments, this becomes even more critical due to the speed and complexity of technological change.

Therefore, risk leadership functions as the behavioral foundation that enables governance and ERM to operate effectively.

Integrated ERM Governance–Leadership Framework

The central contribution of this study is the development of an integrated conceptual framework that combines three interdependent layers:

1. Enterprise Risk Management – Structural Layer

ERM provides the foundational structure for:

- Identifying AI-related risks
- Assessing risk exposure
- Implementing mitigation strategies
- Monitoring risk performance over time

However, ERM alone is insufficient without governance and leadership support.

2. Risk Governance – Control Layer

Risk governance ensures institutional control through:

- Regulatory compliance mechanisms
- AI model validation systems
- Ethical oversight committees
- Transparency and accountability structures

Governance acts as the bridge between technical systems and institutional responsibility.

3. Risk Leadership – Behavioral Layer

Risk leadership ensures cultural and behavioral alignment by:

- Embedding risk awareness in organizational culture
- Promoting ethical AI usage
- Enabling cross-functional coordination
- Supporting adaptive decision-making under uncertainty

Leadership ensures that governance and ERM are not merely procedural but actively practiced.

Systemic Interaction Between the Three Layers

The interaction between ERM, governance, and leadership forms a dynamic risk management ecosystem.

- ERM identifies and structures risk exposure
- Governance regulates and controls decision processes
- Leadership shapes organizational behavior and ethical orientation

These three components operate in a continuous feedback loop, where changes in AI systems require simultaneous adjustments in risk identification, governance mechanisms, and leadership responses.

This integrated system enhances organizational resilience by enabling health insurance organizations to respond more effectively to emerging AI-driven uncertainties.

Theoretical Contribution of the Study

This study contributes to the literature in three main ways:

1. It extends Enterprise Risk Management theory into AI-driven environments where risk is dynamic and non-linear.
2. It positions risk governance as an essential institutional mechanism for ensuring accountability in algorithmic decision-making.
3. It highlights risk leadership as a critical behavioral dimension that enables sustainable risk management in digital transformation contexts.

Conceptual Framework

Based on the synthesis of Enterprise Risk Management, risk governance, and risk leadership literature, this study proposes an integrated conceptual framework for managing emerging Artificial Intelligence risks in health insurance organizations. The framework emphasizes that effective AI risk management requires the integration of structural, institutional, and behavioral dimensions within a unified system.

The proposed framework is illustrated in Figure 1.

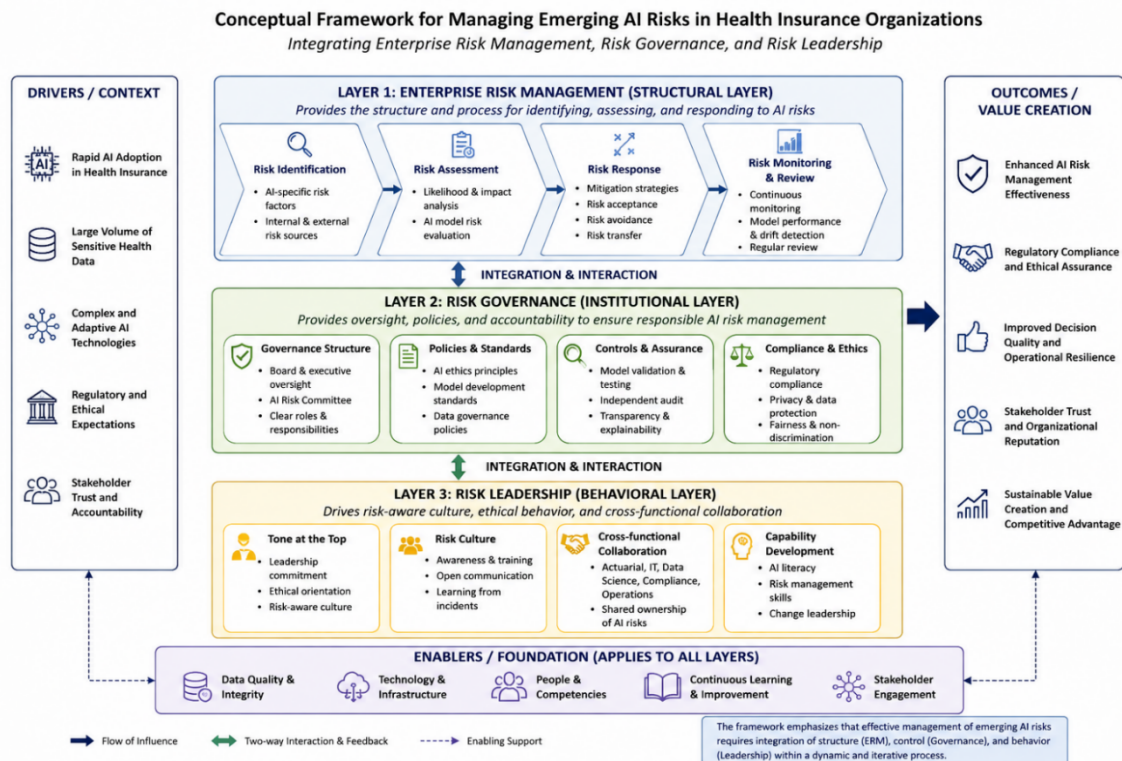


Figure 1. Conceptual framework for managing AI risks in health insurance organizations

5. Conclusion

Conclusion

This study develops a conceptual framework for managing emerging Artificial Intelligence (AI) risks in health insurance organizations through the integration of Enterprise Risk Management (ERM), risk governance, and risk leadership. The increasing adoption of AI in health insurance has transformed core operational processes such as underwriting, claims management, fraud detection, and customer analytics. However, this transformation also introduces complex and dynamic risks that cannot be adequately addressed by traditional risk management approaches alone.

The findings of this study indicate that AI-related risks—such as algorithmic bias, lack of explainability, data privacy concerns, and model drift—are systemic in nature and evolve continuously alongside technological developments. Traditional ERM frameworks, while still relevant, are limited in their ability to manage these adaptive risks due to their reliance on historical and relatively stable risk assumptions.

To address these limitations, this study proposes an integrated three-layer framework. Enterprise Risk Management functions as the structural layer responsible for identifying, assessing, and mitigating risks. Risk governance operates as the control layer that ensures accountability, regulatory compliance, and ethical oversight in AI deployment. Risk leadership serves as the behavioral layer that shapes organizational culture, promotes ethical awareness, and ensures cross-functional alignment in managing AI-driven uncertainty.

The integration of these three dimensions forms a comprehensive approach that enhances organizational resilience in responding to emerging AI risks in the health insurance sector.

Theoretical Implications

This study contributes to the existing literature in several important ways.

First, it extends Enterprise Risk Management theory into the context of AI-driven environments, where risk is no longer static but dynamic, adaptive, and systemically interconnected.

Second, it strengthens the role of risk governance by positioning it as a central mechanism for ensuring transparency, accountability, and ethical compliance in algorithmic decision-making systems.

Third, it highlights risk leadership as a critical but often underexplored dimension that determines whether risk frameworks are effectively implemented in practice. This adds a behavioral and cultural perspective to existing risk management literature, which has traditionally focused more on structural and technical aspects.

Overall, the study bridges fragmented theoretical perspectives into a unified conceptual model for AI risk management in insurance organizations.

Practical Implications

From a practical perspective, this study offers several implications for health insurance organizations.

First, organizations should strengthen their ERM systems by incorporating AI-specific risk indicators, such as model drift monitoring, algorithm bias detection, and data quality assurance mechanisms.

Second, risk governance structures should be enhanced through the establishment of dedicated AI oversight committees, ethical review boards, and continuous model validation processes to ensure transparency and accountability.

Third, leadership within insurance organizations must play a more active role in driving risk-aware culture, particularly by fostering collaboration between technical teams (data science and IT), actuarial departments, compliance units, and executive management.

By implementing these measures, health insurance organizations can improve their ability to manage uncertainty while maintaining trust, compliance, and operational efficiency in AI-driven environments.

Policy Implications

At the policy level, regulators and industry bodies should consider developing more specific guidelines for AI governance in the insurance sector. Existing frameworks such as ISO 31000:2018 and the NIST AI RMF (2023) provide strong

foundations, but sector-specific adaptation is necessary to address the unique challenges of health insurance applications.

Regulatory authorities should also encourage transparency requirements for AI-based decision-making systems, particularly in underwriting and claims processing, to ensure fairness and accountability.

Limitations and Future Research

This study is conceptual in nature and does not involve empirical testing or quantitative validation of the proposed framework. Therefore, the findings are theoretical and require further empirical investigation.

Future research is recommended to:

- Empirically test the proposed ERM–governance–leadership framework in real insurance organizations
- Conduct case studies on AI implementation in health insurance companies
- Develop quantitative models to measure AI risk maturity levels
- Explore industry-specific adaptation of AI governance frameworks

Such studies would strengthen the practical applicability and validation of the conceptual framework proposed in this research.

6. References

- COSO. (2017). Enterprise risk management—Integrating with strategy and performance. Committee of Sponsoring Organizations of the Treadway Commission.
- Dignum, V. (2019). Responsible artificial intelligence: How to develop and use AI in a responsible way. Springer.
- Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., et al. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and Machines*, 28(4), 689–707. <https://doi.org/10.1007/s11023-018-9482-5>
- International Organization for Standardization. (2018). ISO 31000:2018 risk management Guidelines. ISO.
- Kaplan, R. S., & Mikes, A. (2012). Managing risks: A new framework. *Harvard Business Review*, 90(6), 48–60.
- National Institute of Standards and Technology. (2023). Artificial intelligence risk management framework (AI RMF 1.0). U.S. Department of Commerce.
- OECD. (2021). Artificial intelligence, machine learning and big data in finance and insurance: Risks and opportunities. OECD Publishing.
- Renn, O. (2008). Risk governance: Coping with uncertainty in a complex world. Earthscan.
- Rudin, C. (2019). Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. *Nature Machine Intelligence*, 1, 206–215. <https://doi.org/10.1038/s42256-019-0048-x>
- World Economic Forum. (2024). The global risks report 2024. World Economic Forum.