Community Engagement & Emergence Journal
Volume 7 Nomor 6, Tahun 2026
Halaman : 5084-5098

Managing Risks Emerging in AI-Based Claims Verification: The Role of Enterprise Risk Management and Risk Governance in Health Insurance Operations

Franciska Natalia[a], Franciskus Antonius[b]
Master of Management Study Program, Sekolah Tinggi Manajemen Asuransi (STMA) Trisakti, Jakarta[a,b]
franciska.nat81@gmail.com[a], franciskus.antonius.alijoyo63@gmail.com[b]

Abstract
The digital transformation of the health insurance industry, particularly through the implementation of Artificial Intelligence (AI) in claims verification processes, has enhanced operational efficiency while simultaneously introducing new, complex, and technology-driven risks. This study aims to identify the risks emerging from AI implementation, evaluate the application of Enterprise Risk Management (ERM), analyze key risk factors, and examine the role of risk governance in overseeing AI-based claims verification processes. This research adopts a qualitative case study approach focusing on a health insurance company in Indonesia that has implemented AI in cashless claims services. Data were collected through document analysis, process observation, semi-structured interviews involving the three lines of defense, and literature review. The analysis was conducted using thematic analysis, supported by the ISO 31000 ERM framework and the Three Lines Model for risk governance. The findings indicate that the implementation of AI in datafication, verification, and claim settlement significantly improves operational efficiency in processing large volumes of claims. However, it also introduces new risks, including data dependency risk, model risk, algorithmic bias, and systemic risk amplification. Furthermore, the current ERM implementation remains general and has not fully incorporated AI-specific risks. Although a risk governance structure has been established, its effectiveness in overseeing technology-driven risks remains limited. This study concludes that AI implementation not only transforms operational processes but also fundamentally reshapes the organization's risk profile. Therefore, strengthening ERM and risk governance through more adaptive, integrated, and technology-oriented approaches is essential to effectively manage emerging AI-related risks.
Keywords*: Artificial Intelligence, Claims Verification, Enterprise Risk Management, Risk Governance, Health Insurance.*

1. Introduction

The rapid advancement of Artificial Intelligence (AI) has significantly transformed operational processes in the insurance industry, particularly in health insurance services. One of the most critical areas affected is the claims verification process, especially in cashless claims provided through healthcare partners such as hospitals and clinics. AI-driven systems enable automated datafication, real-time validation, and enhanced decision-making efficiency in processing claims. According to Martin Eling and Martin Lehmann (2022), digitalization and AI adoption are reshaping the insurance value chain by improving efficiency while simultaneously increasing system complexity and interdependencies.

However, the implementation of AI in operational processes also introduces a new spectrum of emerging risks. These include model risk, data quality issues, algorithmic bias, cybersecurity threats, and regulatory compliance challenges, particularly concerning sensitive health data. Recent studies highlight that AI adoption in financial services increases exposure to operational and cyber risks due to the complexity and opacity of algorithmic decision-making processes (Eling & Lehmann, 2022). Recent global studies further emphasize that AI adoption in financial services

introduces systemic and operational risks that require stronger governance and regulatory oversight (Boukherouaa et al., 2021; Financial Stability Board, 2023). This indicates that AI not only enhances efficiency but also amplifies uncertainty in risk exposure.

In the context of health insurance, AI-driven claims verification fundamentally transforms decision-making processes, where claim approval or rejection may increasingly rely on automated systems. This shift raises critical concerns regarding decision accuracy, accountability, and transparency. Drawing from decision-making theory developed by Herbert Simon, organizational effectiveness depends not only on the quality of decisions but also on how decisions are executed within structured processes. Therefore, the integration of AI into claims verification requires careful consideration of both technological capability and decision governance.

To address these challenges, organizations are required to adopt a more integrated and structured risk management approach. Enterprise Risk Management (ERM) provides a comprehensive framework for identifying, assessing, and mitigating risks across organizational processes. As noted by Cristina Florio and Giulia Leoni (2021), ERM implementation enhances an organization's ability to manage risks holistically and improves decision-making quality in complex and uncertain environments.

Furthermore, effective risk governance plays a crucial role in ensuring that AI-driven decision-making processes are properly controlled, monitored, and aligned with organizational objectives and regulatory requirements. In AI-driven claims verification, risk governance becomes essential to define accountability, establish control mechanisms, and ensure oversight over automated decisions. In the Indonesian context, Wulan Utami and Lutfi Nugroho (2021) emphasize that the adoption of Enterprise Risk Management strengthens organizational resilience, particularly in responding to digital transformation challenges.

This study contributes to the existing literature by integrating ERM and risk governance frameworks into AI-driven operational processes, particularly in claims verification. It also provides an operational-level analysis of emerging AI risks and offers practical recommendations for improving risk management and governance in health insurance organizations.

Despite the increasing adoption of Artificial Intelligence (AI) in health insurance operations, significant challenges remain in managing the risks associated with AI-driven claims verification processes. This creates a critical gap between technological adoption and the organization's capability to manage associated risks effectively.

One of the key challenges lies in the emergence of AI-related risks at the operational level, including model risk, data inaccuracy, algorithmic bias, and lack of transparency in automated decision-making. Despite these challenges, there is still limited empirical evidence on how Enterprise Risk Management (ERM) frameworks are implemented to manage such risks, particularly in claims verification processes.

Furthermore, the role of risk governance in overseeing AI-driven decision-making remains underexplored, especially in ensuring accountability, control, and alignment with regulatory requirements. This gap indicates that while organizations adopt AI technologies, the corresponding risk management and governance mechanisms may not be fully developed.

2. Literature Review

Artificial Intelligence in Health Insurance Operations

The adoption of Artificial Intelligence (AI) has become a key driver of digital transformation in the insurance industry, particularly in improving operational efficiency and service delivery. In health insurance, AI is widely utilized in claims processing, including datafication, fraud detection, and automated decision-making. According to Martin Eling and Martin Lehmann (2022), digitalization and AI technologies are reshaping the insurance value chain by enhancing efficiency, reducing processing time, and improving customer experience. However, the integration of AI also introduces new complexities in operational processes. AI systems rely heavily on large volumes of data and algorithmic models, which may lead to risks such as data inaccuracies, model bias, and lack of transparency. These risks are particularly critical in claims verification processes, where decisions directly impact financial outcomes and customer trust. Therefore, while AI provides operational benefits, it simultaneously creates emerging risks that must be managed effectively.

Emerging Risks in AI-Driven Decision-Making

The implementation of AI in decision-making processes has shifted organizational practices from human-based judgment to algorithm-driven decisions. This transition introduces new forms of risk, commonly referred to as emerging risks. These include model risk, data risk, operational risk, and compliance risk.

AI-driven decision-making systems are often characterized by limited transparency (black-box models), making it difficult for organizations to fully understand how decisions are generated. This lack of transparency raises concerns regarding accountability and explainability, particularly in regulated industries such as insurance.

From a decision-making perspective, the theory developed by Herbert Simon emphasizes that effective decision-making involves structured stages, including problem identification, design of alternatives, and choice selection. In the context of AI, these stages are increasingly automated, raising critical questions regarding the balance between human oversight and machine autonomy. This highlights the importance of integrating governance mechanisms into AI-driven decision processes.

Enterprise Risk Management (ERM) and ISO 31000

Enterprise Risk Management (ERM) is a comprehensive framework designed to manage risks across organizational processes in a structured and integrated manner. ERM enables organizations to identify, assess, and mitigate risks holistically, ensuring alignment with strategic objectives.

According to Cristina Florio and Giulia Leoni (2021), the implementation of ERM enhances organizational performance by improving risk awareness and supporting better decision-making in uncertain environments.

One of the most widely adopted ERM frameworks is ISO 31000, developed by the International Organization for Standardization. ISO 31000 outlines key processes in risk management, including risk identification, risk assessment, and risk treatment. In addition, it emphasizes eight principles of effective risk management, such as integration, structured approach, and continual improvement.

In the context of AI implementation, ERM plays a critical role in ensuring that emerging risks are systematically managed. The integration of ERM into AI-driven

processes allows organizations to address uncertainties and enhance resilience in dynamic environments.

Governance and the Three Lines Model

Risk governance refers to the structures, processes, and mechanisms used to direct and control risk management activities within an organization. Effective risk governance ensures that risks are managed in a transparent, accountable, and consistent manner.

The Three Lines Model developed by the Institute of Internal Auditors provides a widely accepted framework for understanding roles and responsibilities in risk management. The model divides organizational functions into three lines:

- First Line: Operational management responsible for executing processes and managing risks
- Second Line: Risk management and compliance functions providing oversight and guidance
- Third Line: Internal audit providing independent assurance

In the context of AI-driven claims verification, risk governance becomes increasingly important due to the complexity of automated decision-making processes. Clear roles and responsibilities are required to ensure that AI systems operate within acceptable risk boundaries and comply with regulatory requirements.

Studies in the Indonesian context, such as Wulan Utami and Lutfi Nugroho (2021), highlight that strong governance structures are essential for enhancing organizational resilience, particularly in managing risks associated with digital transformation.

Analysis of the 8 Principles of ISO 31000

The ISO 31000:2018 framework provides a comprehensive set of principles that guide the effective implementation of risk management within organizations. These principles are designed to ensure that risk management is not only systematic but also aligned with organizational objectives and decision-making processes. According to the International Organization for Standardization (2018), there are eight key principles that underpin effective risk management.

First, integration emphasizes that risk management should be embedded in all organizational activities, including strategic planning and operational processes. In the context of AI-driven claims verification, this implies that risk considerations must be incorporated into system design, data processing, and decision-making workflows.

Second, a structured and comprehensive approach ensures that risk management processes are consistent, systematic, and comparable across the organization. This principle is particularly important in managing AI-related risks, where complex systems require clearly defined procedures for risk identification, assessment, and treatment.

Third, customization highlights the need to tailor risk management frameworks to the organization's internal and external context. AI implementation introduces unique risks such as algorithmic bias and model uncertainty, which require specific risk management approaches beyond traditional frameworks.

Fourth, inclusiveness ensures that relevant stakeholders are involved in the risk management process. Effective management of AI-driven risks requires collaboration

between operational units, IT, risk management, compliance, and top management to ensure comprehensive oversight.

Fifth, the dynamic principle recognizes that risks are continuously evolving. AI systems, in particular, are adaptive and may introduce new risks over time, requiring organizations to continuously monitor and respond to changes in the risk environment.

Sixth, the use of the best available information emphasizes that risk management decisions should be based on reliable and up-to-date data. In AI-driven systems, data quality plays a critical role, as inaccurate or incomplete data can significantly increase risk exposure.

Seventh, human and cultural factors highlight the importance of human judgment, organizational culture, and behavioral aspects in risk management. Despite the increasing reliance on AI, human oversight remains essential to ensure accountability, ethical considerations, and sound decision-making.

Finally, continual improvement underscores the need for organizations to continuously enhance their risk management practices. In the context of AI, this involves regular model evaluation, system updates, and learning from past incidents to improve future performance.

Overall, these eight principles provide a foundational framework for managing risks in complex and dynamic environments, including those arising from the adoption of Artificial Intelligence in health insurance operations

Research Gap

Although prior studies have extensively discussed digital transformation and AI adoption in the insurance industry, most of them focus on strategic and technological perspectives at a macro level. Limited attention has been given to operational-level risk management, particularly in AI-driven claims verification processes.

Furthermore, existing literature tends to examine Enterprise Risk Management and risk governance separately, with limited integration between the two frameworks in the context of AI implementation. There is also a lack of empirical analysis on how organizations operationalize ERM principles and governance mechanisms to manage emerging risks in real-world settings.

Therefore, this study seeks to fill this gap by providing a focused analysis of how Enterprise Risk Management and risk governance are applied in managing risks associated with AI-driven claims verification in health insurance operations.

More importantly, there is a lack of operational-level analysis that explicitly integrates Enterprise Risk Management (ERM) and risk governance within AI-driven claims verification processes. This gap is significant because claims verification represents a critical decision point where algorithmic errors can directly impact financial outcomes, regulatory compliance, and customer trust.

3. Method

Research Approach

This study focuses on a case study of a health insurance company in Indonesia that has implemented AI-driven claims verification systems, particularly in cashless claim services. The case is selected to provide an in-depth understanding of how AI-related risks emerge and are managed within real operational settings.

Methodological Process Framework

This research adopts a process-based analytical framework integrating Enterprise Risk Management (ERM), decision-making theory, and risk governance principles. The methodology is structured into sequential stages to systematically analyze AI-driven claims verification.

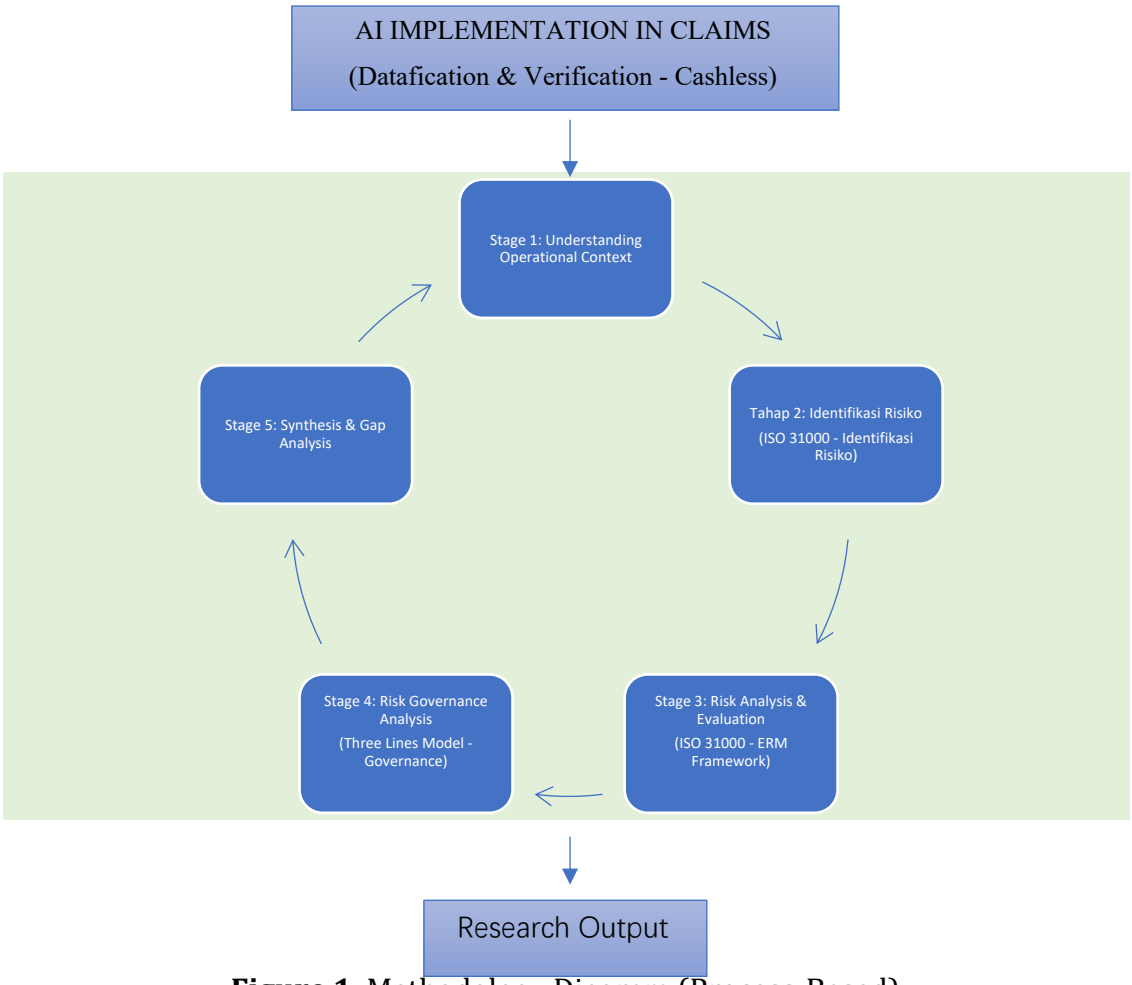

Figure 1. Methodology Diagram (Process-Based)

Stage 1: Understanding Operational Context (Herbert Simon - Intelligence Stage):
- Mapping claims datafication and verification processes
- Identifying AI involvement in decision-making
- Understanding internal and external organizational context

Stage 2: Risk Identification (ISO 31000 - Risk Identification)
- Model Risk
- Data Risk
- Operational Risk
- Compliance Risk
- Reputational Risk

Stage 3: Risk Analysis & Evaluation (ISO 31000 - ERM Framework)
- Risk assessment

- Risk treatment
- Evaluation of 8 ERM principles

Stage 4: Risk Governance Analysis (Three Lines Model - Governance)
- 1st Line: Claims Operations
- 2nd Line: Risk Management
- 3rd Line: Internal Audit

Stage 5: Synthesis & Gap Analysis
- Compare practice vs framework
- Identify weaknesses
- Evaluate effectiveness

Research Output
- Findings on AI risk management
- ERM effectiveness
- Governance evaluation
- Recommendations

The research methodology follows a structured process-based approach, beginning with understanding the operational context of AI implementation in claims verification. The study then identifies and classifies emerging risks, followed by risk analysis using the Enterprise Risk Management framework based on ISO 31000. Subsequently, governance structures are evaluated using the Three Lines Model to assess oversight and accountability.

Finally, the study synthesizes the findings to identify gaps between current practices and theoretical frameworks, leading to recommendations for improving risk management and governance.

Data Collection Methods

To ensure comprehensive and triangulated findings, this study utilizes qualitative data obtained through:

a. Document Analysis
   - Standard Operating Procedures (SOP) for claims verification
   - Internal risk management policies
   - AI implementation guidelines

b. Process Observation
   - Observation of claims verification workflow
   - Identification of AI involvement in decision-making

c. Semi-Structured Interviews
   - Claims operations staff (first line)
   - Risk management and compliance personnel (second line)
   - Internal audit representatives (third line)

   The interviews aimed to capture insights regarding AI usage, perceived risks, control mechanisms, and governance practices.

d. Secondary Data

   Secondary data were collected from:
   - Peer-reviewed academic journals

- Industry reports
- Regulatory frameworks and standards

Data Analysis Technique

Data is analyzed using qualitative thematic analysis, which involves:

- Identifying key themes related to AI implementation and risk exposure
- Mapping identified risks into ERM categories
- Evaluating risk management practices using ISO 31000 principles
- Analyzing governance structure using the Three Lines Model
- Interpreting findings to assess gaps between theory and practice

Table 1. Mapping AI Risk vs ERM Response

All Risk Type	**Description**	**ERM Response (ISO 31000)**	**Risk Governance Role**
Model Risk	Inaccurate AI Prediction	Model Validation & Monitoring	Risk Management (2nd line)
Data Risk	Poor data quality/incomplete data	Data governance framework	IT & Compliance
Algorithmic Bias	Unfair decision outcomes	Bias testing & audit	Internal audit (3rd line)
Cyber risk	Data breach/hacking	Cybersecurity controls	IT, Risk Management
Compliance risk	Violation of regulations	Regulatory monitoring	Compliance function

Research Validity

To ensure the credibility of findings, this study applies:

- Data triangulation (documents, observation, literature)
- Theoretical triangulation (ERM, governance, AI risk)

4. Result and Discussion

AI Implementation and the Emergence of New Risks in Claims Verification

This study was conducted over a six-month period, from November 2025 to April 2026, as part of a pilot project involving 62 healthcare providers, consisting of hospitals and clinics. These providers represent a subset of the company's total network of 2,880 partner providers. The implementation of Artificial Intelligence (AI) was primarily focused on the processes of datafication and claims verification within cashless services, with the objective of improving operational efficiency in handling high claim volumes.

During the observation period, the volume of claims processed exhibited significant fluctuations, with the highest volumes recorded in November 2025 (27,771 claims) and April 2026 (27,560 claims), and lower volumes observed in December 2025 (17,898 claims) and January 2026 (17,712 claims). These variations indicate that the AI system was tested under dynamic operational conditions, reflecting the real workload characteristics of the health insurance industry.

From an operational perspective, the implementation of AI in the cashless claims process encompasses three main stages: datafication, verification, and claim settlement.

In the datafication stage, claim documents submitted by healthcare providers—such as medical summaries, billing details, and administrative documents—are processed using AI technologies to be transformed into structured data. The system performs optical character recognition (OCR), document classification, and mapping of medical information into machine-readable formats. At this stage, the readability rate serves as a key performance indicator, which in this study ranges between 79% and 85%. This indicates that a portion of the data cannot be optimally interpreted by the AI system, highlighting limitations in processing unstructured or low-quality inputs.

In the verification stage, the structured data is assessed against policy terms, insurance benefits, and applicable medical rules. The AI system supports decision-making by providing recommendations on whether claims should be approved, rejected, or require further review. However, interview findings reveal that final decisions still involve human intervention, particularly in cases characterized by high complexity or incomplete information.

The final stage is claim settlement, where the decisions generated are used as the basis for payment to healthcare providers. In a cashless scheme, speed and accuracy at this stage are critical, as they directly affect service quality for policyholders as well as relationships with provider networks.

The digital transformation across these three stages reflects a shift from manual processes to semi-automated and fully automated systems. In line with the methodological framework at Stage 1 (understanding operational context), this transformation not only enhances efficiency but also fundamentally alters the nature of operational risk.

In traditional processes, risks are primarily associated with human error, processing delays, and inconsistencies in decision-making. However, in AI-driven systems, risks evolve into more complex, technology-driven forms. Based on the analysis, a new operational risk mapping can be identified as a result of AI implementation.

Table 2. Risk Mapping of AI-Driven Claims Verification Process

Process Stage	**Key Activities**	**AI-Driven Risk Category**	**Risk Description**	**Operational Impact**	**ERM Response (ISO 31000)**	**Risk Governance Role**
Datafication	Extraction and structuring of claim documents (OCR, classification, data transformation)	Data Dependency Risk	High reliance on input data quality and structure	Misinterpretation of medical and administrative data	Data governance and standardization	IT, Compliance
		Data Quality Risk	Incomplete, inconsistent, or unstructured data across providers	Reduced AI accuracy (readability variability 79%–85%)	Data validation and cleansing mechanisms	Claim Management (1st Line), IT
		Processing Error Risk	System errors in document recognition and classification	Increased need for manual reprocessing	Performance monitoring and error tracking	IT, Risk Management (2nd line)
Verification	Validation against policy terms and medical rules	Model Dependency Risk	Over-reliance on AI model performance for decision-making	Inaccurate or inconsistent claim decisions	Model validation and periodic review	Risk Management (2nd line)

		Algorithmic Bias	Unequal outcomes due to data or model bias	Potential unfair treatment of claims	Bias testing and audit procedures	Internal Audit (3rd Line)
		Opacity / Explainability Risk	Lack of transparency in AI decision logic	Difficulty in audit and decision justification	Model documentation and transparency controls	Compliance
		Decision Error Risk	Incorrect AI recommendations for claim approval/rejection	Financial loss and customer dissatisfaction	Human review and fallback control mechanisms	Claim Management (1st line)
Claim Settlement	Approval and payment execution	Operational Amplification Risk	Errors amplified due to high claim processing volumes	Increased operational burden and rework	Process control and workload management	Operations
		Systemic Risk Amplification	Replication of errors at scale across large datasets	Significant financial and reputational impact	Risk monitoring and escalation mechanisms	Risk Management (2nd line)
		System Dependency Risk	High reliance on AI system availability and performance	Service disruption in case of system failure	Business continuity planning (BCP)	IT, Risk Management (2nd line)
Cross-Process	Human–AI interaction and system integration	Human–Machine Interdependency Risk	Dependency between human operators and AI systems	Over-reliance or underutilization of AI	Training and awareness programs	All Lines
		Compliance Risk	Non-compliance with regulatory and ethical standards	Legal sanctions and reputational damage	Regulatory monitoring and compliance controls	Compliance
		Cyber Risk	Data breaches and cybersecurity threats	Exposure of sensitive health data	Cybersecurity framework and controls	IT

Table 2 presents a structured mapping of operational risks arising from the implementation of Artificial Intelligence (AI) across the claims verification process. The mapping integrates process stages, identified AI-driven risks, their operational implications, corresponding Enterprise Risk Management (ERM) responses based on ISO 31000, and the roles of risk governance aligned with the Three Lines Model. This table illustrates how AI transforms traditional operational risks into more complex, technology-driven, and interconnected risk categories.

At the datafication stage, the primary risks include data dependency risk and data quality risk, where the quality of documents submitted by providers becomes a critical determinant of system accuracy. Unstructured, incomplete, or low-quality data may lead to errors in extraction, which subsequently affect downstream processes.

At the verification stage, model dependency risk and algorithmic risk emerge, as decision outcomes heavily rely on the logic embedded within AI models. Imperfections in model design or training may lead to systematic errors in claim decisions. Additionally, opacity and explainability risks arise, as the decision-making

processes of AI systems are not always transparent to users, thereby complicating auditability and justification of decisions.

At the claim settlement stage, risks evolve into operational amplification risk, where errors originating from earlier stages may have widespread impacts due to the system's ability to process large volumes of claims simultaneously. This significantly increases the potential for financial losses and reputational damage in the event of systemic errors.

Furthermore, cross-stage risks such as human–machine interdependency risk are identified, where the effectiveness of the overall process depends on the interaction between AI systems and human operators. Imbalances in understanding or trust toward the system may result in either over-reliance or underutilization of AI.

Therefore, while the implementation of AI enhances operational efficiency in claims verification, it simultaneously creates a new configuration of risks that are more dynamic, interconnected, and large-scale in nature. These risks are no longer isolated at the individual level but tend to be systemic, thereby requiring more integrated and technology-oriented risk management approaches.

These findings directly address the first research question, demonstrating that the implementation of AI in datafication and claims verification processes not only transforms operational practices but also fundamentally reshapes the risk structure within the health insurance industry.

Evaluation of Enterprise Risk Management (ERM) Implementation in Managing AI-Related Risks

Based on Stage 3 of the methodological framework (risk analysis using ISO 31000), the findings indicate that the company has established an Enterprise Risk Management (ERM) framework. However, its implementation in the context of Artificial Intelligence (AI) remains insufficiently adaptive to address emerging technology-driven risks.

Operational and compliance risks have been identified within internal policies. Nevertheless, AI-specific risks—such as model risk, algorithmic bias, and data risk—have not been formally structured or systematically integrated into the existing ERM framework. This indicates a gap between the current risk management practices and the increasing complexity of AI-driven operational risks.

In terms of risk assessment, the organization has not yet incorporated quantitative indicators that explicitly measure AI performance. Empirical data from this study show that the system's readability rate ranges between 79% and 85%, which could serve as a critical metric for assessing AI-related operational risk.

For instance, a readability level of 79% in November 2025 implies that approximately 21% of the data was not optimally processed by the system, potentially leading to errors in claims verification. Despite its significance, this indicator has not been formally integrated into the organization's risk assessment and monitoring mechanisms.

From a risk control perspective, the company continues to rely on manual interventions, such as reprocessing or reviewing unreadable claims. However, there is no evidence of systematic model validation procedures or continuous performance monitoring of AI systems. The absence of such mechanisms limits the organization's ability to detect, evaluate, and mitigate risks associated with AI in a proactive and structured manner.

Therefore, although ERM has been implemented at a general level, its current application remains insufficient to comprehensively address AI-specific risks. This finding highlights the need for a more adaptive and technology-oriented ERM framework, thereby directly addressing the second research question.

Key Risk Factors in AI-Based Decision-Making for Claims Verification

Based on the thematic analysis conducted in Stage 2 of the methodological framework, this study identifies several key risk factors influencing AI-based decision-making in claims verification.

First, data risk emerges as the most dominant factor. The variability in system readability rates (79%–85%) indicates that data quality significantly affects the accuracy of AI outputs. Unstructured, incomplete, or inconsistent data leads to errors in classification and validation processes, thereby reducing the reliability of decision outcomes.

Second, model risk arises from the organization's reliance on algorithms that are not yet fully stable. The observed fluctuations in system performance suggest that AI models remain sensitive to variations in input data and have not achieved full robustness.

Third, algorithmic bias may occur due to disparities in data quality across healthcare providers. Providers with more standardized and higher-quality documentation tend to produce more accurate outputs, potentially resulting in unequal treatment in claim decision outcomes.

Fourth, operational risk increases in line with the high volume of claims processed. With monthly claim volumes reaching tens of thousands, even minor error rates can have significant implications for operational workload and efficiency.

Fifth, compliance risk arises from the limited transparency of AI systems. The lack of explainability in algorithmic decision-making may hinder the organization's ability to meet regulatory requirements, particularly those related to data protection, fairness, and accountability.

These findings indicate that risk factors in AI-based systems are multidimensional and highly interconnected, thereby directly addressing the third research question.

The Role of Risk Governance in AI Oversight

Referring to Stage 4 of the methodological framework (Three Lines Model), the findings indicate that while a risk governance structure has been established, its effectiveness in managing AI-related risks remains limited.

At the first line, operational units actively utilize AI in the claims verification process. However, they tend to rely heavily on system outputs without a comprehensive understanding of the underlying algorithmic processes. This condition increases the risk of over-reliance on technology.

At the second line, risk management and compliance functions perform oversight roles, yet they face limitations in addressing technical AI-related risks, such as model validation and algorithmic bias. This gap reduces the effectiveness of risk identification and monitoring processes.

At the third line, the internal audit function has not fully incorporated AI systems as a primary audit focus. As a result, the level of independent assurance over AI processes remains insufficient.

These findings highlight a misalignment between the existing governance structure and the emerging needs of AI risk management. Therefore, while risk governance plays a critical role in overseeing AI-based processes, it requires enhanced capabilities and integration to effectively address technology-driven risks, thereby answering the fourth research question.

Enhancing ERM and Risk Governance in Managing AI-Related Risks

Based on Stage 5 of the methodological framework (synthesis and gap analysis), this study identifies several areas for improvement in ERM practices and risk governance to effectively manage AI-related risks.

First, organizations need to develop a dedicated AI risk management framework that includes model risk management, data governance, and algorithmic bias testing. This is essential to ensure that AI-related risks are systematically identified, assessed, and mitigated.

Second, performance indicators such as system readability should be formally integrated into the ERM framework as key metrics for operational risk assessment. This would enable more data-driven decision-making and risk monitoring.

Third, improving data quality and standardization across healthcare providers is critical for enhancing AI accuracy and reducing data-related risks.

Fourth, organizations must strengthen human resource capabilities, particularly in understanding AI-related risks, across all lines of defense, including operational staff, risk management, and internal audit functions.

Fifth, stronger cross-functional collaboration is required to ensure that AI implementation is supported by effective control and oversight mechanisms.

In conclusion, enhancing ERM and risk governance requires not only structural improvements but also a broader transformation in organizational capabilities. These findings directly address the fifth research question, emphasizing the need for a more adaptive, integrated, and technology-oriented approach to managing AI-related risks.

5. Conclusion

This study examines the emerging risks associated with the implementation of Artificial Intelligence (AI) in claims datafication and verification processes, as well as the role of Enterprise Risk Management (ERM) and risk governance in managing these risks within health insurance operations. Based on the findings, several key conclusions can be drawn:

1. AI implementation in claims verification introduces new categories of operational risk.
   While AI significantly enhances efficiency in processing large volumes of claims, it simultaneously creates new risks, particularly model risk, data risk, operational risk, and algorithmic bias. These risks emerge primarily from the system's dependency on data quality and algorithm performance.
2. The application of Enterprise Risk Management (ERM) remains partially adaptive to AI-related risks.
   Although ERM frameworks are in place, their implementation is still largely focused on traditional risk categories. AI-specific risks, such as model validation and bias detection, are not yet fully integrated into formal risk management processes.
3. Data quality and model performance are the primary risk drivers in AI-based claims verification.

The study finds that variations in data readability (ranging from 79% to 85%) directly influence the accuracy and reliability of AI outputs, highlighting the critical importance of structured, consistent, and high-quality data.

4. Risk governance structures exist but are not fully aligned with AI complexity.
   The Three Lines Model is implemented; however, limited technical understanding of AI within each line reduces the effectiveness of oversight, control, and accountability in managing AI-driven processes.
5. Enhancing ERM and risk governance requires the integration of AI-specific frameworks and capabilities.
   Effective management of AI-related risks requires organizations to evolve beyond traditional approaches by incorporating model risk management, data governance, and algorithm accountability into their ERM and governance practices.

Recommendations

Based on the findings of this study, several recommendations are proposed to improve the management of AI-related risks in claims verification processes:

1. Develop AI-specific risk management frameworks
   Organizations should integrate model risk, data risk, and algorithmic bias into their ERM framework to ensure comprehensive risk coverage.
2. Strengthen data governance and standardization
   Improving the quality, consistency, and structure of data across healthcare providers is essential to enhance AI performance and reduce data-related risks.
3. Implement model validation and performance monitoring systems
   Regular evaluation of AI models, including accuracy testing, bias detection, and continuous monitoring, should be established as part of risk control mechanisms.
4. Enhance governance capabilities and AI literacy
   Organizations should strengthen the technical understanding of AI within operational, risk management, and audit functions to improve oversight effectiveness.
5. Integrate AI performance metrics into ERM processes
   Indicators such as readability rates should be formally incorporated into risk assessment and monitoring systems to support data-driven decision-making.

6. References

Boukherouaa, E. B., AlAjmi, K., Deodoro, J., Farias, A., Ravikumar, R., & Svirydzenka, K. (2021). Powering the digital economy: Opportunities and risks of artificial intelligence in finance. International Monetary Fund. https://doi.org/10.5089/9781513594068.087

Eling, M., & Lehmann, M. (2022). The impact of digitalization on the insurance value chain and the InsurTech ecosystem. The Geneva Papers on Risk and Insurance – Issues and Practice, 47(3), 359–396. https://doi.org/10.1057/s41288-021-00201-7

Financial Stability Board. (2023). The financial stability implications of artificial intelligence. https://www.fsb.org

Florio, C., & Leoni, G. (2021). Enterprise risk management and firm performance: The Italian case. The British Accounting Review, 53(1), 100888. https://doi.org/10.1016/j.bar.2020.100888

Institute of Internal Auditors. (2020). The IIA's three lines model: An update of the three lines of defense. The Institute of Internal Auditors.

International Organization for Standardization. (2018). ISO 31000:2018 risk management Guidelines. ISO.

OECD. (2021). Artificial intelligence, machine learning and big data in finance: Opportunities, challenges, and implications for policy makers. OECD Publishing. https://doi.org/10.1787/7c2c1c4e-en

Rahmawati, D. (2022). Manajemen risiko operasional dalam transformasi digital perusahaan. Jurnal Manajemen Indonesia, 22(1), 45–56.

Simon, H. A. (1947). Administrative behavior: A study of decision-making processes in administrative organizations. Free Press.

Utami, W., & Nugroho, L. (2021). Penerapan enterprise risk management pada industri keuangan di Indonesia. Jurnal Manajemen dan Keuangan, 10(2), 123–135.