MIX: Jurnal Ilmiah Manajemen

Management Scientific Journal
ISSN (Online): 2460-5328, ISSN (Print): 2088-1231
https://publikasi.mercubuana.ac.id/index.php/jurnal_Mix

Transformation of Risk Management through the Integration of an Artificial Intelligence Approach in Various Industrial Sectors

Martua Eliakim Tambunan[1*]; Perdana Wahyu Santosa[2)]

[1)] martua.tambunan@uki.ac.id, Universitas Kristen Indonesia, Indonesia
[2)] perdana.wahyu@yarsi.ac.id, Universitas YARSI, Indonesia
**) Corresponding Author*

ABSTRACT

Background: *The development of artificial intelligence (AI) technology has brought fundamental changes to various industrial sectors, including risk management practices. Conventional risk management systems are often considered inefficient in dealing with the complexity, dynamics, and uncertainty of the digital era. This drives the need for a new, more adaptive, predictive, and data-driven paradigm to improve the effectiveness of risk mitigation.*
Objectives*: This research aims to analyze the paradigm shift in risk management practices influenced by the development of AI technology, as well as to identify the contributions, challenges, and ethical implications of integrating AI in various industrial sectors.*
Methodology*: The research employed a qualitative approach, utilizing systematic literature reviews, cross-sectoral case studies, and inter-industry comparisons. The analysis was conducted descriptively and analytically to gain a holistic understanding of the application of AI in the risk management cycle, encompassing the identification, analysis, mitigation, and monitoring stages.*
Finding*: The study's findings demonstrate that AI integration significantly improves operational efficiency, risk prediction accuracy, and strategic decision-making acumen. These findings also highlight the importance of robust data governance, algorithmic transparency, and an ethical framework for the sustainable implementation of AI. The study's novelty lies in its comprehensive, cross-industry mapping of AI's role in the risk management cycle. The primary contribution of this research is to provide a theoretical foundation and practical implications for policymakers and practitioners in designing more responsive and responsible risk mitigation strategies in the era of digital transformation.*
Conclusion*: This study confirms that AI plays a central role in transforming the risk management paradigm from a reactive to a proactive and adaptive system. The research's novelty lies in its comprehensive, cross-industry mapping of AI's role in the risk management cycle. Its primary contribution is providing a theoretical foundation and practical implications for policymakers and practitioners in designing more responsive, transparent, and responsible risk mitigation strategies in the era of digital transformation.*

Keywords*: Risk Management; Artificial Intelligence; Digital Transformation; Data Governance; Cross-sector Case Studies.*

Submitted: 06-10-2025	Revised: 23-03-2026	Accepted: 15-04-2026

Article Doi:
http://dx.doi.org/10.22441/jurnal_mix.2026.v16i1.020

p-ISSN: 2088-1231
e-ISSN: 2460-5328

INTRODUCTION

Risk management is a systematic framework that integrates principles, frameworks, and processes to proactively identify, analyze, and control risks that may hinder organizational objectives (Ostapenko and Kholboeva 2021). When properly implemented, it not only protects organizational assets but also minimizes losses and creates opportunities for innovation and growth (Tambunan 2024a). In today's complex business environment—characterized by volatility, interconnected risks, and rapid technological change—traditional reactive approaches are no longer sufficient. Emerging risks such as cyberattacks, climate change, geopolitical instability, and technological disruption require more adaptive and integrated risk management systems (Eling, McShane, and Nguyen 2021; Ikudabo and Kumar 2024; Oktavianus, Naibaho, and Rantung 2023). This study addresses the gap between modern risk challenges and conventional approaches by examining the evolution of risk management and the integration of artificial intelligence (AI) to improve efficiency, accuracy, and effectiveness. It explores how risk management paradigms have shifted and how AI enhances strategic decision-making across sectors. Using a qualitative approach including literature review, cross-sector case studies, and comparative analysis this research develops an interpretive framework of these transformations and highlights the evolution of Enterprise Risk Management (ERM) toward more integrated systems (Popa et al. 2025). The study contributes theoretically by clarifying the relationship between AI and ERM evolution, and practically by offering strategic recommendations for developing intelligent, responsible, and sustainable risk management systems in the digital era (Manurung et al. 2021; Tambunan 2024a).

LITERATURE REVIEW

The concept of risk has evolved from early practices such as bottomry in ancient maritime trade to modern approaches based on quantitative analysis and organizational governance. (Mousavi, Ghazi, and Omaraee 2017). Developments in probability theory and statistics have enabled more accurate risk measurement in strategic decision-making. Standards such as ISO 31000 and ISO 31010 provide a systematic framework for identifying, analyzing, evaluating, and controlling risks (Manurung et al. 2021). This evolution has driven the emergence of Enterprise Risk Management (ERM), which integrates risk management across the organization and aligns it with strategic objectives (Putra et al. 2021). ERM emphasizes participation at all levels of the organization and managing risk appetite to achieve sustainable performance. Its implementation is crucial in sectors like banking, which face market, credit, operational, and liquidity risks (Tambunan 2024b; Yulianto et al. 2022). In the energy and infrastructure sector, risk management is a crucial aspect, given the characteristics of projects that are generally large-scale, capital-intensive, and have significant environmental and social impacts (Iso 2009). The main risks in this sector include project, construction, and operational risks, which require a comprehensive and multidimensional management approach (Bauerle et al. 2025; West, Turner, and Zhao 2010). Effective risk management is becoming increasingly important as the complexity of infrastructure and products handled increases, ensuring that the integrity and safety of design, construction, and operations are at an acceptable level of risk for the company and public pressure (Owczarski 2022). Similar approaches are also applied in the energy, infrastructure, healthcare and public sectors with analytical methods such as Monte Carlo, FMEA and Bowtie to improve the effectiveness of risk mitigation (Alshammari and Ghazali 2024; Caron 2013; Li et al. 2019).

p-ISSN: 2088-1231
e-ISSN: 2460-5328

Digital transformation and the development of artificial intelligence (AI) have significantly changed risk management practices (Eling et al. 2021). AI enables real-time analysis of large amounts of data, enhancing early risk detection capabilities by identifying patterns and anomalies that are difficult to recognize conventionally (Blum 2020; Idellie and Atok 2023). In addition, AI supports the automation of processes in the risk cycle from identification to monitoring thus increasing efficiency and accuracy, and allowing human resources to focus more on strategic decision-making (Ernis and Pirdaus 2022). This application is relevant across sectors, including finance, healthcare, and infrastructure, which face increasing risk complexity. The integration of risk management with organizational governance is becoming increasingly important, particularly through the active role of top management and the board in risk oversight (Manurung et al. 2021). In the digital era, cybersecurity and data protection issues have become key components of cross-sector risk management (Eling et al. 2021). Frameworks such as those developed by the National Institute of Standards and Technology (NIST) provide guidelines for strengthening cyber resilience and maintaining data integrity (Blum 2020; Herdiana, Munawar, and Putri 2021).

In the public sector, risk management is also closely linked to policies and their impact on the wider community, requiring a systematic approach such as that developed by the OECD. Overall, governance, ethics, and data management are essential foundations for ensuring that risk management implementation including AI-based risk management is carried out responsibly, securely, and sustainably (Huda and Suwahyu 2024).

METHOD

The research design used is multiple cross-sector case studies. A case study is a research design that focuses on collecting information about a specific object, event, or activity within an analysis unit. Information is collected to explain the analysis unit. In conducting research for this case study, the researcher must collect information from various perspectives that comprehensively explain the unit of analysis in accordance with the research objectives (Manurung et al. 2021; Tambunan 2024a). This approach is suitable for analyzing the interaction between AI technology and risk management systems, which vary depending on the sector and operational environment. The unit of analysis in this study is the organizational risk management system, particularly the integration of artificial intelligence within the risk lifecycle (identification, assessment, mitigation, and monitoring). Cases were selected using purposive sampling based on the following criteria: (1) the presence of AI implementation in risk management practices, (2) sectoral representation (technology, healthcare, finance, and public/government sectors), (3) availability of credible and accessible data sources, and (4) relevance to contemporary risk challenges such as cybersecurity, regulatory complexity, and digital transformation. This selection ensures analytical comparability while capturing contextual diversity.

Data collection was conducted through three main methods: systematic literature review, case study documentation, and in-depth interviews (Fink 2019). Secondary data constitute the primary source, including academic publications, industry reports, policy documents, and institutional publications related to AI-based risk management. Case documentation includes publicly available materials such as reports on digital tracing systems (e.g., TraceTogether in Singapore), AI-driven cybersecurity frameworks, and banking risk monitoring systems. Primary data were obtained, where applicable, through semi-structured in-depth interviews with an expert informant, Mr. Andri Puspo Heriyanto, whose expertise spans accounting,

p-ISSN: 2088-1231
e-ISSN: 2460-5328

information technology (digital forensics), and AI. To enhance validity and reliability, this study employs data triangulation by comparing findings across multiple sources (literature, case documents, and interviews). Methodological triangulation is also applied by integrating qualitative document analysis with expert insights. Additionally, source triangulation is conducted by cross-verifying information from academic, institutional, and industry perspectives to ensure consistency and reduce bias. Cross-case analysis was performed using a comparative thematic approach. Each case was first analyzed individually to identify key themes related to (1) risk management evolution and ERM practices, (2) AI capabilities within the risk lifecycle, and (3) governance, ethics, and data management. Subsequently, patterns, similarities, and differences across cases were systematically compared to identify common frameworks and sector-specific variations. Coding and categorization were guided by an analytical framework derived from the literature, allowing for both within-case depth and cross-case generalization.

RESULTS AND DISCUSSION

Results

Case Study of AI Implementation in Cross-Industry Risk Management Practices. As explained in the previous section, risk management practices have been widely implemented across various industrial sectors, including finance and banking, energy and infrastructure, healthcare and pharmaceuticals, information technology and cybersecurity, as well as government and public policy. (Manurung et al. 2021) presents several case studies that illustrate the application of ISO 31000 and risk management principles across various sectors, including financial institutions, manufacturing, infrastructure projects, healthcare, and information technology. This section presents selected real-world case studies from reliable sources. The case studies of AI implementation in cross-industry risk management practices demonstrate how artificial intelligence technology has been integrated into the risk management frameworks in these sectors.

1. Case Studies in the Financial and Banking Sector

Case studies in the financial and banking sector are sourced from HSBC & Google Cloud, "How HSBC fights money launderers with artificial intelligence" (cloud.google.com, quantexa.com, arxiv.org), BestPractice.ai, "HSBC reduces false positives for money laundering detection by 20% using AI" (bestpractice.ai), and Quantexa case, HSBC: decision intelligence platform (quantexa.com). Based on these sources, the case study related to HSBC Bank integrating AI into Anti-Money Laundering (AML) Risk Management is described and analyzed as follows:

Table 1. Evaluation of Risk Management Implementation at HSBC Bank

ISO 31000 Stage	HSBC Implementation
Risk Identification	AI expands the detection of suspicious patterns — more proactive and contextual.
Risk Analysis	The model assesses the severity and frequency of alerts in real time, replacing static rules.
Risk Evaluation	False positives—operational risks are identified and minimized through AI iteration.
Risk Treatment	Thresholds and models are adjusted based on team reviews—an adaptive system for continuous control.
Monitoring & Review	Real-time monitoring, integrated feedback loop, facilitating improvement and recalibration.

p-ISSN: 2088-1231
e-ISSN: 2460-5328

ISO 31000 Stage	HSBC Implementation
Communication & Consultation	AI results are presented to staff and auditors, providing auditable claims for internal and regulatory audits.

Source: Data processed (2025)

2. Case Study in the Energy and Infrastructure Sector

Case studies in the energy and infrastructure sector are sourced from Shell's expansion of predictive maintenance to 10,000 global units using the C3 AI platform (linkedin.com, c3.ai). Shell reports a reduction in unplanned downtime of approximately 20% and a decrease in maintenance costs of approximately 15% (energiesmedia.com). The implementation of AI has yielded significant results and impacts, including a reduction in downtime by more than 20% and a decrease in maintenance costs by approximately 15%, as well as improvements in safety and environmental protection due to a decrease in incidents caused by equipment failures and minimal potential for leaks or hazardous emissions. Additionally, operational efficiency has improved because interventions are based on accurate predictions, no longer following a fixed schedule, resulting in more optimal resource utilization.

Table 2. Evaluation of Risk Management Implementation at Shell

ISO 31000 Stage	Shell Implementation
Risk Identification	Sensors and models detect abnormal patterns that indicate risk.
Risk Analysis	AI evaluates the severity and probability of failure.
Risk Evaluation	Automatic prioritization of critical risk cases based on a scoring model.
Risk Treatment	Inspections and maintenance are triggered by predictions—preventive.
Monitoring & Review	The model's performance is proactively evaluated and continuously updated.
Communication & Consultation	Dashboards and periodic reports are delivered to stakeholders on a regular basis.

Source: Data processed (2025)

3. Case Studies in the Health and Pharmaceutical Sector

Case studies in the healthcare and pharmaceutical sector are sourced from Pfizer, "Applying AI and Other Tech to Monitor Medicine and Vaccine Safety" (pfizer.com), a study titled "Impact of AI Tools on Regulatory Reporting in Pharmacovigilance" (researchgate.net), and an Insight article "How AI Is Reshaping Pharmacovigilance" (linkedin.com). The implementation of AI in managing adverse event (AE) reports has produced significant impacts, with high efficiency achieved through a 50–60% reduction in processing time, as well as an increase in accuracy thanks to NLP technology and model learning, which reduces false positives and negatives. Additionally, responses to regulations have become faster, helping to maintain public trust and ensure compliance across various jurisdictions.

Table 3. Evaluation of Risk Management Implementation at Pfizer

ISO 31000 Stage	Pfizer AI-PV Implementation
Risk Identification	AI identifies early adverse event (AE) patterns that are difficult to capture through manual screening.
Risk Analysis	Data-driven risk scoring to prioritize cases with significant clinical impact.
Risk Evaluation	Prioritizing severe cases automatically helps focus mitigation efforts.
Risk Treatment	Quick follow-up on high-risk cases accelerates mitigation and notification.
Monitoring & Review	Models are evaluated periodically; updates minimize errors and adjust to the data context.

p-ISSN: 2088-1231
e-ISSN: 2460-5328

ISO 31000 Stage	Pfizer AI-PV Implementation
Communication & Consultation	Dashboard and reporting to regulators provide strong transparency and audit trails, ensuring accountability and compliance.

Source: Data processed (2025)

4. Case Study in the Information Technology and Cybersecurity Sector

Case studies in the information technology sector are sourced from: Drax Group case study via Darktrace: "Drax Group leveraged Darktrace AI …" (darktrace.com), Darktrace blog & report on AI cybersecurity trends (darktrace.com), Whitepaper "Towards Responsible AI in Cybersecurity" – principles of privacy and response (darktrace.com). The implementation of AI at Drax has produced significant impacts, including the early detection of advanced intrusions before conventional security systems can respond, a reduction in system disruption risks and regulatory compliance requirements, as well as enhanced operational resilience through the integrated protection of IT and OT systems to maintain the continuity of critical energy supply.

Table 4. Evaluation of Risk Management Implementation at Drax Group

ISO 31000 Stage	Drax dan Darktrace AI Implementation
Risk Identification	Automatic and real-time detection of IT & OT anomalies
Risk Analysis	In-depth probabilistic assessment of abnormal behavior
Risk Evaluation	Prioritization of threats by an AI scoring model with high severity scores
Risk Treatment	Antigen provides automatic isolation and mitigation during critical risk.
Monitoring & Review	The AI model is updated with feedback and human oversight.
Communication & Consultation	Threat visualization and SAR/SCAR discussions are conducted through the dashboard.

Source: Data processed (2025)

5. Case Studies in the Government and Public Policy Sector

Case studies in the government and public policy sector are sourced from the PMC Study on TraceTogether's efficacy and privacy dynamics (businessofgovernment.org, pmc.ncbi.nlm.nih.gov) and Evmi.com, as well as BMC Public Health (bmcpublichealth.biomedcentral.com). The implementation of AI in the contact tracing system has had a significant impact, accelerating contact identification from days to just a few hours and improving tracing accuracy, where 10% of contacts that were previously difficult to detect manually were successfully identified. Additionally, public compliance drastically increased, as evidenced by the adoption of Bluetooth tokens, which reached around 92% in 2021, making this system one of the most comprehensive AI-based tracking models in the world.

Table 5. Evaluation of the Implementation of Risk Management for the TraceTogether Application in Singapore

ISO 31000 Stage	TraceTogether AI Implementation
Risk Identification	Detecting potential transmission based on close contact automatically.
Risk Analysis	Categorizing risk levels with AI algorithms—high accuracy and real-time.
Risk Evaluation	Prioritize public actions and case notifications to ensure effective mitigation and response.
Risk Treatment	Execution of data-based tracing and quarantine—quickly reducing public risk.
Monitoring & Review	Analysis of adoption rates, data quality, and tracing effectiveness is conducted regularly.

p-ISSN: 2088-1231
e-ISSN: 2460-5328

ISO 31000 Stage	TraceTogether AI Implementation
Communication & Consultation	Reports to the government, regulators, and the public—supporting transparency and accountability.

Source: Data processed (2025)

Discussion

The HSBC Case Study

The implementation of artificial intelligence (AI) in the Anti-Money Laundering (AML) risk management system at HSBC Bank illustrates how financial institutions respond to increasing complexity in risk environments. The banking sector is inherently exposed to operational, compliance, and reputational risks, particularly in relation to financial crimes such as money laundering (Adhikari, Hamal, and Jnr 2024; Buchanan 2019; Patil 2024). High regulatory pressure and the potential systemic impact of failures necessitate more adaptive and data-driven risk management approaches. Rather than viewing this case in isolation, it reflects broader cross-sector patterns in AI adoption, particularly the use of advanced analytics to enhance risk detection and monitoring capabilities. The transition from rule-based systems to AI-driven models at HSBC enables more contextual identification of suspicious transactions. Reported outcomes, such as reduced false positives and increased detection rates, suggest potential efficiency gains; however, these findings should be interpreted cautiously given their reliance on secondary and context-specific data (Ikudabo and Kumar 2024). Similar patterns of data-driven anomaly detection are also observed in other sectors, including cybersecurity and infrastructure monitoring, indicating a general trend toward predictive and continuous risk assessment. At the same time, the financial sector demonstrates distinct characteristics compared to other industries. AI implementation in banking is strongly shaped by regulatory compliance and global standards, such as the Basel Accords, which emphasize internal risk oversight and systemic stability. Unlike sectors such as energy or healthcare, where operational continuity or safety outcomes dominate, financial institutions prioritize transaction monitoring accuracy and regulatory reporting. In this context, AI appears to function primarily as a complementary tool to established methods such as stress testing and Value at Risk (VaR), rather than a complete replacement.

However, the HSBC case also highlights limitations that are consistent across sectors. Challenges related to model risk, data bias, algorithmic transparency, and vendor dependency remain significant concerns. In addition, organizational factors such as resistance to change and varying levels of digital maturity can influence implementation outcomes. These issues underscore the importance of robust governance frameworks, human oversight, and continuous capability development. Overall, while AI adoption in this case indicates a shift toward more adaptive and data-driven risk management practices, its effectiveness remains contingent on sectoral context, data quality, and governance readiness. Therefore, generalizations about AI benefits should be approached with caution, particularly when based on heterogeneous secondary evidence. Future research is needed to strengthen the empirical and conceptual understanding of AI integration in risk management. Key areas include the development of an AI-ERM framework maturity model to assess organizational readiness, evaluation of governance and regulatory preparedness across sectors, and empirical testing in the Indonesian context to validate the applicability of these approaches in emerging markets.

The Shell Case Study

The application of artificial intelligence (AI) in operational risk management at Shell reflects how organizations in the energy and infrastructure sectors respond to high levels of complexity,

p-ISSN: 2088-1231
e-ISSN: 2460-5328

capital intensity, and exposure to environmental and social risks (Manurung et al. 2021; Tambunan 2024b). These characteristics necessitate risk management approaches that are not only comprehensive but also capable of handling large-scale and real-time operational data. When viewed in a broader cross-sector context, the Shell case exhibits common patterns observed in other industries, particularly the use of AI for predictive monitoring and early risk detection. Through the analysis of large volumes of sensor data across thousands of equipment units, AI enables the identification of anomalies that may indicate potential system failures. This approach is conceptually aligned with preventive frameworks such as Failure Mode and Effects Analysis, where risks are anticipated before they materialize. Reported outcomes, including reductions in downtime and maintenance costs, suggest potential operational benefits; however, these results should be interpreted with caution given their dependence on specific organizational settings and predominantly secondary data sources. At the same time, important sectoral differences emerge. In contrast to sectors such as finance or healthcare, where compliance and safety outcomes dominate, the energy sector places stronger emphasis on asset reliability, operational continuity, and infrastructure resilience. The integration of AI in this context is closely tied to physical systems and real-time industrial processes. Tools such as interactive dashboards and risk visualization mechanisms, which resemble Bowtie analysis, support decision-making by mapping causal pathways and control measures (Alshammari and Ghazali 2024). Furthermore, AI-based monitoring complements established analytical techniques such as Monte Carlo simulation by incorporating real-time data into risk scenario evaluation (Caron 2013; Husein and Majdi 2020).

Despite these advantages, similar limitations to those identified in other sectors are also evident. Challenges related to data quality, model interpretability, and system integration remain significant, particularly in environments with complex legacy systems. In addition, the reliance on automated systems raises concerns regarding over-dependence and the need for continued human oversight in critical operational decisions. These factors highlight that the effectiveness of AI in risk management is contingent upon governance structures, data infrastructure, and organizational readiness. Overall, the Shell case indicates a broader shift toward data-driven and adaptive risk management practices, but it does not suggest a uniform or universally applicable improvement across contexts. The observed outcomes are shaped by sector-specific conditions, technological maturity, and implementation strategies. Future research should further explore the integration of AI in risk management through the development of an AI-ERM framework maturity model, enabling systematic assessment of organizational capabilities. In addition, there is a need to evaluate governance readiness across sectors, particularly in relation to data management, ethical considerations, and regulatory compliance. Finally, empirical studies in the Indonesian context are essential to validate the applicability of these approaches in emerging economies with different institutional and technological environments.

The Pfizer Case Study

The case of Pfizer's implementation of artificial intelligence (AI) in pharmacovigilance illustrates how organizations in highly regulated sectors respond to increasing complexity in risk management. The healthcare and pharmaceutical industries face interconnected risks related to regulatory compliance, cost pressures, patient safety, and product quality (Noviriani and Mukaromah 2023). In this context, traditional manual systems for managing adverse event (AE) reports are often constrained by limitations in time, human resources, and processing capacity. The use of AI technologies, particularly Natural Language Processing (NLP) and

p-ISSN: 2088-1231
e-ISSN: 2460-5328

machine learning, enables the automation of data classification and analysis processes within pharmacovigilance systems. From a cross-sector perspective, this case reflects common patterns observed in other industries, especially the use of AI to support data-intensive risk identification, monitoring, and reporting processes. Similar to applications in finance and infrastructure, AI in pharmacovigilance facilitates the handling of large and complex datasets, allowing for faster detection of potential risk signals. Reported outcomes, such as reduced processing time and improved classification accuracy, indicate potential efficiency gains; however, these findings should be interpreted cautiously due to their reliance on secondary data and context-specific implementation conditions (Health 2023; Mualimah et al. 2021). At the same time, important sectoral differences are evident. Compared to sectors such as finance or energy, the pharmaceutical industry places stronger emphasis on clinical safety, regulatory compliance, and ethical responsibility. The role of human expertise remains critical, as final decision-making must involve healthcare professionals to ensure patient safety and maintain clinical integrity (Ardianto, Jati, and Nandini 2025). In addition, compliance with international regulatory bodies such as the FDA and EMA shapes how AI systems are designed, validated, and implemented within pharmacovigilance processes (Bucalo and Jereb 2017).

Despite its potential, the implementation of AI in this context also reveals challenges consistent with other sectors. Issues related to data quality (particularly unstructured data), model transparency, and the risk of overreliance on automated systems remain significant. These limitations highlight the importance of robust governance, continuous validation, and the integration of human oversight in AI-supported risk management systems. Overall, the Pfizer case suggests a broader shift toward data-driven and semi-automated risk management practices, but it does not imply uniform effectiveness across contexts. Outcomes are influenced by regulatory environments, data infrastructure, and organizational readiness. Therefore, the transferability of such approaches to other settings should be carefully evaluated. Future research should focus on developing an AI-ERM framework maturity model to assess the level of integration and capability across organizations. In addition, further studies are needed to evaluate governance readiness by sector, particularly in relation to ethical standards, data protection, and regulatory compliance. Finally, empirical research in the Indonesian context is essential to examine how AI-based pharmacovigilance and risk management systems can be adapted to local institutional, technological, and regulatory conditions.

The Drax Group Case Study

The Drax Group case study reflects the implementation of innovative, strategic, and highly relevant AI-based cyber risk management in the context of an increasingly integrated digital era. The organization's dependence on digital systems and network connectivity has increased its exposure to cyber threats, which not only impact financial and reputational aspects but also threaten the organization's overall operational continuity (Idellie and Atok 2023). As a major energy provider in the UK, Drax has adopted the Darktrace AI system to strengthen its cyber defenses through early detection, automated response, and continuous risk assessment. The implementation of Darktrace AI technology aligns with the principles outlined in the National Institute of Standards and Technology (NIST) framework, specifically emphasizing the need for technical control structures, formal procedures, and best practices to maintain the integrity of information systems (Herdiana et al. 2021). AI in the Darktrace platform is capable of recognizing normal behavior patterns of every device and network user, as well as detecting even the smallest deviations in real-time, even against previously undocumented zero-day

p-ISSN: 2088-1231
e-ISSN: 2460-5328

attacks. This platform provides a tactical advantage in anticipating potential security breaches before they cause significant damage.

Automatic responses through the Antigen module allow the system to take isolated actions without human intervention in the face of high-risk threats. This approach accelerates mitigation while simultaneously minimizing human error. On the other hand, the presence of the Threat Visualizer dashboard supports the principles of transparency and accountability, facilitating security audits and regular discussions among operational teams (Purba, Purnawan, and Pratama 2018). Drax has also successfully integrated the principles of a Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP) into its IT security architecture, ensuring operational continuity in the event of disruptions (Blum 2020). Protection is not only applicable in the IT (Information Technology) domain but also extends to OT (Operational Technology) systems that are directly connected to the physical electricity infrastructure, making Drax's cyber resilience an integral part of national energy resilience. However, this study also highlights important challenges, including privacy issues, the interpretability of black-box AI models, and the risk of over-reliance on automated systems. Considering that cybersecurity practices must align with regulations such as the General Data Protection Regulation (GDPR), systems like Darktrace should prioritize the principles of responsible AI, namely, algorithmic transparency, personal data protection, and human control in critical decision-making (Luo 2021). In conclusion, the integration of AI in Drax Group's cyber risk management system marks a paradigm shift from reactive security systems to predictive, adaptive, and autonomous systems. This approach not only enhances the effectiveness of detection and response but also demonstrates the importance of responsibly adopting intelligent technology to protect the organization's continuity in an ever-evolving digital threat landscape. This case can serve as a strategic reference for other organizations, especially those managing critical infrastructure, in building layered security systems that leverage collaboration between advanced technology and mature risk governance.

The Covid-19 Case Study in Singapore

The case of the Singaporean Government's implementation of the AI-based contact tracing system TraceTogether during the COVID-19 pandemic represents a model of strategic and widely impactful technology-based risk management in the public sector. In the context of governance, policies related to public health, such as pandemic tracking, are complex, dynamic, and potentially multidimensional in their consequences if not managed properly. In line with the public policy risk management model developed by the OECD, the TraceTogether system highlights the importance of a structured and systematic process for identifying, assessing, and mitigating risks in national crisis governance. By detecting potential transmission based on digital interactions between users, TraceTogether successfully reduced tracking time from days to just a few hours. This AI demonstrates the effectiveness of a technological approach in accelerating the response cycle to public health risks. Moreover, the AI algorithms used are capable of analyzing contact intensity and providing real-time risk classification, allowing the government to prioritize mitigation actions efficiently and accurately.

The implementation of this risk management not only encompasses technical dimensions but also touches on social and regulatory aspects. Public concerns about data privacy and the use of information by law enforcement agencies pose a significant trust challenge that must be addressed through the principles of transparency and accountability. The Singaporean government is addressing this issue through public communication, legislative consultation, and the development of physical tokens as part of its effort to promote digital inclusion,

p-ISSN: 2088-1231
e-ISSN: 2460-5328

particularly for communities without access to smart devices. This approach underscores the importance of adaptive policy risk management within a social and ethical context. From the perspective of digital governance, the existence of TraceTogether also opens important discussions regarding the protection of information systems and cybersecurity in the public sector. As noted by (Admi and Maulana 2020), government agencies are vulnerable to cyberattacks due to the large volume of sensitive data they manage and process. Therefore, in addition to focusing on health risks, this system must also prioritize system integrity and the associated digital vulnerabilities (Herdiana et al. 2021). Overall, the implementation of TraceTogether demonstrates that risk management in the government sector cannot be separated from technological factors, regulations, public participation, and the evolving social context. The success of this system in reducing pandemic risks and enhancing the effectiveness of public policies makes it a crucial case study on how AI can be responsibly utilized to support risk-based decision-making in the government sector.

CONCLUSION

From the research results, three conclusions can be drawn:

A. Key Findings

1. Risk management has evolved toward more integrated and data-driven approaches across sectors, driven by increasing complexity, regulatory pressure, and technological advancement.
2. Artificial intelligence (AI) shows potential in supporting risk identification, monitoring, and decision-making processes, although outcomes vary depending on sectoral context and data maturity.
3. Common challenges across sectors include algorithmic bias, limited model transparency, data governance issues, and the risk of over-reliance on automated systems.
4. The effectiveness of AI in risk management is contingent on organizational readiness, including data infrastructure, governance quality, and human resource capabilities.

B. Practical Implications

1. Organizations should adopt a balanced AI integration strategy, combining technological capabilities with strong governance, data management, and human oversight.
2. Investment in data infrastructure and workforce competencies is essential to support effective and responsible AI-based risk management.

C. Policy Implications

1. Policymakers should develop clear regulatory frameworks for AI governance, emphasizing transparency, accountability, and data protection.
2. Cross-sector collaboration is needed to establish standardized guidelines and best practices for AI-based risk management, particularly in high-risk and critical sectors.

REFERENCES

Adhikari, Prabin, Prashamsa Hamal, and Francis Baidoo Jnr. 2024. "Artificial Intelligence in Fraud Detection: Revolutionizing Financial Security." International Journal of Science and Research Archive *13(01):1457–72.*

Admi, Adrian, and Abdul Hakim Nur Maulana. 2020. "Penerapan Elastic Stack Sebagai Tools Alternatif Pemantauan Traffic Jaringan Dan Host Pada Instansi Pemerintah Untuk Memperkuat Keamanan Dan Ketahanan Siber Indonesia." JUSTINDO (Jurnal Sistem &

Teknologi Informasi Indonesia) *5(2):69–77.*

Alshammari, Adel, and Farid E. Mohamed Ghazali. 2024. "A Comprehensive Review of the Factors and Strategies to Mitigate Construction Projects Delays in Saudi Arabia." The Open Construction & Building Technology Journal *18(1).*

Ardianto, Yoga Dwi, Sutopo Patria Jati, and Nurhasmadiar Nandini. 2025. "Analisis Kebutuhan Pelatihan Berdasarkan Kemampuan Kerja Jabatan (KKJ) Dan Kemampuan Kerja Pribadi (KKP) Petugas Klinik Satmoko." MEDIA KESEHATAN MASYARAKAT INDONESIA *20(4):283–90.*

Bauerle, Tim, Tashina Robinson, Alison Hunt, and Yongli Zhao. 2025. "The Prevalence of Risk Factors for Work-Related Fatigue in the US Mining Industry: A Brief Literature Review and Exploratory Investigation of Public Data Sets." Available at SSRN 5030595.

Blum, Dan. 2020. "Institute Resilience Through Detection, Response, and Recovery." Pp. 259–95 in Rational Cybersecurity for Business. *Berkeley, CA: Apress.*

Bucalo, Nina, and Borut Jereb. 2017. "Risk Management in the Pharmaceutical Industry in Slovenian Companies." Logistics & Sustainable Transport *8(1):42–49. doi: 10.1515/jlst-2017-0004.*

Buchanan, Bonnie G. 2019. "Artificial Intelligence in Finance."

Caron, Franco. 2013. "Project Risk Analysis and Management." Pp. 35–36 in Managing the Continuum: Certainty, Uncertainty, Unpredictability in Large Engineering Projects. *Milano: Springer Milan.*

Eling, Martin, Michael McShane, and Trung Nguyen. 2021. "Cyber Risk Management: History and Future Research Directions." Risk Management and Insurance Review *24(1):93–125. doi: 10.1111/rmir.12169.*

Ernis, Putri Dwima, and Padli Pirdaus. 2022. "Dampak Teknologi Artificial Intelligence Pada Profesi Akuntansi." EKOMA: Jurnal Ekonomi, Manajemen, Akuntansi *2(1):131–37.*

Fink, Arlene. 2019. Conducting Research Literature Reviews: From the Internet to Paper. *Sage publications.*

Health, Center for Devices and Radiological. 2023. "VENTANA PD-L1 (SP263) Assay – P160046/S013." FDA.

Herdiana, Yudi, Zen Munawar, and Novianti Indah Putri. 2021. "Mitigasi Ancaman Resiko Keamanan Siber Di Masa Pandemi Covid-19." Jurnal ICT: Information Communication & Technology *21(1):42–52.*

Huda, Miftahul, and Irwansyah Suwahyu. 2024. "Peran Artificial Intelligence (Ai) Dalam Pembelajaran Pendidikan Agama Islam." REFERENSI ISLAMIKA: Jurnal Studi Islam *2(2):53–61.*

Husein, Akeel A., and Ali Majdi. 2020. "Assessment of Risk Management and Evaluate the Level of Risk in Construction Project: Case Study."

Idellie, Putri Lathifah, and Raden Mohamad Atok. 2023. "Pemodelan Distribusi Kerugian Siber Dengan Pendekatan Copula Dan Perhitungan Premi Asuransi Siber." Jurnal Sains Dan Seni ITS *12(1):D1–7.*

Ikudabo, Ayodeji Oyindamola, and Pravin Kumar. 2024. "AI-Driven Risk Assessment and Management in Banking: Balancing Innovation and Security." International Journal of Research Publication and Reviews *5(10):3573–88.*

Iso, I. 2009. "Risk Management–Principles and Guidelines." International Organization for Standardization, Geneva, Switzerland.

Li, Fei, Meixuan Song, Linxia Xu, Bo Deng, Shiqin Zhu, and Xianrong Li. 2019. "Risk Factors for Catheter-associated Urinary Tract Infection among Hospitalized Patients: A

p-ISSN: 2088-1231
e-ISSN: 2460-5328

Systematic Review and Meta-analysis of Observational Studies." Journal of Advanced Nursing *75(3):517–27. doi: 10.1111/jan.13863.*

Luo, Yadong. 2021. "A General Framework of Digitization Risks in International Business." Journal of International Business Studies *53(2):344.*

Manurung, Adler Haymans, David Tjahjana, Christian Haposan Pangaribuan, and Martua Eliakim Tambunan. 2021. "Metode Riset: Akuntansi, Investasi Keuangan Dan Manajemen."

Mousavi, Majid, Iran Ghazi, and Behrooz Omaraee. 2017. "Risk Assessment in the Maritime Industry." Engineering, Technology & Applied Science Research *7(1):1377–81.*

Mualimah, Siti, Rizki Yeni Wulandari, Ikhwan Amirudin, and Ardinata Ardinata. 2021. "Hubungan Tingkat Pengetahuan Perawat Terhadap Identifikasi Patient Safety Di Ruang Rawat Inap Rumah Sakit Permata Hati Lampung Timur." Journal of Current Health Sciences *1(1):29–34.*

Noviriani, Eliza, and Lailatul Mukaromah. 2023. "Studi Literatur Industrialisasi Dalam Perekonomian Indonesia." Jurnal Ekuilnomi *5(1):109–15.*

Oktavianus, Arnolus Juantri E., Lamhot Naibaho, and Djoys Anneke Rantung. 2023. "Pemanfaatan Artificial Intelligence Pada Pembelajaran Dan Asesmen Di Era Digitalisasi." Jurnal Kridatama Sains Dan Teknologi *5(02):473–86.*

Ostapenko, Maria, and Umida Kholboeva. 2021. "Analysis of the Effectiveness of Quality Management Tools Aimed at Risk-Management of Organizations." P. 3054 in Vol. 346. EDP Sciences.

Owczarski, Kimberly. 2022. "Toward a 'New Normal': A Case Study of the Pandemic's Effect on Film Exhibition." Popular Culture Review *33(2):1–40. doi: 10.18278/pcr.33.2.2.*

Patil, Dimple. 2024. "Artificial Intelligence In Financial Risk Assessment And Fraud Detection: Opportunities And Ethical Concerns." Available at SSRN 5057434.

Popa, Ion, Simona Cătălina Ştefan, Andrei Josan, Corina-Elena Mircioiu, and Nicoleta Căruceru. 2025. "Artificial Intelligence as a Catalyst for Management System Adaptability, Agility and Resilience: Mapping the Research Agenda." Systems *13(1):47.*

Purba, A. David, I. K. Adi Purnawan, and I. P. Agus Eka Pratama. 2018. "Audit Keamanan TI Menggunakan Standar ISO/IEC 27002 Dengan COBIT 5." J. Ilm. Merpati (Menara Penelit. Akad. Teknol. Informasi) *6(3):148.*

Putra, Ardi, Dhani Akbar, Ryan Anggria Pratama, and Derlina Siregar. 2021. "Manajemen Risiko Perusahaan Tambang Di Wilayah Kabupaten Karimun Riau: Sebuah Review Implementasi Standar Internasional." Equilibrium: Jurnal Pendidikan *9(2):228–34.*

Tambunan, Martua Eliakim. 2024a. "Manajemen Risiko: Dasar-Dasar, Strategi, Dan Aplikasi Praktis."

Tambunan, Martua Eliakim. 2024b. "Manajemen Risiko Keuangan: Mitigasi Risiko Dalam Investasi Dan Perbankan."

West, Richard L., Lynn H. Turner, and Gang Zhao. 2010. Introducing Communication Theory: Analysis and Application. *Vol. 2. McGraw-Hill New York, NY.*

Yulianto, Erwin, Iman Sudirman, Azhar Affandi Sutarman, Sidik Priadana, and Ina Primiana Sagir. 2022. "Implementasi Integrasi Fungsi-Fungsi Bisnis Pada Kinerja Proses Bisnis Internal Menggunakan Metode Kualitatif Dengan Pendekatan Quantitative Strategic Planning Matrix." Business Innovation and Entrepreneurship Journal *4(1):68–73.*