ZESZYTY NAUKOWE POLITECHNIKI POZNAŃSKIEJ
Nr 92 Organizacja i Zarządzanie 2025

Łukasz PACEK[1], Barbara MRÓZ-GORGOŃ[2], Marcin CZUGAN[3]

RISK MANAGEMENT IN AN ORGANIZATION IN THE ERA OF AI – A THEORETICAL APPROACH

DOI: 10.21008/j.0239-9415.2025.092.03

In an era marked by complex global interdependencies, organizational risk management has emerged as a key strategic function. Risk is no longer confined to financial loss or operational disruption but encompasses a wide spectrum of uncertainties with implications for long-term sustainability and competitiveness. Traditional approaches, including ISO 31000 and COSO ERM, emphasize risk identification, evaluation, and mitigation within a structured governance framework. However, recent technological advancements, particularly in the field of artificial intelligence (AI), have introduced new paradigms in how risks are perceived, predicted, and managed. The primary aim of article is to systematize core definitions, clarify key theoretical frameworks, and identify unresolved questions through a comprehensive review of contemporary academic literature. This article provides a comprehensive theoretical overview of organizational risk management while integrating AI-driven tools and approaches. The main conclusions of the article indicate that risk management has undergone a transformation from a reactive to a proactive approach. Today's organizations not only respond to risk, but learn to anticipate and exploit it. In addition, the use of AI significantly increases organizational capabilities in the field of risk identification, analysis and control. On the other hand, integrating AI brings ethical and systemic challenges, and risk management alone in the future requires hybrid intelligence. The conclusions drawn are theoretical – further empirical research is needed.

Keywords: enterprise risk management, AI in risk analysis, predictive analytics and risk, machine learning for compliance, digital transformation in risk governance

[1] Wroclaw University of Economics and Business, Faculty of Management. ORCID: 0009-0006-1332-345X.

[2] Wroclaw University of Economics and Business. ORCID: 0000-0001-9116-485X.

[3] Wroclaw University of Economics and Business, Faculty of Management.

1. INTRODUCTION

Operating in a volatile, uncertain, complex, and ambiguous (VUCA) environment, modern organizations face a continuously evolving array of risks. These range from geopolitical instability and cyber threats to supply chain disruptions and regulatory changes. The ability to anticipate and manage such risks is critical not only for an organization's survival but also for sustained competitive advantage (Aven, 2023). Risk is no longer viewed solely as a negative occurrence to be mitigated; contemporary management theory increasingly recognizes it as a dual-edged phenomenon capable of generating opportunity as well as loss.

Traditional approaches to risk management, including ISO 31000 and COSO ERM, provide structured methodologies for identifying, assessing, and responding to threats within a governance framework. These systems have contributed to standardizing risk practices across sectors, promoting consistency and accountability. However, the dynamic nature of today's risk landscape demands more than procedural compliance and static models. Rapid shifts in market behaviour, technological innovation, and environmental volatility call for adaptable, data-driven approaches.

Artificial intelligence is becoming a cornerstone of this evolution. AI-powered tools such as machine learning algorithms, natural language processing systems, and predictive analytics engines offer organizations powerful means of interpreting complex datasets and forecasting risk scenarios in real time (Brock, von Wangenheim, 2019; Ghosh, 2023). For instance, AI can detect early warning signals in financial trends, automate the monitoring of regulatory compliance, and model the potential impacts of disruptive events such as pandemics or cyberattacks (Shrestha, Ben-Menahem, von Krogh, 2019).

The integration of AI into risk management signifies a fundamental shift – from a retrospective, reactive orientation to one that is proactive and forward-looking. Rather than merely mitigating adverse events after they occur, organizations can now anticipate and prepare for risks with a high degree of accuracy. This shift has profound implications for enterprise strategy, resource allocation, and operational agility.

However, the adoption of AI also raises critical questions about transparency, ethical oversight, and systemic risk. AI systems, particularly those based on complex machine learning models, can act as "black boxes", producing outputs that are difficult to interpret or audit (Rudin, 2019). Moreover, if not carefully governed, algorithmic decision-making can reinforce bias or introduce unintended vulnerabilities (O'Neil, 2016).

This article seeks to explore both the theoretical underpinnings and practical implications of AI-augmented risk management. By combining traditional models with emerging technologies, it aims to contribute to a new paradigm in which human judgment and artificial intelligence work in tandem to enhance resilience and strategic foresight in modern organizations.

2. RESEARCH METHODOLOGY

This article is based on a qualitative research design employing a systematic literature review (SLR) methodology. The primary objective of the review is to examine the evolution of risk management theories and practices in organizational contexts, with a particular emphasis on the integration of artificial intelligence (AI) into risk management frameworks. This methodological approach was chosen due to its effectiveness in identifying conceptual patterns, mapping theoretical development, and synthesizing findings across diverse disciplines (Tranfield, Denyer, Smart, 2003).

The literature search was conducted across multiple scholarly databases, including Scopus, Web of Science, ScienceDirect, JSTOR, and Google Scholar. To ensure relevance and academic rigor, only peer-reviewed journal articles, academic books, and institutional research reports published between 2015 and 2024 were included. Key search terms utilized in the query process included: “enterprise risk management”, “AI in risk analysis”, “predictive analytics and risk”, “machine learning for compliance”, and “digital transformation in risk governance”.

The inclusion criteria focused on publications that address risk management models (such as COSO ERM, ISO 31000, and the Three Lines Model), empirical and theoretical studies on AI applications in business contexts, and interdisciplinary works bridging management, information systems, and computational sciences. Excluded were non-peer-reviewed articles, non-English sources, and practitioner blogs without scientific validation and MDPI publications.

To supplement the academic sources, recent bibliometric analyses were also reviewed to track the volume and trajectory of scholarly work relating to AI in enterprise risk management (Felch, Asdecker, 2022). These analyses revealed a growing yet fragmented body of research, underscoring the need for a comprehensive theoretical framework that unifies classical risk management principles with contemporary AI capabilities.

Following the guidelines of the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA), the study involved four stages: identification, screening, eligibility assessment, and inclusion. The selected literature was then analysed through thematic coding to extract recurring themes, critical challenges, and proposed solutions regarding the intersection of AI and risk management.

This methodological approach allows the article to synthesize both foundational theory and emergent technological practice. It serves as a basis for proposing a future-oriented framework for AI-augmented risk management – one grounded in empirical trends and guided by ethical governance.

3. RISK MANAGEMENT IN THEORY AND PRACTICE

Risk management, as a discipline, has evolved significantly over the past decades – from a narrowly defined, reactive approach centred on compliance and loss prevention to a dynamic, enterprise-wide function with strategic significance. Traditionally, risk has been defined as the probability of an adverse event negatively affecting an organization's operations or strategic objectives. In early models, risk was framed primarily as a threat – something to avoid or mitigate through control systems, audits, or insurance (Aven, 2023).

Contemporary theory, however, acknowledges a more nuanced understanding: risk embodies not only threats but also potential opportunities. In the strategic management literature, this duality is essential. Uncertainty, when properly managed, can lead to innovation, competitive advantage, and long-term growth. This shift is reflected in the widespread adoption of frameworks such as ISO 31000 and COSO ERM, which advocate a systematic approach to identifying, analysing, evaluating, treating, and monitoring risk across all levels of the organization (COSO, Deloitte, 2019).

These frameworks also foster the integration of risk management into corporate governance and decision-making processes, enabling risk-informed strategies that balance performance with resilience. COSO ERM, for example, emphasizes the importance of aligning risk appetite with value creation, while ISO 31000 stresses the need for contextual and continuous risk assessment.

Artificial intelligence introduces a new dimension to these practices by expanding the analytical capabilities of organizations beyond human constraints. AI tools can ingest vast amounts of structured and unstructured data – ranging from financial metrics and operational performance indicators to geopolitical developments and social media sentiment – and extract patterns that would be imperceptible to traditional human analysis (Brock, von Wangenheim, 2019; Shrestha et al., 2019).

For example, predictive analytics enables firms to forecast potential disruptions such as supply chain bottlenecks, cyber threats, or regulatory shifts. Machine learning algorithms improve over time by learning from new data, refining risk models, and reducing false positives. Natural language processing (NLP) tools automatically review policy documents, legal contracts, or news articles to flag emerging risks or compliance gaps (IBM Security, 2021).

By automating routine tasks, AI frees risk managers to focus on strategic insights and scenario planning. Furthermore, real-time anomaly detection systems facilitate an immediate response to irregularities in financial transactions, IT systems, or employee behaviour – providing early warnings that can prevent cascading failures (Ghosh, 2023). In this way, AI elevates risk management from an auxiliary function to a core component of strategic foresight.

However, this integration does not negate the importance of human judgment. The most effective models emphasize collaborative intelligence, where human decision-makers interpret AI outputs within a broader strategic and ethical framework (Davenport, Ronanki, 2018). Risk, in this integrated model, is not just an operational concern but a dynamic element of innovation and adaptation.

In sum, modern risk management theory acknowledges that uncertainty is not merely a problem to be solved, but a condition to be navigated with insight, agility, and increasingly, algorithmic assistance. The incorporation of AI into these frameworks marks a critical evolution – one that reflects the complexity and pace of risks facing 21st-century organizations.

4. RESEARCH FINDINGS: NEW ERA OF RISK MANAGEMENT IN ORGANIZATIONS – A REVIEW OF DEFINITIONS

Risk can be defined as “the possibility that something will not succeed, an undertaking whose outcome is unknown” (Woźniak, Szalbo, 2003). More broadly, it is understood as a measure of uncertainty regarding future outcomes resulting from a specific event (Dubisz, 2008; Wojniłko, Sikorska-Michalak, 1996; Sobolewski, Marcinkowski, 2017). In colloquial terms, risk is perceived primarily as a situation whose occurrence leads to loss, creates problems, limits, or prevents the achievement of planned objectives. The etymology of the word “risk” supports this negative interpretation, with its roots in Latin, Italian, or Greek, each connoting danger, courage, or potential failure (Campbell, 2005; Willis, 2007; Graham, Weiner, 1995). Such origins contribute to the traditional view of risk as disutility or loss – an approach widely reflected in early literature on risk (Filipiak, 2010; Peter-Bombik, 2023).

Within decision theory, risk is conceptualized as a situation involving uncertainty about future developments, but also the availability of probabilistic knowledge regarding potential outcomes (Buschgen, 1997). In this sense, risk becomes not only a threat but also a calculated exposure to possibility. This is especially relevant in enterprise environments where every initiative entails a combination of potential opportunity and potential threat (FERMA, 2003). Achieving economic success depends on risk-taking – “no risk, no reward” – though such risks must be strategically managed and mitigated (Sobel, 2004).

Management science emphasizes this duality. Risk can be seen as either a purely negative phenomenon – uncertainty and the probability of failure, damage, or loss – or through a neutral lens that recognizes both threats and opportunities (Jajuga, 2007; Pleczeluk, 2011; Zasępa, 2013; Małkowska-Borowczyk, 2012; Urbanowska-Sojkin, 2012; Bartkowiak, Koszel, 2013; Rudawska, 2013). Financial literature has widely adopted this neutral stance, describing “good risk” (opportunity) and “bad risk” (threat) in analogous terms to beneficial and harmful cholesterol (Kasiewicz, Rogowski, 2006, 2009; Kasiewicz, 2011).

Risk management is thus defined as the process of making decisions and implementing actions to achieve an acceptable level of risk. It forms an element of comprehensive enterprise management and is central to organizational strategy (Peter-Bombik, 2023). The process includes risk identification, measurement, control, and monitoring. Strategic and systematic risk management enables leadership to deal with uncertainty, enhance decision-making, and protect stakeholder value (AIRMIC, ALARM, IRM, 2010; Samborski, 2012).

Organizations such as FERMA and COSO emphasize that risk management is central to strategy setting and operational control. FERMA (2003) views enterprise risk management as a methodical approach to addressing risks at all organizational levels to ensure sustainable benefits. COSO (2006) defines ERM as a process, implemented across the enterprise, for identifying potential events and managing risk within the organization's appetite, in order to provide reasonable assurance regarding goal attainment (Nowak, 2014). The Institute of Internal Auditors (IIA) and the International Federation of Accountants (IFAC) offer complementary definitions focused on maximizing organizational value while controlling risk exposure across operational, strategic, financial, and reputational domains (International Federation of Accountants, 2009; Sobolewski, 2017).

In practice, risk management enables organizations to realize benefits such as improved goal achievement, stakeholder trust, strategic agility, reduced surprises and losses, optimized resource allocation, and increased resilience (Chapman, 2011; Marcinkowski, 2016; Merna, Al-Thani, 2011; Olson, Wu, 2010). Arena et al. (2010) identify eight stages in the risk process from defining risk attitude and identifying events to continuous monitoring and feedback – a model reflecting complexity and strategic importance (Nowak, 2014).

Moreover, authors such as Jajuga (2007), Makarowski (2008), and Moeller (2011) define risk management as a multistage process of identification, assessment, control, and monitoring, all aimed at delivering long-term enterprise value.

Artificial Intelligence now significantly reshapes this landscape. AI systems offer capabilities that traditional models cannot: real-time data processing, automated risk classification, predictive modelling, and natural language processing to scan regulations or legal documents for emerging compliance threats (Brock, von Wangenheim, 2019; IBM Security, 2021). Machine learning algorithms can autonomously detect behavioural anomalies, assess risk patterns, and improve over time with new data. These tools turn static, cyclical risk frameworks into adaptive, dynamic systems that support continuous risk intelligence.

The integration of AI also necessitates a rethinking of risk agency and responsibility. With AI participating in both detection and decision-making, transparency becomes critical. Critics warn of "black box" models that lack explainability, potentially reinforcing bias or operational vulnerabilities if not subject to governance (Rudin, 2019; O'Neil, 2016). Thus, AI introduces not only capability but ethical complexity.

In summary, the definition of risk and its management is no longer confined to traditional frameworks. AI extends and transforms both concepts, demanding new theoretical models that combine human oversight with autonomous analytical capability. Future-oriented risk management requires this hybrid intelligence to address the fast-paced, data-saturated, and uncertain environments modern enterprises now face.

5. RISK MANAGEMENT MODELS AND AI ENHANCEMENT

The key to effective risk management lies in adopting a structured, repeatable model that organizes and sequences the process. Risk management models serve not only as conceptual frameworks but also as operational guides. Their application enhances the ability to identify, assess, control, and monitor risks systematically and consistently.

Among the most widely recognized and applied models is the Three Lines Model, presented by the Institute of Internal Auditors (IIA), which distinguishes between three fundamental levels of responsibility:

- the first line (operational management),
- the second line (risk and compliance functions),
- the third line (internal audit).

This model emphasizes the clear division of duties and responsibilities between risk creators, controllers, and independent assessors, creating a robust defence-in-depth strategy within the organization.

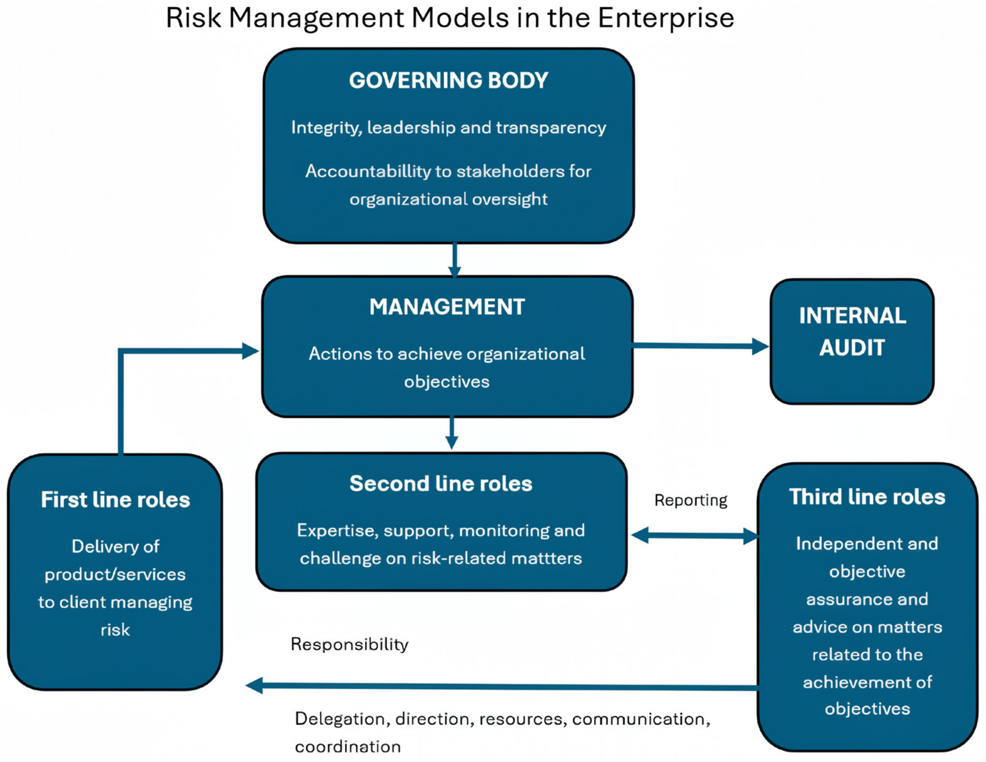
Risk Management Models in the Enterprise
GOVERNING BODY
Integrity, leadership and transparency
Accountabillity to stakeholders for organizational oversight
MANAGEMENT
Actions to achieve organizational objectives
INTERNAL AUDIT
First line roles
Delivery of product/services to client managing risk
Second line roles
Expertise, support, monitoring and challenge on risk-related mattters
Reporting
Third line roles
Independent and objective assurance and advice on matters related to the achievement of objectives
Responsibility
Delegation, direction, resources, communication, coordination

Fig. 1. The Three Lines Model of Risk Management (on the basis of "The Institute of Internal Auditors", 2020, AI-generated)

This model assumes the existence of consistent communication and cooperation between these three levels and, more broadly, the embedding of risk management within the organization's strategic planning and operational execution (Nowak, 2014).

In addition to the Three Lines Model, risk management literature (both Polish and international) emphasizes cyclical models. One of the most comprehensive is the eight-step model proposed by Arena et al. (2010), which includes:

1) defining the organization's risk attitude,
2) determining objectives for individual organizational units,
3) identifying internal and external events,
4) risk assessment (probability and impact),
5) developing actions aligned with the organization's risk appetite,
6) applying control activities,
7) ensuring effective communication flows,
8) monitoring and continuous improvement (Nowak, 2014).

This cyclicality is also emphasized by Polish scholars such as Jajuga (2007) and Moeller (2011), who see risk management as an ongoing process embedded in enterprise strategy and decision-making.

With the emergence of artificial intelligence (AI), these traditional models are not discarded but rather extended and enhanced.

AI tools such as machine learning, predictive analytics, and natural language processing now enrich traditional frameworks in ways previously unfeasible. For instance:

- In the first line, operational managers can utilize AI-powered dashboards to receive real-time alerts from key risk indicators.
- In the second line, compliance officers apply natural language processing to scan new legislation or regulations and automatically align internal policies.
- In the third line, internal auditors deploy anomaly detection tools to flag potential irregularities in financial records or supply chains (IBM Security, 2021).

In the ISO 31000 standard, which promotes a principle-based, organizationally integrated approach to risk, AI enables dynamic context awareness. Risk assessments no longer rely solely on historical or subjective analysis; instead, real-time data streams and probabilistic modelling now support risk identification, evaluation, and treatment in continually shifting environments.

Likewise, COSO's emphasis on performance, strategy, and risk appetite is strengthened by AI's predictive capabilities. Strategic scenario modelling – once manually executed through static spreadsheets – is now handled by AI platforms that simulate thousands of outcome combinations and recommend optimal courses of action (Davenport, Ronanki, 2018; Shrestha et al., 2019).

Importantly, AI does not eliminate the need for human judgment. These models reinforce the need for hybrid decision environments, where automated systems assist (but do not override) the decision-making autonomy and ethical responsibility of human leaders (Rudin, 2019; O'Neil, 2016).

Thus, risk management models evolve from cyclical diagrams to intelligent, learning ecosystems. The structured foundation remains, but the tools – driven by AI – make these systems faster, smarter, and more adaptive to complex, nonlinear risk environments.

6. SUMMARY

This article examined risk management as a central strategic discipline for organizations operating in environments defined by complexity, globalization, technological disruption, and accelerating uncertainty. The primary aim was to systematize core definitions, clarify key theoretical frameworks, and identify unresolved questions through a comprehensive review of contemporary academic literature.

The findings reveal significant terminological inconsistency and ongoing debate regarding the very definition of "risk". However, there is a growing consensus around a more nuanced, neutral view of risk – not only as a threat to be mitigated, but also as a potential source of opportunity and innovation. This shift underscores a broader redefinition of risk management, from a defensive mechanism to a proactive instrument for enabling strategic foresight and resilience.

Key frameworks – including COSO ERM, ISO 31000, and the Three Lines Model – offer important structural guidance, advocating integrated, governance-aligned approaches to managing risk. Despite their strengths, these models also exhibit fragmentation, implementation challenges, and insufficient responsiveness to unstructured, dynamic environments. Their real-world applicability may be further limited by rigid procedural design, especially in fast-evolving or data-intensive contexts.

This limitation highlights the transformative role of artificial intelligence (AI) in expanding the reach and capability of modern risk systems. AI tools such as machine learning, real-time anomaly detection, and natural language processing can be integrated into traditional risk models to enable adaptive, predictive, and data-driven decision-making. These technologies have the potential to overcome human limitations in perception and scale, equipping organizations with tools for real-time monitoring, automated compliance, and advanced scenario planning.

At the same time, the adoption of AI introduces a new layer of complexity. The lack of transparency in black-box models, the risk of embedded algorithmic bias, and the ethical implications of automated decision-making require strong governance mechanisms, explainable AI (XAI) frameworks, and interdisciplinary oversight. These issues, while addressed conceptually in emerging literature, lack sufficient empirical validation in real organizational settings.

This brings us to the methodological limitations of this study. The findings are based exclusively on a systematic literature review, without empirical data collection or case study verification. The review's scope – limited to academic sources published between 2018 and 2024 – may have excluded relevant industry reports, sector-specific innovations, and non-English-language contributions. Moreover, the absence of a quantitative meta-analysis means that the conclusions are qualitative and conceptual, offering insights but not statistically generalizable evidence.

Therefore, future research should address several critical gaps:

- conduct empirical studies to test and validate AI-augmented risk models in diverse organizational contexts,
- develop implementation frameworks for the practical integration of AI with existing risk structures,
- apply quantitative simulation tools, such as agent-based modelling, to assess risk propagation and mitigation dynamics,
- explore the governance, legal, and ethical dimensions of AI in risk-sensitive areas,
- examine how organizational maturity influences the success of AI-based risk strategies.

In sum, risk management today stands at a crossroads. Classical models offer tested stability; AI brings unprecedented power. The challenge lies in synthesizing these domains to build agile, transparent, and intelligent systems that not only protect organizations but also help them thrive in a future defined by both uncertainty and opportunity.

LITERATURE

AIRMIC, ALARM, IRM (2010). A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000. Institute of Risk Management.

Arena, M., Arnaboldi, M., Azzone, G. (2010). The organizational dynamics of Enterprise Risk Management. Accounting. *Organizations and Society*, 35(7), 659-675.

Aven, T. (2023). *Foundations of Risk Analysis*, 3rd ed. Wiley.

Bartkowiak, P., Koszel, M. (2013). *Zarządzanie ryzykiem gospodarczym*. Warszawa: Wydawnictwo Naukowe PWN.

Brock, J.K.-U., von Wangenheim, F. (2019). Demystifying AI in business: A critical review and agenda for future research. *Journal of Business Research*, 115, 202-213.

Buschgen, H.E. (1997). *Grundlagen der Finanzwirtschaft*. Wiesbaden: Gabler Verlag.

Campbell, J. (2005). *Risk and the legal process*. Oxford University Press.

Chapman, R.J. (2011). *Simple Tools and Techniques for Enterprise Risk Management*. Wiley.

COSO & Deloitte (2019). Enterprise Risk Management: Integrating with Strategy and Performance. Committee of Sponsoring Organizations of the Treadway Commission.

Davenport, T.H., Ronanki, R. (2018). Artificial Intelligence for the Real World. *Harvard Business Review*, 96(1), 108-116.

Dubisz, S. (ed.) (2008). *Uniwersalny słownik języka polskiego*. Warszawa: PWN.

Felch, V., Asdecker, B. (2022). Mapping the field of AI in enterprise risk management: A bibliometric review. *Journal of Risk Research*, 25(5), 621-639.

FERMA (2003). A Risk Management Standard. Federation of European Risk Management Associations.

Filipiak, B. (2010). *Ryzyko w zarządzaniu publicznym*. Difin.

Ghosh, R. (2023). Predictive Analytics in Financial Risk. *Harvard Business Review*, 101(4), 78-84.

Graham, J.D., Weiner, J.B. (1995). *Risk vs. Risk: Tradeoffs in Protecting Health and the Environment*. Harvard University Press.

IBM Security (2021). *AI for Cyber Defense*. IBM Research White Paper.

IIA (2020). The IIA's Three Lines Model: An update of the Three Lines of Defense.

International Federation of Accountants (IFAC) (2009). Evaluating and Improving Governance and Management Processes.

Jajuga, K. (2007). *Zarządzanie ryzykiem*. Warszawa: Wydawnictwo Naukowe PWN.

Kasiewicz, S. (2011). *Ryzyko jako czynnik strategii przedsiębiorstwa*. Wydawnictwo SGH.

Kasiewicz, S., Rogowski, W. (2006). *Ryzyko w działalności banków*. Oficyna Ekonomiczna.

Kasiewicz, S., Rogowski, W. (2009). *Zarządzanie ryzykiem w bankowości*. Oficyna Ekonomiczna.

Komitet Organizacji Sponsorujących Komisję Treadway (COSO) (2006). Zarządzanie ryzykiem – zintegrowana koncepcja.

Makarowski, R. (2008). *Zarządzanie ryzykiem w przedsiębiorstwie*. PWE.

Małkowska-Borowczyk, M. (2012). *Zarządzanie ryzykiem w jednostkach sektora publicznego*. Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu.

Marcinkowski, B. (2016). *System zarządzania ryzykiem*. Wolters Kluwer.

Merna, T., Al-Thani, F. (2011). *Corporate Risk Management*. Wiley.

Moeller, R.R. (2011). *COSO Enterprise Risk Management: Establishing Effective Governance, Risk, and Compliance Processes*. Wiley.

Nowak, M. (2014). *Modele zarządzania ryzykiem w organizacjach*. Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu.

Olson, D.L., Wu, D. (2010). *Enterprise Risk Management*. World Scientific.

O'Neil, C. (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Crown Publishing Group.

Peter-Bombik, K. (2023). *Koncepcje ryzyka w zarządzaniu strategicznym*. Wydawnictwo Uniwersytetu Warszawskiego.

Pleczeluk, M. (2011). *Zarządzanie ryzykiem operacyjnym*. CeDeWu.

Rudawska, A. (2013). *Ryzyko w usługach zdrowotnych*. Wydawnictwo Uniwersytetu Szczecińskiego.

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

Samborski, A. (2012). Rola systemu zarządzania ryzykiem w organizacjach. *Ekonomika i Organizacja Przedsiębiorstwa*, 1(744), 29-37.

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

Sobel, P.J. (2004). *Auditor's Risk Management Guide*. CCH Inc.

Sobolewski, H., Marcinkowski, B. (2017). *Zarządzanie ryzykiem korporacyjnym*. Warszawa: Wydawnictwo Naukowe PWN.

Tranfield, D., Denyer, D., Smart, P. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *British Journal of Management*, 14(3), 207-222.

Urbanowska-Sojkin, E. (2012). Strategiczne zarządzanie ryzykiem. Wydawnictwo Uniwersytetu Ekonomicznego w Poznaniu.

Willis, H.H. (2007). Guiding resource allocations based on terrorism risk. *Risk Analysis*, 27(3), 597-606.

Wojniłko, J., Sikorska-Michalak, B. (1996). *Zarządzanie przedsiębiorstwem*. PWE.

Woźniak, W., Szalbo, J. (2003). *Zarządzanie ryzykiem*. Wydawnictwo Akademickie.

Zasępa, E. (2013). *Ryzyko w działalności gospodarczej*. Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu.

ZARZĄDZANIE RYZYKIEM W ORGANIZACJI W DOBIE AI – PODEJŚCIE TEORETYCZNE

Streszczenie

W epoce charakteryzującej się złożonymi globalnymi współzależnościami zarządzanie ryzykiem organizacyjnym stało się kluczową funkcją strategiczną. Ryzyko nie ogranicza się już do strat finansowych lub zakłóceń operacyjnych, ale obejmuje też szerokie spektrum niepewności, które mają wpływ na długoterminową stabilność i konkurencyjność. Tradycyjne podejścia, w tym ISO 31000 i COSO ERM, kładą nacisk na identyfikację, ocenę i ograniczanie ryzyka w ramach ustrukturyzowanych ram zarządzania. Jednak niedawny postęp technologiczny, szczególnie w dziedzinie sztucznej inteligencji (AI), wprowadził nowe paradygmaty w sposobie postrzegania, przewidywania i zarządzania ryzykiem. Głównym celem artykułu było usystematyzowanie podstawowych definicji, wyjaśnienie kluczowych ram teoretycznych oraz wskazanie nierozstrzygniętych kwestii poprzez kompleksowy przegląd współczesnej literatury naukowej. Praca zawiera kompleksowy przegląd teoretyczny zarządzania ryzykiem organizacyjnym przy jednoczesnej integracji narzędzi i podejść opartych na sztucznej inteligencji. Główne wnioski płynące z artykułu wskazują, że zarządzanie ryzykiem przeszło transformację od podejścia reaktywnego do proaktywnego. Dzisiejsze organizacje nie tylko reagują na ryzyko, ale też uczą się je przewidywać i wykorzystywać. Ponadto stosowanie AI znacząco zwiększa możliwości organizacyjne w zakresie identyfikacji, analizy i kontroli ryzyka. Z drugiej strony integracja sztucznej inteligencji niesie ze sobą wyzwania etyczne i systemowe, a samo zarządzanie ryzykiem w przyszłości wymaga inteligencji hybrydowej. Wyciągnięte wnioski mają charakter teoretyczny – potrzebne są dalsze badania empiryczne.

Słowa kluczowe: zarządzanie ryzykiem korporacyjnym, sztuczna inteligencja w analizie ryzyka, analityka predykcyjna i ryzyko, uczenie maszynowe na rzecz zgodności, transformacja cyfrowa w zarządzaniu ryzykiem