UDC: 65.012.4

TRANSFORMATIONS IN THE GLOBAL RISK LANDSCAPE: CONSIDERATIONS FOR STRATEGIC RISK MANAGEMENT SYSTEM DEVELOPMENT

CHMUTOVA Iryna[1], HAINALII Anastasiia[2]
[1] Simon Kuznets Kharkiv National University of Economics
https://orcid.org/0000-0001-7932-7652
[2] Simon Kuznets Kharkiv National University of Economics

The dynamic evolution of the global risk landscape necessitates a re-evaluation of traditional risk management frameworks to address the growing complexity and interconnectedness of modern threats. This study examines the transformations in global risks over recent years, highlighting trends such as the convergence of environmental and technological risks and the increasing significance of health crises, economic instability, and misinformation. Utilizing insights from global risk reports (2018–2024), the study identifies short-term risks driven by immediate socio-economic impacts and long-term risks with broader strategic implications, such as climate change and biodiversity loss.

The research synthesizes key risk management frameworks, including COSO ERM, Balanced Scorecard (BSC), Prevent-Detect-Correct (PDC), Risk-Based Decision-Making (RBD), Risk Matrix, NIST, ISO 31000, and COBIT. Each framework's adaptability, scope, and applicability across diverse organizational needs are analyzed. While COSO ERM and BSC align risk management with strategic goals, PDC and RBD emphasize proactive and data-driven approaches. The Risk Matrix simplifies prioritization, whereas NIST and COBIT provide robust methodologies for IT and cybersecurity risks. ISO 31000 emerges as the most versatile, offering a flexible, principle-driven approach to managing risks across industries.

Special emphasis is placed on utilizing these systems for managing financial risks and safeguarding the financial security of enterprises.

Findings underscore the necessity of integrating risk management into strategic decision-making to enhance resilience and proactive preparedness. Organizations must select tailored frameworks that align with their unique risk profiles, regulatory environments, and strategic objectives. This study contributes to the discourse on strategic risk management, providing actionable insights for organizations navigating the complexities of a rapidly evolving risk environment.

Keywords: *risk, threats, strategic risk management, financial risk management, integration, digitalization, financial security of enterprise.*

https://doi.org/10.31891/mdes/2024-14-43

INTRODUCTION

In an era characterized by rapid and multifaceted global changes, understanding the transformations in the global risk landscape is of paramount importance for both academic research and practical implementation. The increasing complexity and interconnectedness of risks – spanning economic volatility, geopolitical tensions, climate change, pandemics, and technological disruptions – underscore the urgency of reevaluating and enhancing traditional risk management frameworks. These risks, which transcend national and sectoral boundaries, have profound implications for organizations, governments, and societies, making their assessment and mitigation a critical component of strategic planning and sustainability efforts.

This article highlights the necessity of integrating an in-depth understanding of global risk dynamics into the development of a strategic risk management system. Such systems must not only address existing challenges but also anticipate emerging threats, thereby enabling organizations to remain agile and resilient in an increasingly uncertain environment. By exploring how global risk transformations influence organizational decision-making processes, this study emphasizes the importance of a proactive and adaptive approach to risk identification, prioritization, and mitigation.

LITERATURE REVIEW

The dynamic nature of global risks has intensified scholarly attention to the development and adaptation of strategic risk management systems (SRMS). As global interconnectedness grows, risks such as geopolitical tensions, climate change, economic instability, and cyber threats have evolved, reshaping the priorities for risk management frameworks (Beck et al., 2022) [2]. Scholars emphasize the importance of understanding these transformations to design proactive and resilient SRMS tailored to contemporary challenges (Kaplan & Mikes, 2021) [9].

Global risks have undergone significant transformations over the past decade, with new risks emerging and existing ones escalating in complexity. Geopolitical uncertainties, characterized by trade disputes and political instability, have become pivotal considerations in enterprise risk assessments. Climate risks, particularly extreme weather events, have garnered heightened attention due to their profound economic and environmental impacts (IPCC, 2023) [7]. Furthermore, the COVID-19 pandemic underscored the vulnerability of systems to health crises, prompting enterprises to reassess their risk mitigation strategies.

The literature highlights the shift toward integrated SRMS that account for interdependencies among various risks. Emphasis is placed on the adoption of advanced analytical tools, including machine learning and big data analytics, to predict and mitigate risks effectively (Rostami et al., 2021) [11]. Cybersecurity has emerged as a critical focus, with researchers advocating for robust frameworks to counter the growing prevalence of cyber threats and data breaches (Cheng et al., 2020) [3].

Several studies propose frameworks that prioritize flexibility and resilience in SRMS. Wieland and Wallenburg (2013) [19] argue for a supply chain resilience framework that accommodates the unpredictable nature of global risks. Similarly, Aven (2022) [1] emphasizes the need for a holistic approach that integrates quantitative and qualitative methods for risk assessment. These frameworks stress the importance of dynamic risk registers and real-time monitoring to address evolving risks effectively.

Scholars have increasingly focused on prioritizing risks based on their probability and impact. Using tools such as risk heatmaps and Likert-scale assessments, enterprises can allocate resources effectively to address high-priority risks (Kaplan & Mikes, 2021) [9]. The literature suggests a growing trend toward sustainability-focused risk management, aligning organizational strategies with environmental, social, and governance goals to mitigate reputational and operational risks (Beck et al., 2022) [2].

International collaboration is identified as a cornerstone of effective risk management. Studies highlight the role of multilateral organizations, such as the United Nations and the World Economic Forum, in fostering cooperative efforts to address transnational risks (Global risk report, 2024) [18]. Policy recommendations include harmonizing regulatory frameworks to address risks uniformly across borders, particularly in the areas of cybersecurity and environmental protection (de Assis Santos et al., 2022) [11].

Despite advancements, gaps remain in the integration of different components and technologies into holistic SRMS.

The **aim** of this article is to examine the contemporary transformations of the global risk landscape, synthesize strategic risk management frameworks, and identify their areas of application within business entities.

RESULTS

The 2018 Global Risks Report [12] identified environmental and technological threats as key global challenges, with extreme weather events, natural disasters, cyberattacks, fraud, and data theft emerging as the most likely risks. This emphasis on environmental and technological issues coincided with a growing public awareness of climate change and an increasing dependence on digital technologies, which in turn raised concerns regarding cyber vulnerabilities. Extreme weather events were ranked as the most likely risk, underscoring the urgency associated with climate change and the frequent occurrence of natural disasters. Likewise, cyberattacks and fraud/data theft were highlighted as significant risks, reflecting rising concerns over information security in an increasingly interconnected society.

By the publication of the 2019 Global Risks Report [13], the failure to mitigate and adapt to climate change had become an even more pressing concern, occupying the top position in terms of both likelihood and impact. This shift marked a significant change in global awareness regarding the insufficient response to climate change. While extreme weather events and natural disasters remained significant risks, illustrating the ongoing challenge of addressing environmental issues, cyberattacks and fraud/data theft continued to be major concerns, signaling the persistence of technological vulnerabilities amidst growing digitalization.

The 2020 Global Risks Report [14] further intensified the focus on environmental risks, with the failure to address climate change emerging as the dominant concern, ranked highest for its potential impact. It was followed by threats such as weapons of mass destruction and biodiversity loss. This heightened emphasis on climate inaction reflected increasing alarm over the inability of world leaders to implement effective policies to mitigate climate change's negative effects. This shift signified not only heightened awareness but also a critical tipping point in global perception: a recognition that continued inaction or insufficient efforts could precipitate catastrophic global consequences. Extreme weather events, natural disasters, and human-induced environmental catastrophes continued to rank among the top risks, reinforcing the growing urgency of the environmental crisis.

So, in recent years, a key trend has been the convergence of environmental and technological risks. Both categories have consistently ranked among the top global risks, reflecting the increasing complexity and interdependence of contemporary threats. Environmental degradation, combined with rapid technological advancements, has given rise to multifaceted risks that jeopardize digital infrastructure, financial stability, and public well-being.

The inclusion of infectious diseases as a significant risk in the 2020 report further underscores the dynamic nature of global risk landscapes. Although not as prominent in prior years, its rise to the top of the risk rankings in 2020 was a direct response to the global pandemic. This shift brought health risks to the forefront, highlighting the unpredictability of emerging threats.

A comparative analysis of short-term and long-term risks, as presented in the Global Risks Reports from 2021 to 2024 [15-18], reveals important trends that reflect shifting global priorities and the interconnectedness of economic, environmental, and social challenges. The World Economic Forum employs a structured framework to distinguish between risks anticipated to manifest in the short term (within two years) and those projected over a longer horizon (ten years). This distinction is crucial for understanding the evolving nature of global threats, their underlying causes, and potential consequences. By analyzing this data, we gain valuable insights into how global priorities have evolved and how perceptions of risks have shifted over time.

Short-term risks, particularly from 2021 to 2024, frequently reflect the immediate consequences of recent events and their socio-economic impacts. For instance, the 2021 and 2022 Global Risks Reports identified "infectious diseases" as the primary short-term risk, driven by the severe repercussions of the COVID-19 pandemic. The pandemic's effects on health systems, global supply chains, and societal stability were seen as urgent and critical concerns. Concurrently, short-term economic risks, such as the cost of living crisis and economic recession, were closely linked to the consequences of government-imposed lockdowns and disruptions in global trade and services.

In contrast, long-term risks identified in the reports represent a broader strategic assessment of threats to the global community over the coming decade. The World Economic Forum consistently identifies climate change-related risks, such as failure of climate action, extreme weather events, and biodiversity loss, as the most pressing challenges for the 10-year horizon. Delayed implementation of mitigation strategies, inadequate policy coordination, and insufficient resources for adaptation are all factors that could exacerbate the climate crisis, potentially leading to a global temperature rise of 3°C by the 2024 report. A key distinction between short-term and long-term risks lies in their complexity and scale of impact. Short-term risks tend to be more immediate and specific. For example, the cost of living crisis, as noted in the 2023 and 2024 reports, is a result of rising inflation, energy price surges, and supply chain disruptions tied to geopolitical instability, such as the war in Ukraine. These risks have direct consequences for households, influence consumer spending, and generate social pressures that require prompt governmental intervention. In contrast, long-term risks, such as biodiversity loss, involve intricate interdependencies and gradual processes. The degradation of natural ecosystems and the erosion of biodiversity are not abrupt events, but cumulative processes that, over time, undermine foundational systems, ultimately threatening food security, public health, and economic stability.

Another significant distinction between short-term and long-term risks lies in their impact on resilience and preparedness. The reports indicate that while short-term risks necessitate rapid, adaptive responses to mitigate their immediate effects, long-term risks require a more proactive and systemic approach. The 2023 and 2024 Global Risks Reports [17, 18] particularly emphasize the importance of preparing for a polycrisis – a scenario in which multiple long-term risks, such as resource scarcity, climate inaction, and geopolitical fragmentation, converge to create an insurmountable challenge. The interconnectedness of these risks suggests that failing to address one, such as climate change, can trigger cascading disruptions across other areas, including economic stability and social security.

Notably, the shift in priorities from 2021 to 2024 reflects changes in both geopolitical and socio-economic contexts. In 2021 and 2022, the impact of the COVID-19 pandemic was a dominant factor in shaping short-term risk perceptions. However, the 2023 and 2024 reports pivot towards risks related to inflation, conflict, and societal polarization. The growing prominence of the misinformation and disinformation as a critical risk in 2024 highlights the increasing significance of digital and informational threats in a world marked by rising polarization. The rapid proliferation of artificial intelligence and social media tools is amplifying disinformation, influencing electoral outcomes, and exacerbating political divisions. This, in turn, undermines the collective capacity to manage other short-term crises effectively. The evolving global risk landscape is depicted in Figure 1.

Drawing conclusions from this analysis, it is evident that while short-term risks are primarily addressed through reactive measures, long-term risks necessitate a more proactive and strategic approach. Effective management of long-term risks requires the development of systemic resilience, enhanced international cooperation, and a strong commitment to sustainable practices. The reports highlight a growing disparity between the nature of these risks and global preparedness to address them. For instance, the insufficient progress in combating climate change is a challenge that spans both short-term and long-

term risk frameworks, underscoring a persistent lack of sustained focus and political will to prioritize environmental sustainability over immediate economic gains. The short-term emphasis on tackling the cost of living and economic instability further diverts critical resources and attention from long-term objectives, potentially exacerbating future crises related to climate change and resource scarcity.

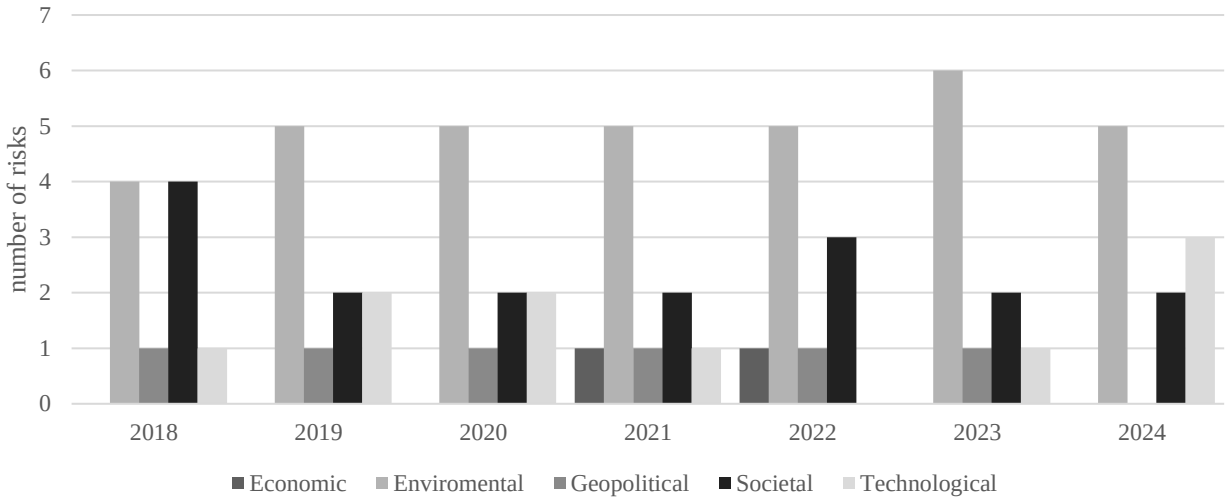

Fig. 1. Global Risks by Category, 2018–2024

Source: compiled based on [12 - 18]

The analysis also reveals that contemporary enterprise risk management recognizes the interconnectivity of risks across all business domains. Risks are no longer confined to isolated business areas but are embedded in every operational facet, thereby necessitating a holistic and integrated approach to risk management.

Modern approaches to risk management emphasize the integration of risk management processes into strategic decision-making at all organizational levels. This integration ensures that risks are not merely addressed reactively but are proactively identified, assessed, and mitigated as part of the enterprise's daily operations. Such an approach enhances organizational resilience and strategic alignment by embedding risk considerations into routine functions and decision-making frameworks.

Key concepts in contemporary risk management include the following:

1. COSO ERM Framework: Focuses on governance, strategy, and performance through comprehensive risk oversight.
2. Balanced Scorecard (BSC): Aligns risk management with strategic objectives by linking risks to performance metrics.
3. Prevent-Detect-Correct (PDC) Model: Emphasizes proactive prevention, timely detection, and effective correction of risks.
4. Risk-Based Decision-Making (RBD) Model: Guides decision-making by prioritizing risks based on their impact and likelihood.
5. Risk Matrix Model: Provides a visual tool for assessing and categorizing risks according to severity and probability.
6. NIST Risk Management Framework (RMF): A structured approach for integrating cybersecurity risk management into system development.
7. ISO 31000: Offers principles and guidelines for managing risks across all types of organizations.
8. COBIT: Focuses on governance and management of enterprise IT, integrating risk management into IT frameworks.

Table 1 provides a detailed summary of these risk management systems, highlighting their core features and applications.

Table 1

Characteristics and Applications of Risk Management Systems

Risk management system	Organizations Suitable for Implementing the System	Typical Situations and Applications
COSO ERM Framework	Large Enterprises, Multinational Corporations, and Firms	Situations Requiring Integration of Risk Management with Enterprise Objectives. These scenarios arise when aligning risk management with organizational objectives is critical to ensure coherence between risk considerations and overall strategic goals. This approach is particularly valuable in contexts where maximizing enterprise value involves balancing growth, profitability, and risk exposure.
Balanced Scorecard (BSC)	Organizations seeking strategic alignment (e.g., medium and large enterprises, government agencies)	Organizations Prioritizing Strategic Alignment. This category includes medium and large enterprises, as well as government agencies, that aim to align their risk management processes with strategic objectives to enhance decision-making, operational efficiency, and long-term resilience.
Prevent-Detect-Correct (PDC) model	Organizations operating in highly regulated industries, such as finance and healthcare	Especially well-suited for organizations that require a proactive approach to risk management, encompassing risk prevention, early issue detection, and the implementation of corrective actions to ensure compliance and mitigate regulatory risks.
Risk-Based Decision Making (RBD) model	Design organizations, as well as engineering and construction companies	Used in environments where decision-making is impacted by significant risks, such as projects with high uncertainty, complex stakeholder dynamics, or critical safety implications.
Risk Matrix	Organizations of all sizes, particularly small and medium-sized enterprises, and industries with diverse risk profiles	Useful for prioritizing risks by classifying them as low, medium, or high priority, allowing organizations to focus efforts on high-impact risks. Commonly used in environments with clearly defined and quantifiable risks.
NIST RMF	Federal agencies, IT-dependent organizations, and sectors specializing in cybersecurity, such as finance and healthcare	Primarily suited for managing information security risks in federal or critical information systems, particularly when adherence to structured security standards is a priority. It is widely adopted for its emphasis on categorization, control selection, and continuous monitoring.
ISO 31.000	Organizations of all sizes, in both the public and private sectors	Suitable for scenarios that require a flexible, comprehensive, and proactive approach to risk management. It is applicable across various industries, making it particularly relevant for integrating risk management into decision-making processes at all organizational levels.
COBIT	IT-oriented organizations and companies with substantial IT infrastructure	Useful for managing IT-related risks, particularly in organizations that focus on aligning IT initiatives with business goals and require a robust IT governance structure. Typically employed when the effective management of IT systems is critical to achieving the organization's overall objectives.

The COSO Enterprise Risk Management (ERM) framework, developed in collaboration with PricewaterhouseCoopers, is one of the most widely adopted models for integrating risk management directly with business objectives. By embedding risk management into an organization's overarching management system, COSO ERM fosters alignment between risk considerations and organizational strategy. This structured approach enables organizations to identify and address risk issues that may hinder the achievement of business objectives, with the ultimate goal of maximizing value through a balance of growth, profitability, and risk.

The COSO ERM framework comprises five interrelated components, each supported by core principles. These components collectively enable organizations to effectively identify, assess, manage, and monitor risks (Moeller, 2011) [10]:

1. Governance and Culture. The first component emphasizes the establishment of a robust governance structure that supports a culture of risk awareness. The board of directors and senior management are central to this process, with clearly defined responsibilities for overseeing risk management. This component fosters an organizational culture grounded in ethical behavior, transparency, and accountability, creating a solid foundation for managing risks effectively.
2. Strategy and Objective Setting. This component focuses on integrating risk management into the organization's strategic planning processes. It encourages the assessment of risks at a strategic level, ensuring that potential challenges and uncertainties are accounted for in decision-making. This alignment allows organizations to proactively address risks that could impact their strategic objectives.
3. Performance. The performance component centers on identifying, assessing, and responding to risks that may affect the achievement of organizational goals. This involves key risk

management activities, such as risk identification, analysis, and prioritization. COSO ERM advocates for the use of both qualitative and quantitative methods to better understand the likelihood and potential impact of various risk scenarios.

4. Review and Revision. This component ensures that the risk management process remains dynamic and adaptable. By analyzing past experiences and incorporating lessons learned, organizations can refine their risk management practices, enhancing resilience and flexibility in the face of emerging threats.

5. Information, Communication, and Reporting. Effective communication is integral to the success of risk management. This component emphasizes the timely dissemination of accurate risk-related information across all levels of the organization, from the board of directors to operational teams. Leveraging technology for real-time monitoring and reporting of risks is a key aspect, enabling organizations to proactively address risks as they arise.

Through these interrelated components, the COSO ERM framework provides a comprehensive and adaptable model for embedding risk management into organizational processes, ensuring that risks are managed in a way that supports strategic objectives and enhances overall resilience.

The Balanced Scorecard (BSC) approach integrates risk management into the broader framework of strategic management by aligning risk management activities with the organization's key performance indicators (KPIs). It emphasizes identifying the interrelationships among various business risks and their impact on achieving long-term objectives.

The core of the BSC approach lies in its ability to balance four key perspectives, each representing a distinct dimension of organizational success: financial perspective, customer focus, internal processes, and learning and growth.

Financial perspective focuses on how the organization creates value for shareholders and other stakeholders from a financial standpoint. Traditional metrics such as profitability, revenue growth, and cost management are evaluated here. In the context of risk management, BSC allows organizations to incorporate risk-adjusted financial metrics, such as Risk-Adjusted Return on Capital (RAROC) or Economic Value Added (EVA), to reflect the financial implications of risks.

Customer perspective measures the organization’s success in delivering value to its customers. Metrics include customer satisfaction, retention, and market share. From a risk management perspective, BSC can track customer-related risks, such as reputational damage, service disruptions, or regulatory compliance breaches, which may affect customer relationships and perceptions.

Internal process perspective evaluates operational efficiency, quality control, and innovation. By integrating risk management into this dimension, organizations can identify and mitigate operational risks, such as process failures, supply chain disruptions, or cybersecurity threats, that could hinder the achievement of business objectives.

Learning and Growth perspective assesses the organization’s ability to innovate, improve, and develop its workforce and systems. It encompasses metrics related to employee training, organizational culture, and technology adoption. Through a risk management lens, this perspective ensures that organizations address risks associated with skills gaps, cultural resistance to change, and technological vulnerabilities.

The BSC approach provides a structured framework for organizations to align risk management with strategic objectives across these four dimensions, ensuring that risks are managed comprehensively and proactively in support of long-term organizational success.

The Prevent-Detect-Correct (PDC) model emphasizes a proactive and structured approach to risk management, focusing on preventing risks from materializing, detecting problems at an early stage, and swiftly addressing them (Grynko et al, 2024) [6]. The model is divided into three main phases:

1. Prevent Phase. This phase aims to identify potential risks and implement measures to avoid them. Preventive actions include developing robust policies, establishing standards, and providing comprehensive staff training. The primary objective is to reduce the likelihood of risks occurring by addressing vulnerabilities before they manifest.

2. Detect Phase. The detection phase is centered on continuous monitoring and auditing to identify emerging risks promptly. This phase employs tools such as data analysis, automated reporting systems, and regular assessments to facilitate early detection of risks. Proactive identification enables organizations to respond more effectively and mitigate potential damage.

3. Correct Phase. In the corrective phase, actions are taken to manage and eliminate risks once they have been identified. This includes revising procedures, rectifying errors, and updating strategies to

prevent recurrence. The focus is on resolving issues swiftly while incorporating lessons learned to improve resilience and preparedness for future risks.

The Risk-Based Decision Making (RBD) model integrates comprehensive risk analysis into the decision-making process. This model is particularly advantageous in scenarios where risks have a significant potential to influence project outcomes or organizational objectives.

The RBD process begins with the identification of risks that could impact decisions. This is followed by assessing the likelihood and severity of these risks, utilizing methods such as statistical modeling, scenario analysis, or expert judgment. Once risks are quantified, management strategies are developed to mitigate their impact, ensuring more informed and balanced decision-making.

The RBD approach enhances organizational control over uncertainties, enabling decision-makers to better anticipate challenges and allocate resources effectively. However, it introduces complexities to the decision-making process, as thorough risk analysis can require significant time and resources. Despite these challenges, the RBD model remains a critical tool for achieving strategic alignment between risk management and organizational objectives.

The risk matrix model is a widely adopted tool for categorizing risks based on two dimensions: the likelihood of occurrence and the potential impact. This approach enables organizations to systematically prioritize risks, directing attention and resources to those that pose the greatest threat. Risks are typically classified into priority levels – low, medium, or high – using a grid format where likelihood and impact intersect. High-priority risks, which are both highly probable and potentially severe, are addressed with the greatest urgency, ensuring a structured and efficient risk management process (Grynko et al, 2024) [6].

The NIST Risk Management Framework is a structured methodology primarily focused on information security risk management, particularly for federal information systems . However, its comprehensive and adaptable approach has made it widely applicable across various sectors. This framework consists of six iterative steps that collectively provide a robust framework for managing risks.

In the initial step, the information system is categorized based on its criticality and alignment with the organization's mission and objectives. This step ensures that security controls are appropriately tailored to the system's importance and sensitivity. Following categorization, a tailored set of security controls is selected. The controls are drawn from the extensive catalog provided in NIST Special Publication 800-53, which addresses a wide range of risk scenarios. This ensures a customized approach that aligns with the organization's specific risk profile. During implementation of security controls phase, the selected controls are implemented within the system infrastructure. Activities include configuring, deploying, and integrating these controls to effectively mitigate identified risks and protect the system. After implementation, the effectiveness of the controls is rigorously evaluated. This process identifies vulnerabilities, deficiencies, or areas for improvement, ensuring that the controls function as intended. Based on the assessment, senior management determines whether the system is secure enough for operational use. This decision is formally documented, and if the system does not meet security requirements, further remediation actions are recommended. A defining feature of this framework is its emphasis on continuous monitoring and improvement. This step involves ongoing evaluation of security controls to adapt to evolving threats and system changes, ensuring dynamic and effective risk management throughout the system lifecycle.

While the NIST was originally designed for U.S. federal agencies, its structured and standardized approach has been widely adopted by non-governmental organizations due to its effectiveness in addressing cybersecurity challenges. The framework provides a clear and actionable methodology for aligning information security practices with organizational goals, fostering resilience and compliance in the face of ever-evolving risks (Efe, 2023) [5].

ISO 31000 offers a principles-based and flexible framework for managing risks, applicable across industries and not limited to specific domains such as information security. This comprehensive approach encourages organizations to embed risk management into all aspects of their operations and decision-making processes, ensuring a holistic view of risk across the enterprise.

At its core, the ISO 31000 framework emphasizes three interconnected components: risk assessment, risk management, and ongoing risk monitoring. A notable strength of ISO 31000 lies in its adaptability, enabling organizations to tailor the framework to their unique contexts and operational needs (ISO 31000:2018) [8].

The risk management process begins with establishing the context, where the organization identifies both external and internal factors that could influence its objectives and risk profile. By thoroughly understanding these factors, the organization gains insights into the broader environment in which it operates, laying the foundation for targeted risk identification. The subsequent risk assessment

phase is a systematic process comprising three steps: risk identification, risk analysis, risk evaluation. This structured analysis aids in the efficient allocation of resources to address the most critical risks effectively. Following the assessment, the organization advances to the risk management phase, where it decides on appropriate responses to mitigate or address risks. These responses may include: avoiding the risk entirely; reducing the risk's likelihood or potential impact; transferring the risk to a third party, such as through insurance; accepting the risk if it aligns with the organization's risk appetite.

The iterative and proactive nature of ISO 31000 fosters a dynamic approach to risk management, enabling organizations not only to address existing risks but also to anticipate and prepare for emerging uncertainties. This adaptability makes ISO 31000 a versatile framework, suitable for organizations of varying sizes, sectors, and complexities.

Ultimately, ISO 31000 serves as a universal guide for developing, implementing, and refining risk management systems. By embedding risk considerations into strategic and operational processes, it empowers organizations to achieve their objectives while navigating an increasingly complex risk landscape (Efe, 2023) [8].

COBIT, developed by ISACA, is a specialized framework designed to manage IT-related risks by embedding risk management into IT governance. It emphasizes the alignment of IT systems and processes with an organization's overarching business objectives, ensuring that technology supports and enhances strategic goals (COBIT, 2019) [4].

The COBIT framework incorporates several key components, including risk management, risk assessment, and risk response. By providing a comprehensive list of IT processes and control objectives, COBIT enables organizations to identify, evaluate, and mitigate risks associated with their IT infrastructure. This structured approach is particularly valuable for organizations heavily reliant on IT systems, as it facilitates effective management of risks such as cybersecurity threats, system failures, and data breaches. Its robust methodology makes it an essential tool for organizations where IT plays a critical role in operational and strategic success (Efe, 2023) [5].

Effective financial risk management is crucial for maintaining financial security and stability in organizations. SRMS play a pivotal role in identifying, assessing, and mitigating financial risks while aligning risk management efforts with organizational objectives.

Table 3 shows the suitability of different SRMS for managing financial risks and ensuring financial security.

Table 3

Applications of Strategic Risk Management Systems in Financial Risk Management

SRMS	Applications in Financial Risk Management
COSO ERM	Integrates financial risk with strategy; ideal for complex financial risk scenarios.
Balanced Scorecard	Links financial risks to performance indicators; suitable for performance-driven organizations.
Risk Matrix	Prioritizes financial risks; effective for resource allocation in SMEs.
ISO 31000	Proactive monitoring and management; adaptable for dynamic financial risk environments.

The COSO Enterprise Risk Management (ERM) Framework is highly effective for financial risk management due to its comprehensive approach to integrating risk considerations into strategic planning. COSO ERM enables organizations to evaluate financial risks, such as credit, market, and liquidity risks, within the context of overall business strategy, providing a balanced approach to risk and performance optimization. Its emphasis on risk-adjusted metrics, such as Risk-Adjusted Return on Capital (RAROC), makes it particularly relevant for financial institutions.

The Balanced Scorecard (BSC) supports financial risk management by linking financial security objectives to key performance indicators. Through its financial perspective, BSC monitors metrics like profitability, cost management, and revenue growth while incorporating risk-adjusted financial measures. This alignment ensures financial risks are integrated into performance management and decision-making processes.

The Risk Matrix Model is widely used for prioritizing financial risks based on their likelihood and potential impact. Its simplicity and adaptability make it suitable for small to medium-sized enterprises that require a straightforward tool for resource allocation to high-priority risks.

The ISO 31000 Framework is versatile and applies to various industries, including finance. Its emphasis on continuous monitoring and adaptability supports the proactive identification and

management of financial risks, making it suitable for dynamic environments where risk profiles frequently change.

Selecting the appropriate SRMS depends on organizational needs and the complexity of financial risks. COSO ERM and BSC are ideal for aligning financial risk management with strategic objectives, while the Risk Matrix and ISO 31000 offer flexibility and practicality for diverse financial risk scenarios.

CONCLUSION

The transformative landscape of global risks necessitates continuous evolution in SRMS. By leveraging strategic approaches, organizations can build resilience against diverse and interconnected threats.

The choice of a SRMS should align with an organization's unique needs, industry requirements, and strategic objectives. Different frameworks offer distinct advantages depending on the organization's priorities and risk environment. COSO ERM and the Balanced Scorecard (BSC) are particularly effective for organizations aiming to integrate risk management into their overall strategy and performance measurement. These systems provide a comprehensive approach, aligning risk management with business objectives and key performance indicators to ensure strategic cohesion.

In contrast, the Prevent-Detect-Correct (PDC) model and Risk-Based Decision-Making (RBD) framework focus on proactive risk management and informed decision-making under uncertainty. These approaches are well-suited for highly regulated industries and project-oriented organizations where anticipating and mitigating risks are critical to operational success. Similarly, the risk matrix offers a straightforward and adaptable tool for organizations needing to prioritize risks and allocate resources effectively. By categorizing risks based on their likelihood and potential impact, it helps organizations address high-priority threats efficiently.

For IT-focused environments, the NIST Risk Management Framework (RMF) and COBIT provide robust methodologies for managing IT-related risks and ensuring information security. These frameworks are particularly valuable for organizations that prioritize data protection and require structured approaches to address cybersecurity threats and compliance requirements.

ISO 31000, with its adaptability and focus on continuous risk monitoring and improvement, is the most versatile framework, applicable across a wide range of industries. Its principles-based design allows organizations to embed risk management into their processes, enhancing resilience and preparedness in dynamic environments.

Ultimately, selecting the right risk management system requires a tailored approach that considers an organization's specific risk profile, regulatory obligations, and strategic goals. Integrating risk management into strategic planning and decision-making not only ensures effective risk mitigation but also enhances an organization's resilience and capacity to adapt to emerging challenges.

Future research should focus on bridging existing gaps and developing adaptive frameworks that align with the dynamic nature of global risks.

REFERENCES:

1. Aven T. Foundations of risk management: Current challenges and future perspectives. *Risk Analysis*. 2022. No 42(1). P.24-35. https://doi.org/10.1111/risa.12132.
2. Beck U., Giddens A., Lash S. *Risk Society: Towards a New Modernity*. 2nd ed. SAGE Publications, 2022. 260 p.
3. Goel R., Haddow J., Kumar A. Managing Cybersecurity Risk in Government: An Implementation Model. IBM Center for The Business of Government. 2018. 53 p.
4. COBIT 2019 Framework: Introduction & Methodology. ISACA. 2018. 64 p.
5. Efe A. A comparison of key risk management frameworks: COSO-ERM, NIST RMF, ISO 31.000, COBIT. *Journal of Auditing and Assurance Services*. 2023. No. 3 (2). P. 185-205.
6. Grynko T., Gviniashvili T., Yuldashev R. Analysis of risk management systems in enterprises. *Economic Analysis*. 2024. No 34(2). P. 223–236. URL: https://www.econa.org.ua/index.php/econa/article/view/5966 (Last accessed on 17.10.2024)
7. IPCC, 2023: Climate Change 2023: Synthesis Report. Contribution of Working Groups I, II and III to the Sixth Assessment Report of the Intergovernmental Panel on Climate Change [Core Writing Team, H. Lee and J. Romero (eds.)]. IPCC, Geneva, Switzerland, 184 p. doi: 10.59327/IPCC/AR6-9789291691647.
8. ISO 31000:2018 - Risk management. A practical guide. Vienna : United Nations Industrial Development Organization, 2021. 305 p.
9. Kaplan R.S., Mikes A. Managing risks: A new framework. *Harvard Business Review*. URL: https://www.hbs.edu/faculty/Pages/item.aspx?num=42549 (Last accessed on 17.10.2024)
10. Moeller R. COSO Enterprise Risk Management (2nd ed.). Wiley. 2011. URL: https://www.perlego.com/book/1011126/coso-enterprise-risk-management-establishing-effective-governance-risk-and-compliance-processes-pdf (Last accessed on 17.10.2024)

11. de Assis Santos L., Marques L. Big data analytics for supply chain risk management: research opportunities at process crossroads. Business Process Management Journal. 2022. Vol. 28 No. 4. pp. 1117-1145. https://doi.org/10.1108/BPMJ-01-2022-0012
12. The global risks report 2018. Geneva : World Economic Forum, 2018. 80 p. https://www.weforum.org/publications/the-global-risks-report-2018/
13. The global risks report 2019. Geneva : World Economic Forum, 2019. 114 p. https://www.weforum.org/publications/the-global-risks-report-2019/
14. The global risks report 2020. Geneva : World Economic Forum, 2020. 102 p.
15. The global risks report 2021. Geneva : World Economic Forum, 2021. 97 p. https://www.weforum.org/publications/the-global-risks-report-2020/
16. The global risks report 2022. Geneva : World Economic Forum, 2022. 107 p. https://www.weforum.org/publications/global-risks-report-2022/
17. The global risks report 2023. Geneva : World Economic Forum, 2023. 98 p. https://www.weforum.org/publications/global-risks-report-2023/
18. The global risks report 2024. Geneva : World Economic Forum, 2024. 124 p. https://www.weforum.org/publications/global-risks-report-2024/
19. Wieland A., Wallenburg C.M. The influence of relational competencies on supply chain resilience: a relational view. *International Journal of Physical Distribution & Logistics Management*. 2013. Vol. 43 No. 4, pp. 300-320. https://doi.org/10.1108/IJPDLM-08-2012-0243

ТРАНСФОРМАЦІЇ ГЛОБАЛЬНОГО РИЗИКОВОГО ЛАНДШАФТУ ТА ЇХ ВРАХУВАННЯ ПРИ ФОРМУВАННІ СИСТЕМИ СТРАТЕГІЧНОГО УПРАВЛІННЯ РИЗИКАМИ

ЧМУТОВА Ірина, ГАЙНАЛІЙ Анастасія
Харківський національний економічний університет імені Семена Кузнеця

Динамічна еволюція глобального ландшафту ризиків вимагає переосмислення традиційних підходів до управління ризиками для вирішення проблем зростаючої складності та взаємозв'язку сучасних загроз. У статті досліджено трансформації глобальних ризиків за останні роки, зокрема такі тенденції, як конвергенція екологічних і технологічних ризиків, а також зростання значення криз у сфері охорони здоров'я, економічної нестабільності та дезінформації. Спираючись на дані звітів про глобальні ризики (2018–2024), визначено короткострокові ризики, пов'язані з безпосередніми соціально-економічними наслідками, та довгострокові ризики, які мають ширші стратегічні наслідки, такі як зміна клімату та втрата біорізноманіття.

Дослідження охоплює аналіз ключових систем управління ризиками, зокрема COSO ERM, Balanced Scorecard (BSC), Prevent-Detect-Correct (PDC), Risk-Based Decision Making (RBD), Risk Matrix, NIST, ISO 31000 і COBIT. Проаналізовано адаптивність, сферу застосування та релевантність кожної системи до різних організаційних потреб. COSO ERM і BSC забезпечують інтеграцію управління ризиками зі стратегічними цілями організації, тоді як PDC і RBD підкреслюють значення проактивних підходів, орієнтованих на прогнозні дані. Матриця ризиків спрощує процес визначення пріоритетів, а NIST і COBIT пропонують ефективні методології для управління IT-ризиками та ризиками кібербезпеки. ISO 31000 демонструє найбільшу універсальність, пропонуючи гнучкий, заснований на принципах підхід, що застосовується в різних галузях.

Особливу увагу приділено застосуванню зазначених систем для управління фінансовими ризиками і забезпечення фінансової безпеки підприємств.

Результати дослідження підкреслюють важливість інтеграції управління ризиками в стратегічне планування для підвищення стійкості організацій та їхньої проактивної готовності до викликів. Запропоновані рекомендації сприяють поглибленню дискурсу з питань стратегічного управління ризиками та забезпечують цінні інструменти для організацій, що діють у швидкозмінному ризиковому середовищі.

Ключові слова: *ризик, загрози, стратегічне управління ризиками, управління фінансовими ризиками, інтеграція, цифровізація, фінансова безпека підприємства.*