INNOVATION AND SUSTAINABILITY
Volume 5, No. 3. 2025
Journal homepage: https://inns.com.ua/en
Received: 17.04.2025; Revised: 04.08.2025; Accepted: 30.09.2025
DOI: 10.31649/vis/3.2025.42

UDC 330.34:005.334 [52, 96]

Analysis of the COSO risk management model: Main aspects

Inna Vishtak*
PhD in Technical Sciences, Associate Professor
Vinnytsia National Technical University
21021, 95 Khmelnytske Shose Str., Vinnytsia, Ukraine
https://orcid.org/0000-0001-5646-4996

Alina Podorozhnyuk
Student
Vinnytsia National Technical University
21021, 95 Khmelnytske Shose Str., Vinnytsia, Ukraine
https://orcid.org/0009-0007-5526-9049

Eliza Voitko
Student
Vinnytsia National Technical University
21021, 95 Khmelnytske Shose Str., Vinnytsia, Ukraine
https://orcid.org/0009-0005-4381-2142

Abstract. The relevance of the study was determined by the growing uncertainty in the external environment, which requires the implementation of effective risk management systems. The aim of the study was to analyse the key aspects of the Committee of Sponsoring Organisations of the Treadway Commission Enterprise Risk Management (COSO ERM) model and to justify its application for integrated risk management in enterprises. The study uses methods of analysis of scientific sources, structural and logical generalisation, and a systematic approach. The theoretical and practical aspects of risk management in an enterprise are considered, taking into account the challenges and trends of the global market. A systematic approach to risk management is analysed, which provides comprehensive coverage of all business processes related to the identification, assessment and response to risks. The key components of the COSO ERM methodology, which is one of the most recognised in global practice, are identified. The COSO ERM model is based on the principles of integrated management, where risks are viewed not as isolated threats, but as part of strategic planning and management processes. The application of the three-component COSO structure, which included enterprise objectives, internal environment and organisational levels of influence, was considered. This approach made it possible to harmonise strategic, operational and reporting processes within a single control system. The essence of the relationship between the main elements of risk management was revealed, which made it possible to adapt the model to the specifics of the functioning of enterprises in various industries. The feasibility of implementing the COSO model as a tool for increasing business resilience to external uncertainty is argued. Methodological approaches to improving risk management in accordance with the requirements of economic security and strategic development are proposed. The practical value of the study lies in the possibility of using the results by specialists in the field of risk management, internal audit and strategic management

Keywords: internal control; strategic planning; risk assessment; corporate governance; model adaptation; risk integration; business resilience

Suggested Citation:
Vishtak, I., Podorozhnyuk, A., & Voitko, E. (2025). Analysis of the COSO risk management model: Main aspects. *Innovation and Sustainability*, 5(3), 42-52. doi: 10.31649/vis/3.2025.42.

*Corresponding author

Introduction

Organisations face numerous risks that can affect their stability and effectiveness. An underdeveloped risk management system can lead to financial losses, legal sanctions and reduced competitiveness. The implementation of an integrated approach to risk management, in particular the Committee of Sponsoring Organisations of the Treadway Commission (COSO) model, has helped to reduce negative consequences and improve the effectiveness of corporate governance. This article examined how the COSO model has contributed to improving risk management processes in organisations. A significant number of scientific works have been devoted to risk management issues in the context of corporate governance and strategic planning. After the COSO model was updated in 2017, scientists actively analysed its new components, which covered aspects such as organisational culture, information flows, and the integration of risks into strategic processes.

In scientific literature, the COSO Enterprise Risk Management (ERM) model is considered the leading conceptual framework for integrating risk management into strategic enterprise management. According to J. Fraser *et al.* (2021), COSO not only identifies risks but also fosters a sustainable culture of management decision-making that takes into account both strategic and operational risks. The authors emphasised that the modernised version of COSO 2017 allows organisations to better adapt to changes in the environment, increasing their flexibility and ability to respond quickly to challenges. I. Benekos *et al.* (2020) analysed COSO ERM as a dynamic solution, pointing out that the components of the model – strategic, operational, reporting and regulatory environments – provide an adaptive framework that helps organisations respond quickly to emergencies. An ERM index is emerging that allows the effectiveness of the model's implementation to be measured in order to improve goal setting and management methods. P. Dahmen (2023) noted that COSO ERM forms the basis of organisational resilience in crisis situations. During the COVID-19 pandemic, organisations that implemented ERM effectively reduced revenue volatility and increased their ability to adapt – "flexibility like a rubber ball" – confirming the link between ERM and resilience. The article by W. Gleißner & T. Berger (2023) describes the "robust enterprise" platform, where ERM, combined with a sustainable strategy and financial security, forms, according to the authors' approach, the basis for enterprise sustainability. The main emphasis is on a portfolio approach, early risk warning and a culture of risk awareness. An analysis of sources indicates the effectiveness of the COSO model as a tool for increasing the flexibility and sustainability of organisations, while emphasising the difficulties of its application. Despite numerous studies in the field of risk management, many aspects remain insufficiently developed in the context of modern transformational changes, digitalisation and the growing uncertainty of the external environment. The methodology for adapting the universal COSO ERM model to the specific conditions of enterprises in countries with transitional economies, including Ukraine, needs to be refined. The existing literature focuses mainly on general approaches, without taking into account industry specifics, the organisational structure of enterprises and the practical difficulties of implementing integrated risk management systems. Issues related to the effective integration of internal control systems with strategic planning processes and key risk assessment remain under-researched.

The relationship between the maturity of an enterprise's organisational culture and the effectiveness of COSO ERM implementation requires separate attention. The aim of this article was to analyse the features of COSO Enterprise Risk Management (ERM) model implementation, evaluate its effectiveness, and formulate recommendations for its adaptation to achieve the strategic goals of the enterprise. The objectives were: to address gaps related to the practical application of the three-component COSO model in risk management in a transformational business environment, particularly for enterprises in countries with transitional economies, such as Ukraine; to identify barriers and problems in the practical implementation of this model in the context of digitalisation, growing external uncertainty and organisational inertia; and to develop recommendations for its adaptation to current challenges, taking into account industry specifics, the level of maturity of organisational culture and the need for integration with strategic planning and control systems.

Materials and Methods

This study was based on analytical reports of international organisations (COSO, 2017; SCCE & HCCA, 2020; Walker, 2022; Reuters, 2025), data from statistical databases on risk management (Cybersecurity and ERM…, 2024; How power and…, 2025), national legal and regulatory acts of Ukraine, such as the Law of Ukraine No. 996-XIV (1999) and the Law of Ukraine No. 2258-VIII (2017), as well as international risk management standards ISO 31000:2018 (2018) and ISO 22301:2019 (2019).

The research employed a combination of economic-analytical, comparative, and systemic methods, which allowed for a comprehensive assessment of the effectiveness of the COSO risk management model under modern challenges. The economic-statistical method served as the main tool for analysing the dynamics of change in internal control and risk management systems in organisations of various scales, particularly in enterprises of the industrial and financial sectors. The comparative method was used to identify key differences in the implementation of COSO ERM components. This approach made it possible to determine the effectiveness of the model's application depending on the field of activity, organisational structure, and external environment. The systemic approach enabled the integration of information on COSO ERM components – namely the control environment, risk assessment, control activities, information and communication, and monitoring – into a holistic analytical framework, which helped to reveal interconnections between the level of risk management and

the strategic resilience of organisations. The analysis also included an examination of the interdependence between COSO ERM implementation and indicators of operational efficiency, institutional accountability, and adaptability to crisis situations.

The content analysis method was used to systematise scientific sources and practical case studies regarding the application of COSO in companies. The main information sources included scientific publications, analytical reports, and regulatory-methodological documents on risk management (Makarchuk, 2020; Nazarova *et al*., 2021; Dvorski Lacković *et al*., 2022). To assess the institutional context and global trends, data from the IMD World Competitiveness Ranking (National Competitiveness and Productivity Council, 2024) were utilised, allowing the impact of the external environment on the effectiveness of risk management systems to be examined. The analysis of academic publications, conducted to form the theoretical and methodological basis of the study, encompassed works dedicated to the implementation of the COSO model in the areas of risk management, internal control, and strategic planning. To address the identified shortcomings, a comprehensive methodological approach was applied, which included economic-statistical, comparative, and systemic analysis. This was necessary not only to identify differences in the implementation of the COSO model across enterprises of different types but also to assess its impact on strategic resilience and the capacity for crisis adaptation. The application of the systemic approach facilitated a deeper understanding of the interconnections between individual elements of the risk management system and their influence on the overall level of organisational effectiveness.

Results and Discussion

In the business environment, risk management is a key element of effective corporate governance. A systematic approach to risk management has enabled companies not only to respond to potential threats, but also to strategically plan their activities, taking into account potential risks at various levels. One of the most effective methodologies in this area was the COSO ERM model, which provided a comprehensive approach to identifying, assessing and responding to risks. Before examining the COSO model in detail, it is important to first understand the basic concepts of risk (Table 1) and risk management (Table 2). Without a clear understanding of these concepts, it was impossible to fully appreciate the value of structured risk management methodologies such as COSO. Standards and authors' works were analysed and used to define the concepts of "risk" and "risk management". Risk is considered an integral part of any business activity, and the ability to effectively identify, assess and respond to risks has been key to ensuring the sustainability and development of an organisation. Risk management encompasses the strategies and processes that organisations have used to minimise the potential negative impact of risks on their objectives.

Table 1. Definition of the concept of "risk"

Source	Definition
ISO 31000:2018	Risk – the effect of uncertainty on objectives. This effect can be positive or negative and is associated with the possibility of deviation from expectations.
D. Hillson	Risk – an event or condition that, if it occurs, will affect project objectives. The definition focuses on the uncertainty of the future.
P. Hopkin	Risk – a combination of the probability of an event occurring and its consequences. The definition focuses on risk assessment as a quantitative approach.

Source: summarised by the authors based on P. Hopkin (2017), ISO 31000:2018 (2018), D. Hillson (2020)

Table 2. Definition of the concept of "risk management"

Source	Definition
ISO 31000:2018	Risk management – the coordinated actions of an organisation to manage and control risks that may affect the achievement of its objectives.
COSO	Risk management – a process carried out by the board of directors, management and other employees to identify potential events that may affect the organisation and manage risk within acceptable levels.
J .Fraser *et al.*	Risk management – a continuous process integrated into organisational structures that aims to identify, analyse and respond to risks.

Source: summarised by the authors based on COSO (2017), ISO 31000:2018 (2018), J. Fraser *et al.* (2021)

The COSO internal control system was established in 1992 in the United States against the backdrop of numerous cases of fraud in business practices affecting the US, the UK, Canada and Luxembourg. These events highlighted the need to improve internal control mechanisms and develop unified recommendations for the organisation of control procedures. COSO has developed a basic set of principles and guidelines that form the basis for building a reliable internal control system. These principles outline good professional practice for creating business processes that ensure the effective functioning of organisations and the achievement of their strategic objectives (Moeller, 2016; Braim & Bilal, 2023). More than 30 years have passed since the initial concept was introduced, during which both corporate structures and the level of automation of management processes have undergone significant transformation. In this regard,

the COSO model has evolved, which was reflected in the emergence of three key modifications: COSO I, COSO II and the integrated COSO ERM model (COSO, 2017; SCCE & HCCA, 2020; Walker, 2022; Reuters, 2025).

The latest version of the concept focuses on integrating risk management with the strategic objectives of the enterprise, providing tools that include objective setting, event identification, risk assessment, response development, monitoring and information support – for effective response to changes in the external and internal business environment. The implementation of the COSO ERM system allows enterprises not only to respond effectively to risks, but also to make informed management decisions based on an analytical approach to control. For a deeper understanding of the features of this system, it is advisable to analyse each of its key components separately, as shown in Figure 1, which will allow for a more accurate assessment of its impact on corporate governance.

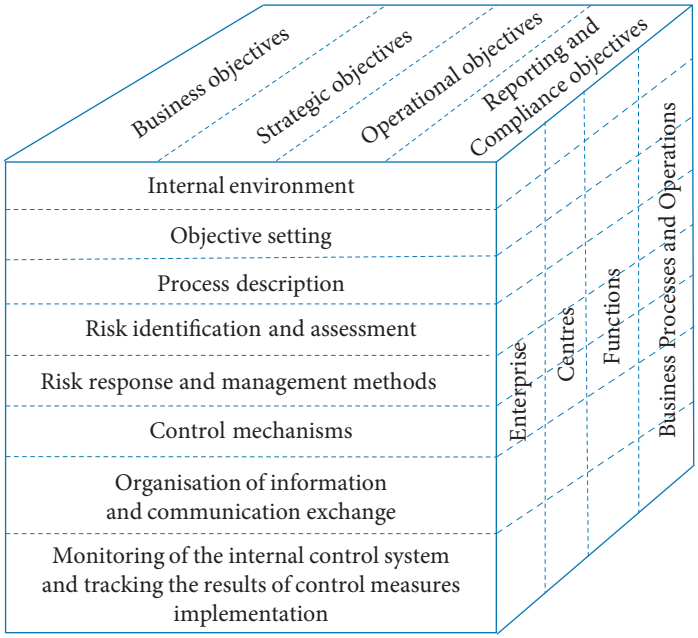

Figure 2. COSO-ERM integrated internal control concept

Source: developed based on COSO (2017)

The image illustrates a three-dimensional model of a risk management system based on the COSO ERM concept, which serves as a visual representation of an integrated internal control system. This model is depicted in the form of a cube, where each face reflects key elements of effective risk management within an organisation. The first key aspect of the COSO model is "Internal Control – Integrated Framework," which focuses on internal control. It is based on five interrelated components. The control environment provides the foundation – it covers ethical standards, staff competence, and the management system. The next step is risk assessment, which allows for the identification and evaluation of threats to achieving objectives (Koli *et al*, 2025). Control activities are the actions and procedures implemented to mitigate risks. Information and communication ensure access to data and effective interaction within the organisation. The final component, monitoring, allows for continuous evaluation of the quality of internal control and its improvement.

In the work of L. Koli *et al.* (2025), the COSO structure is presented as a logical and interdependent system that encompasses the key components of internal control. The authors emphasise the importance of each component in ensuring reliable risk management, which aligns with the classic architecture of the model. This interpretation of the COSO model's components is consistent with its generally accepted understanding and effectively demonstrates their integration into management practice. For comparison, R.R. Moeller (2016) more thoroughly underscores the connection between the control environment and corporate culture, which deepens the understanding of the first component of the COSO model as the basis for forming a long-term risk management strategy. Meanwhile, the findings of J.R.S. Fraser *et al.* (2021) expanded the analysis, demonstrating how COSO ERM components can be adapted to specific industries through flexible monitoring mechanisms and integration with digital tools, which was not detailed in L. Koli *et al.* (2025). The results of this research correlate with the authors' conclusions, confirming that the implementation of the COSO ERM model contributes to increased management maturity, the integration of risks into strategic planning, and the ensuring of enterprise resilience, particularly in the context of digital transformation.

In 2017, COSO updated its framework, creating a second important framework: "Enterprise Risk Management – Integrating with Strategy and Performance" (How

power and…, 2025). This model was aimed not only at control but also at strategic risk management. It focuses on corporate governance and risk management culture, integrates risk assessment into strategic planning and decision-making, and helps to improve performance. The model also includes a continuous review of processes and a reporting system that makes risk management transparent to all stakeholders (Cybersecurity and ERM…, 2024). COSO has become a standard in auditing, financial management, compliance, and corporate governance. It is used worldwide by large companies, banks, government bodies, and auditing firms. Applying the COSO model gives companies strategic advantages that positively affect management effectiveness, control, financial stability, and stakeholder trust. One of the main advantages is improved risk management. COSO allows for a systematic approach to identifying and assessing risks, taking timely measures to minimise them. This means that a company can not only react to problems but also anticipate them and act proactively (How power and…, 2025). The analysis of the source confirmed the strategic nature of the updated COSO ERM model, which integrates risk management into planning, control, and reporting processes, allowing companies to increase their transparency and resilience in a changing environment; the results of this study correlate with own conclusions, as they also attest to the advantages of comprehensive risk management for strengthening management effectiveness and stakeholder trust.

The COSO model significantly enhances corporate compliance with current legislation, especially in areas such as financial accounting, internal control, auditing, and corporate governance. Its application provides a framework for implementing a control system that is necessary for adhering to regulatory requirements, particularly the provisions of the Sarbanes-Oxley Act (SOX), enacted in the US in 2002 in response to financial scandals at companies like Enron and WorldCom (Beasley *et al*., 2017). The findings of this study correlate with the conclusions of M.S. Beasley *et al*. (2017), as it also demonstrates that using COSO ERM helps to create a transparent and controlled management environment, and increases corporate compliance with both national and international legislation. This is particularly relevant given the digital transformation and heightened requirements for financial and non-financial reporting. It is reasonable to agree that the practical value of COSO as a regulatory compliance framework remains considerable, owing to its adaptability and systematic nature.

According to Section 404 of SOX (Public Law No. 107-204, 2002), companies are obliged to report annually on the effectiveness of internal control over financial reporting, while independent auditors must provide attestation of these reports. The COSO Framework 2013 (an updated version of the original 1992 framework) has been officially recognised by the U.S. Securities and Exchange Commission as an authoritative approach for evaluating internal control. The use of COSO enables companies to identify key risks and control points, document control procedures and policies, regularly monitor system effectiveness, and demonstrate transparency and regulatory compliance. In addition, COSO reduces legal risks, improves the reliability of financial reporting, and enhances communication between management, supervisory bodies, and shareholders (Moeller, 2013).

Thus, the implementation of the COSO model is not merely a managerial decision but a critically important step towards legal compliance, reducing regulatory pressure, and building investor confidence, especially within a globalised market environment. It reduces legal risks and increases the overall transparency of corporate operations. Another important advantage of implementing COSO is the growth of operational efficiency. Owing to clearly defined processes and control measures, companies can optimise internal procedures, minimise duplication of functions, reduce costs, and improve cross-departmental interaction. All of these factors contribute to better decision-making based on reliable information (University of Massachusetts Amherst, 2024). Furthermore, the COSO model substantially strengthens the system of corporate governance, grounded in the principles of integrity, transparency, accountability, and effective control.

COSO (2013) identifies five key components of the internal control system, with particular emphasis on the control environment as the foundation upon which the entire risk management framework is built. These include: ethical values and integrity (whereby the organisation cultivates a corporate culture in which honesty and ethics are non-negotiable standards of behaviour); accountability (ensuring responsibility is defined at all managerial levels for both decision-making and compliance with control procedures); board of directors and audit committee involvement (providing oversight of risks and the effectiveness of internal policies); staff competence (ensuring appropriate qualifications and training); and an organisational structure that supports effective control. The role of management in the COSO model is fundamental. Management is responsible for developing and implementing the internal control system, formulating risk management policies, creating an effective information environment, and fostering a culture of transparency (COSO, 2013; Moeller, 2013). Due to these principles, the COSO model helps to increase investor and partner trust for several reasons:

1. Transparent financial reporting allows investors to have a clear understanding of the company's financial status.

2. Reduction of fraud and unethical behaviour through preventative control procedures.

3. Increased stability of management decisions, which signals a company's reliability in the long term.

4. The presence of a clear system for responding to risks reduces investor uncertainty about the company's future.

In combination, this enhances a company's investment appeal, contributes to its resilience to crises, and ensures compliance with ESG (Environmental, Social, and Governance) norms. These are increasingly seen as mandatory for large companies in the global market. A well-structured

control system based on the COSO model also strengthens information security, helps to better protect data, and reduces the risk of cyber attacks (Risk Management Association of India, 2025). Overall, implementing COSO allows organisations not only to meet standards but also to gain a competitive advantage in the market through resilience, flexibility, and long-term strategic thinking.

To better understand the specific features of the COSO ERM model, it was compared with another widely used international framework – ISO 31000:2018 (2018). Both approaches share the common objective of ensuring effective risk management but differ substantially in structure, philosophy, and scope of application. At the national level, the Law of Ukraine No. 996-XIV (1999) defines the legal and regulatory framework for accounting and reporting, including requirements for internal control that guarantee the transparency and reliability of financial information necessary for managerial decision-making. Similarly, the Law of Ukraine No. 2258-VIII (2017) emphasises the importance of ensuring the quality of internal control and risk management systems in order to achieve the reliability of financial reporting, which closely aligns with the principles of the COSO model. The findings of this research are consistent with the provisions of these legislative acts, since COSO ERM likewise integrates risk assessment, control, and monitoring processes into corporate governance systems, thereby supporting compliance with requirements on the quality of accounting, reporting, and auditing. It is reasonable to conclude that these laws provide a solid basis for the implementation of COSO in the Ukrainian corporate sector, ensuring compliance with international standards and fostering the development of effective internal control. Within this study, these normative acts were employed as a methodological foundation for analysing the potential adaptation of COSO ERM to the national regulatory environment.

COSO ERM focuses on integrating risk management into the overall system of strategic management and corporate control. Its peculiarity lies in its clearly structured, multi-dimensional model that includes components of internal control, organisational objectives, and levels of influence. It involves the active participation of the board of directors and management, which is particularly important in large corporations. ISO 31000:2018 (2018), in turn, is built as a flexible framework that can be adapted to any type of organisation. It does not contain rigid requirements or a structured model but provides general principles and guidelines for the risk management process: establishing the context, identification, assessment, response, and monitoring. The main difference is that COSO considers risks as part of achieving strategic goals, while ISO 31000:2018 (2018) focuses on a continuous cycle of assessment and response. Additionally, COSO requires greater effort regarding internal audit and control, which can complicate its implementation in small and medium-sized businesses. At the same time, ISO 31000:2018 (2018) is often used in the public sector, project management, and non-profit organisations. It is also appropriate to consider ISO 22301:2019 (2019), which focuses on ensuring business resilience by creating a business continuity management system. This standard complements the COSO approach by focusing on preparation for disruptions, overcoming them, and a quick resumption of operations, which is especially important for companies operating in a highly volatile external environment. Its advantage is its universality, and its disadvantage is less procedural detail compared to COSO. Thus, the choice between models depends on the scale of the organisation, available resources, industry specifics, and the degree of integration of risk management into the overall strategy. In the practice of large corporations, a combination of both models is appropriate: COSO as a strategic foundation and ISO as a tactical tool for specific processes.

During the analysis of risk management practices, it was established that the COSO ERM model, especially after its 2017 update, significantly transformed approaches to corporate control and risk management in both public and private organisations. The main innovation was a shift in focus from a traditional control approach to strategic risk management, which is integrated into the decision-making process at all levels (COSO, 2017). Before the implementation of COSO ERM, companies typically viewed risks in isolation within individual departments. The emergence of the COSO ERM Framework contributed to the institutionalisation of a systematic approach to risk management, covering strategic, operational, financial, and regulatory risks (Frigo & Anderson, 2011). Thus, control became not only a mechanism for detecting violations but also a tool for building a competitive advantage by identifying risks at the strategic planning stage. The results of this study correlate with the authors' findings, as it was established that the integration of COSO ERM into strategic planning processes increases an organisation's ability to proactively identify and minimise risks, which ensures long-term stability and competitiveness. The authors' approach is worth agreeing with, according to which control within COSO ERM not only performs a function of monitoring and compliance but also serves as a tool for achieving strategic advantages through the early identification of risks and the construction of a management system based on an analytical approach.

G. Mensah & D. Gottwald (2016) noted that the successful implementation of the COSO ERM Framework contributes to an organisation's increased resilience due to better alignment of objectives, resources, and risk assessment that arise both within the company and in the external environment. The research showed that companies that use COSO as a tool for strategic risk management demonstrate better results in the long term. This is worth agreeing with, as the results of this study confirm that the implementation of COSO ERM strengthens the strategic alignment between management objectives, risk assessment, and resource allocation, which correlates with the analytical conclusions obtained regarding the long-term effectiveness of such approaches. The work of J. Lam (2014) also confirmed the effectiveness of COSO as a flexible model that allows management to integrate risk management into business

processes without losing efficiency. The author emphasised that it is the adaptability of the COSO model that enables organisations to create "antifragile" management systems – capable not just of withstanding crises but of growing because of them. This can be agreed with, as the adaptability of the COSO ERM model, identified in the analysis, indeed makes it possible to form management systems that not only maintain functionality during periods of crisis but also contribute to the organisation's development through proactive risk management. In addition, an updated study (Scale digital transformation…, 2021) proves that organisations that use COSO as a basis for building internal control systems and strategic planning demonstrate a higher level of resilience in conditions of economic uncertainty. COSO allows for the creation of mechanisms for quick adaptation through effective monitoring of key risks and opportunities.

The COSO ERM model also transformed the role of a company's governing bodies the board of directors and management received clear guidelines for risk monitoring, responsibility, and accountability, which has become a standard for investors, shareholders, and regulators (Beasley *et al.,* 2017). Through the implementation of COSO ERM, the level of alignment between an organisation's strategic goals and its risk profile increases. In addition, the model has been adapted to changes in the business environment, including the growing impact of cyber risks, ESG factors, and crisis conditions (e.g., the COVID-19 pandemic), which proves its flexibility and relevance in modern corporate governance (SCCE & HCCA, 2020; Huber *et al*., 2025). Comparing the approach of C. Huber *et al*. (2025) with more classic approaches, such as in the work of J. Lam (2014), one can see a certain evolution in the focus of COSO's application. While J. Lam (2014) emphasised the flexibility of the model as a tool for adapting to external threats, C. Huber *et al*. (2025) went a step further, demonstrating its ability to be strategically integrated into management practices and increase organisational resilience in conditions of growing complexity. Thus, the results of the C. Huber *et al*. (2025) study confirmed the relevance of COSO ERM as not only a tool for compliance with regulatory requirements but also an effective means of forming a comprehensive corporate governance system capable of quickly responding to new types of risks. The results of this study correlate with the results of the present analysis of the implementation of the COSO model in the context of the transformational business environment of enterprises with a transitional economy.

T. Viscelli *et al*. (2016) also analysed the role of ERM in the development of corporate risk management, pointing out the importance of the interrelationship between strategy, budget, and risk culture. They argue that a focus on risk management directly correlates with an organisation's adaptability in crisis situations, which reflects some of the COSO principles. It is reasonable to agree with the conclusions of T. Viscelli *et al.* (2016), as the results of the study confirm that an effective combination of risk management with strategic planning and budgeting contributes to an increase in the enterprise's flexibility in response to external threats. C. Hayne & C. Free (2014) described the process of institutional internalisation of COSO ERM as an innovative practice – from the creation of standards to widespread adoption. This shows that COSO has become not just a tool, but a globally recognised model, integrated into the culture and management processes of global organisations. It is worth agreeing with the approach of C. Hayne & C. Free (2014), who argued that the COSO model has transformed from a set of technical instructions into an institutionalised management practice, recognised at a global level and integrated into corporate culture. I. Makarchuk (2020) considered strategic risk management as a prerequisite for increasing the effectiveness of corporate governance in an unstable environment. The results of this study correlate with this approach, as the expediency of integrating risk management into the overall strategy of the enterprise has been confirmed. K. Nazarova *et al*. (2021) analysed the use of a questionnaire as a tool for assessing internal control in accordance with the COSO Framework, with which it is worth agreeing, as the results of this study also confirmed the effectiveness of standardised self-assessment tools for improving the control environment. K. Zajc Kejžar *et al.* (2024) in their work showed that a high level of global uncertainty forces European companies to revise their approaches to risk management, which is consistent with the conclusions of this study regarding the need to adapt COSO ERM to new external environmental challenges. I. Dvorski Lacković *et al.* (2022) proposed a three-factor model for the implementation of ERM in non-financial companies, which emphasises the importance of organisational culture, leadership, and the regulatory framework. This approach can be agreed with, as the results of the analysis also confirmed the dependence of the effectiveness of COSO implementation on internal organisational factors. J. Awad & R. Martín-Rojas (2024) proved that digital transformation strengthens organisational resilience through the development of innovation and learning. The results of the study confirm the relevance of these factors in the context of adapting COSO ERM to the conditions of digitalisation. T. Liu & J. Qi (2024) investigated the mechanism of the impact of digital transformation on enterprise resilience from the perspective of financial sustainability. Their conclusion about the critical importance of digital processes for effective risk management is consistent with the conclusions obtained in this work regarding the adaptation of COSO to the conditions of the digital economy.

Enterprises that implemented elements of this model demonstrated a higher level of adaptability to external threats, a better structure of internal processes, and increased transparency of management decisions. The implementation of COSO ERM, particularly its components of strategic planning, internal control, and monitoring, contributed to the construction of systems oriented toward preventative response (COSO, 2017). In various sectors of the economy, the model has been used as a tool for

integrating risks into a company's overall strategic cycle. Companies that applied a holistic approach were able to reduce losses associated with crisis events such as the COVID-19 pandemic, cyber attacks, supply chain disruptions, or regulatory changes. For example, in 2008, Airbus Group deployed a centralised ERM system based on the Active Risk Manager (ARM) platform, which integrates COSO principles (Airbus Group – case study, n.d.). Due to the standardisation of risks, the centralisation of monitoring, and the transparency of processes, the company achieved: a reduction in the duplication of control measures; a rapid response to external threats; increased flexibility in crisis situations; and the preservation of operational resilience and business value. In Austria, a number of medium-sized family companies modernised their risk management processes during the pandemic by implementing both formal COSO ERM tools (e.g., risk matrices, scenario analysis) and informal practices. This comprehensive approach contributed to an increase in their resilience, employee loyalty, and operational crisis management (Cobb, 2023). The combination of COSO with modern digital tools for analytics and information exchange proved to be effective, which significantly increased the quality of real-time risk monitoring.

One of the strongest aspects of COSO ERM has been the creation of a unified management environment where strategy, control, and risk assessment function in an interconnected way. This synergy has ensured systematic accountability and fostered the development of corporate ethics and transparency. At the same time, challenges have also been observed. Some businesses have applied the model formally, limiting themselves to documenting policies without practical implementation. In such cases, the expected results were not achieved, which indicated a need to change approaches to internal communication and staff training. Another important aspect is the practice of adapting COSO ERM to the conditions of small and medium-sized businesses. Many companies use a simplified version of the model – for example, by focusing only on key risks or operational efficiency. Despite limited resources, even basic implementation allows for the creation of a foundation for long-term risk-oriented management. A further important point is the combination of COSO with other framework models, particularly ISO 31000:2018 (2018). This integration promotes a more flexible approach to risk management, especially in multinational companies. In the context of digital transformation, the effectiveness of COSO has grown when supplemented with IT solutions – analytical platforms, automated control tools, and ERP systems.

The COSO ERM methodology gained significant dissemination in organisations where compliance with regulatory requirements, financial reporting, and accountability to external stakeholders were essential. It enables risks to be formalised, changes in the external environment to be tracked, and complex processes to be effectively managed. In a number of case studies, the model demonstrated a positive impact on reducing losses, improving the effectiveness of internal audit, and strengthening investor trust. For instance, the findings of R. Moshesh *et al.* (2018) showed that the implementation of an adapted ERM framework based on the COSO model contributed to: improving alignment between strategic objectives and risk processes; reducing losses through revised organisational architecture; and enhancing the role of personnel by upgrading their skills to work with ERM. At the same time, critical review revealed that to achieve full effectiveness the model required deep cultural transformation within organisations. Without the formation of a risk management culture, leadership involvement, and systematic engagement with employees, results remained limited. In some cases, there was a lack of flexibility in adapting the model to the specifics of an industry or region, which complicated its implementation. Attention was also paid to the growing importance of innovative risks – in particular, those related to the implementation of artificial intelligence, automation, and cloud services. COSO ERM allowed for the systematisation of approaches to managing these challenges but required a constant updating of practices in response to new threats. Effective management of modern risks became possible only under conditions of a regular review of procedures, openness to change, and the involvement of external expertise. The general assessment of the practical application of COSO ERM has shown its ability to increase the flexibility and resilience of organisations. Its contribution to building systems capable of not only reacting to risks but also using them as a source of strategic opportunities was important.

Conclusions

The study achieved its set objective, which was to analyse the peculiarities of implementing the COSO ERM risk management model in the management practice of enterprises, evaluate its effectiveness, and formulate recommendations for adapting this model to the conditions of the transformational business environment. Attention was paid to Ukrainian enterprises with a transitional economy, where the level of risk, institutional uncertainty, and regulatory pressure remains high, while taking into account the experience of foreign enterprises and organisations.

An analysis of literary sources and examples of COSO ERM application made it possible to conclude that this model is one of the methodologies for organising systematic risk management. It covers five main components (control environment, risk assessment, control activities, information and communication, and monitoring) and is clearly integrated with the processes of strategic planning, internal control, and corporate governance. This ensures not only a reduction in the probability of risky events but also an increase in organisational flexibility, stability, and competitiveness of enterprises. The implementation of COSO ERM contributed to a reduction in losses during the COVID-19 pandemic, faster adaptation to regulatory changes, minimisation of cyber attacks, and a more effective response to disruptions in supply chains. It was also established that COSO significantly increases the level of reporting transparency, builds trust from external stakeholders, reduces

legal risks (in the context of compliance with acts such as the Sarbanes-Oxley Act), and ensures the accountability of management personnel.

At the same time, barriers that complicate the adaptation of COSO in Ukrainian realities were identified: a low level of risk-oriented thinking, limited financial and human resources, and weak integration with digital platforms. This applies to small and medium-sized businesses, where risk management often remains intuitive or fragmented. Promising areas for further research are an empirical analysis of the effectiveness of COSO ERM in enterprises of various industries, a comparison with alternative models, a study of the adaptability of COSO to the conditions of digital transformation (in particular, in the aspects of Big Data, AI, cybersecurity), and the development of industry-specific recommendations for enterprises in countries with a transitional economy.

Acknowledgements
None.

Funding
None.

Conflict of Interest
None.

References
[1] Airbus Group – case study. (n.d.). Retrieved from https://riskonnect.com/customer-success-stories/airbus-group/.
[2] Awad, J., & Martín-Rojas, R. (2024). Digital transformation influence on organisational resilience through organisational learning and innovation. *Journal of Innovation and Entrepreneurship*, 13, article number 69. doi: 10.1186/s13731-024-00405-4.
[3] Beasley, M.S., Branson, B.C., & Hancock, B.V. (2017). *Developing key risk indicators to strengthen enterprise risk management*. Retrieved from https://www.scribd.com/document/802587278.
[4] Benekos, I., Yannis, G., & Mavromatis, S. (2020). Implementing enterprise risk management in road organizations: Considerations and a proposed roadmap. *Risk and Decision Analysis*, 8(1-2), 39-65. doi: 10.3233/RDA-190055.
[5] Braim, S.J., & Bilal, R.B. (2023). The (COSO) framework: Implications of internal control components on the performance manufacturing companies. *Qalaai Zanist Scientific Journal*, 8(1), 1203-1227. doi: 10.25212/lfu.qzj.8.1.48.
[6] Cobb, M. (2023). *ISO 31000 vs. COSO ERM risk management standards*. Retrieved from https://www.techtarget.com/searchcio/feature/ISO-31000-vs-COSO-Comparing-risk-management-standards.
[7] COSO. (2013). *Internal control – integrated framework: Executive summary*. Retrieved from https://www.sechistorical.org/collection/papers/2010/2013_0501_COSOInternal.pdf.
[8] COSO. (2017). *Enterprise risk management: Integrating with strategy and performance*. Retrieved from https://web.archive.org/web/20171029145946/https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf.
[9] Cybersecurity and ERM top audit committee agendas. (2024). Retrieved from https://deloitte.wsj.com/cfo/cybersecurity-and-erm-top-audit-committee-agendas-5f67bb08.
[10] Dahmen, P. (2023). Organizational resilience as a key property of enterprise risk management in response to novel and severe crisis events. *Risk Management and Insurance Review*, 26(2), 203-245. doi: 10.1111/rmir.12245.
[11] Dvorski Lacković, I., Kurnoga, N., & Miloš Sprčić, D. (2022). Three-factor model of Enterprise Risk Management implementation: Exploratory study of non-financial companies. *Risk Management*, 24(2), 101-122. doi: 10.1057/s41283-021-00086-3.
[12] Fraser, J.R.S., Quail, R., & Simkins, B. (2021). *Enterprise risk management* (2nd ed.). Hoboken: Wiley.
[13] Frigo, M.L., & Anderson, R.J. (2011). Strategic risk management: A foundation for improving enterprise risk management and governance. *Journal of Corporate Accounting & Finance*, 22(3), 81-88. doi: 10.1002/jcaf.20677.
[14] Gleißner, W., & Berger, T.B. (2024). Enterprise risk management: Improving embedded risk management and risk governance. *Risks*, 12(12), article number 196. doi: 10.3390/risks12120196.
[15] Hayne, C., & Free, C. (2014). Hybridized professional groups and institutional work: COSO and the rise of enterprise risk management. *Accounting, Organizations and Society*, 39(5), 309-330. doi: 10.1016/j.aos.2014.05.002.
[16] Hillson, D. (2020). *What is risk? Towards a common definition*. A *common definition*. Retrieved from https://www.scribd.com/document/319840259/What-is-Risk-A-Common-Definition.
[17] Hopkin, P. (2017). *Fundamentals of risk management: Understanding, evaluating and implementing effective risk management*. London: Kogan Page Publishers.
[18] How power and utility companies can proactively manage risks in a new era of uncertainty. (2025). Retrieved from https://surl.li/vjnnmw.
[19] Huber, C., Kraus, K., & Meidell, A. (2025). Integrating the balanced scorecard and enterprise risk management: Exploring the dynamics between management control anchor practices and subsidiary practices. *Management Accounting Research*, 66, article number 100924. doi: 10.1016/j.mar.2024.100924.
[20] ISO 22301:2019. (2019). *Security and resilience – business continuity management systems – requirements*. Retrieved from https://www.iso.org/standard/75106.html.

[21] ISO 31000:2018. (2018). *Risk management – guidelines*. Retrieved from https://www.iso.org/standard/65694.html.
[22] Koli, L., Kalra, S., Thakur, R., Saifi, A., & Singh, K. (2025). AI-driven IRM: Transforming insider risk management with adaptive scoring and LLM-based threat detection. *ArXiv*. doi: 10.48550/arXiv.2505.03796.
[23] Lam, J. (2014). *Enterprise risk management: From incentives to controls* (2nd ed.). Hoboken: John Wiley & Sons.
[24] Law of Ukraine No. 2258-VIII "On Auditing Financial Statements and Auditing Activities". (2017, December). Retrieved from https://zakon.rada.gov.ua/laws/show/en/2258-19/ed20171221#Text.
[25] Law of Ukraine No. 996-XIV "On Accounting and Financial Reporting in Ukraine". (1999, July). Retrieved from https://zakon.rada.gov.ua/laws/show/en/996-14/ed19990716#Text.
[26] Liu, T., & Qi, J. (2024). The mechanism of enterprise digital transformation on resilience from the perspective of financial sustainability. *Sustainability*, 16(17), article number 7409. doi: 10.3390/su16177409.
[27] Makarchuk, I. (2020). Strategic enterprise risk management. *Economy and State*, 8, 107-111. doi: 10.32702/2306-6806.2020.8.107.
[28] Mensah, G., & Gottwald, D. (2016). Enterprise risk management: Factors associated with effective implementation. *Risk Governance and Control: Financial Markets & Institutions*, 6(4), 175-206. doi: 10.22495/rcgv6i4c1art9.
[29] Moeller, R.R. (2013). *Executive's guide to COSO internal controls: Understanding and implementing the new framework*. Hoboken: John Wiley & Sons.
[30] Moeller, R.R. (2016). *Brink's modern internal auditing: A common body of knowledge* (8th ed.). Hoboken: John Wiley & Sons.
[31] Moshesh, R., Niemann, W., & Kotzé, T. (2018). Enterprise risk management implementation challenges: A case study in a petrochemical supply chain. *South African Journal of Industrial Engineering*, 29(4), 230-244. doi: 10.7166/29-4-1782.
[32] National Competitiveness and Productivity Council. (2024). *Bulletin 24-4 IMD world competitiveness rankings*. Retrieved from https://competitiveness.ie/media/mgybdk2g/ncpc-bulletin-24-4-imd-world-competitiveness-rankings-2024.pdf.
[33] Nazarova, K., Nezhyva, M., Neviadomski, K., Kyrushko, P., & Bondar, N. (2021). Questionnaire as a tool for assessment of internal control system against COSO internal control – integrated framework. *International Journal of Scientific Research and Management*, 9(11), 2569-2576. doi: 10.18535/ijsrm/v9i11.em06.
[34] Public Law No. 107-204 "An Act to Protect Investors by Improving the Accuracy and Reliability of Corporate Disclosures Made Pursuant to the Securities Laws, and for Other Purposes". (2002, July). Retrieved from https://www.dol.gov/sites/dolgov/files/oalj/PUBLIC/WHISTLEBLOWER/REFERENCES/STATUTES/SARBANES_OXLEY_ACT_OF_2002.PDF.
[35] Reuters, T. (2025). *COSO updates its Enterprise Risk Management (ERM) framework to address modern data sources*. Retrieved from https://www.rehmann.com/resource/coso-updates-its-enterprise-risk-management-erm-framework-to-address-modern-data-sources/.
[36] Risk Management Association of India. (2025). *COSO ERM framework made easy: Turning risk into strategy*. Retrieved from https://rmaindia.org/coso-erm-framework-made-easy-turning-risk-into-strategy/.
[37] Scale digital transformation with risk management. (2021). Retrieved from https://deloitte.wsj.com/cfo/scale-digital-transformation-with-risk-management-01638384271.
[38] SCCE & HCCA. (2020). *Compliance risk management: Applying the COSO ERM framework*. Retrieved from https://www.coso.org/_files/ugd/3059fc_5f9c50e005034badb07f94e9712d9a56.pdf.
[39] University of Massachusetts Amherst. (2024). *FY24 enterprise risk management biennial report*. Amherst: University of Massachusetts Amherst.
[40] Viscelli, T.R., Beasley, M.S., & Hermanson, D.R. (2016). Research insights about risk governance: Implications from a review of ERM research. *SAGE Open*, 6(4). doi: 10.1177/2158244016680230.
[41] Walker, P.L. (2022). *Enabling organizational agility in an age of speed and disruption*. Retrieved from https://www.coso.org/_files/ugd/3059fc_cef1343e024a43c0b65d23ad0178d41e.pdf.
[42] Zajc Kejžar, K., Peljhan, D., Trkman, P., Vangeli, A., & Sprčić, D.M. (2024). Risk management practices of European companies in times of high global uncertainty. *Economic and Business Review*, 26(4), 222-225. doi: 10.15458/2335-4216.1345.

Аналіз моделі управління ризиками COSO: основні аспекти

Інна Віштак
Кандидат технічних наук, доцент
Вінницький національний технічний університет
21021, вул. Хмельницьке шосе, 95, м. Вінниця, Україна
https://orcid.org/0000-0001-5646-4996

Аліна Подорожнюк
Студент
Вінницький національний технічний університет
21021, вул. Хмельницьке шосе, 95, м. Вінниця, Україна
https://orcid.org/0009-0007-5526-9049

Еліза Войтко
Студент
Вінницький національний технічний університет
21021, вул. Хмельницьке шосе, 95, м. Вінниця, Україна
https://orcid.org/0009-0005-4381-2142

Анотація. Актуальність дослідження зумовлена зростанням невизначеності у зовнішньому середовищі, що потребує впровадження ефективних систем ризик-менеджменту. Метою дослідження було проаналізувати ключові аспекти моделі Committee of Sponsoring Organizations of the Treadway Commission Enterprise Risk Management (COSO ERM) та обґрунтувати можливості її застосування для інтегрованого управління ризиками на підприємствах. У дослідженні застосовано методи аналізу наукових джерел, структурно-логічного узагальнення та системного підходу. Розглянуто теоретичні та практичні аспекти управління ризиками на підприємстві з урахуванням викликів і тенденцій глобального ринку. Проаналізовано системний підхід до управління ризиками, який забезпечує комплексне охоплення всіх процесів підприємницької діяльності, пов'язаних з ідентифікацією, оцінкою та реагуванням на ризики. Визначено ключові компоненти методології COSO ERM, яка є однією з найбільш визнаних у світовій практиці. Модель COSO ERM базується на принципах інтегрованого управління, де ризики розглядаються не як ізольовані загрози, а як частина стратегічного планування та управлінських процесів. Було розглянуто застосування трикомпонентної структури COSO, що включала цілі підприємства, внутрішнє середовище та організаційні рівні впливу. Такий підхід дозволив гармонізувати стратегічні, операційні та звітні процеси в межах єдиної системи контролю. Розкрито сутність взаємозв'язку між основними елементами управління ризиками, що дало змогу адаптувати модель до особливостей функціонування підприємств різних галузей. Наведено аргументацію доцільності впровадження моделі COSO як інструменту підвищення стійкості бізнесу до невизначеності зовнішнього середовища. Запропоновано методологічні підходи до удосконалення ризик-менеджменту відповідно до вимог економічної безпеки та стратегічного розвитку. Практична цінність дослідження полягає у можливості використання результатів фахівцями у сфері ризик-менеджменту, внутрішнього аудиту та стратегічного управління

Ключові слова: внутрішній контроль; стратегічне планування; оцінка ризиків; корпоративне управління; адаптація моделей; інтеграція ризиків; бізнес-стійкість