UDC 347.77:330.3

DOI: https://doi.org/10.32782/2304-0920/4-102-3

Maslennikov Yevhen
ORCID: https://orcid.org/0000-0001-6400-7840
Popenko Oleksandr
Odesa I.I. Mechnikov National University

RISK MANAGEMENT AS A KEY FUNCTION OF INTERNAL AUDIT IN GLOBAL CHALLENGES

The risk management process is explored as a key function of internal audit in the context of global challenges such as macroeconomic and political instability, military conflicts, pandemics and climate change. There is a justified need to develop an effective strategy and flexible tools for identification, analysis and monitoring of business threats. Risk mapping stands out among such tools, which allows you to visually represent probable threats and their potential impact on business. An important role in this process has been proven for the internal audit, which ensures the reliability of the company's internal processes and serves as a basis for risk management. Auditors, through their functions, effectively identify weaknesses, analyze business processes, historical data, conduct an environmental assessment and can directly influence the elimination of identified risks. It was found that the risk management system includes several stages: identification, assessment, classification of risks, development of management strategies and constant monitoring. Risk assessment is based on quantitative and qualitative methods, such as statistical data analysis, probability calculation, SWOT analysis and Ishikawa diagram. Risk classification covers strategic, operational, financial and reputational risks. Suggested risk management strategies include avoiding, reducing, transferring, and accepting risks. The important role of internal audit in evaluating the effectiveness of these strategies is substantiated, by ensuring monitoring and regular review of the risk map to maintain their relevance and compliance with changing conditions. The necessity of integrating risk management into the general strategy of the organization to increase its resistance to external and internal threats is proved, which is especially relevant in the conditions of global economic and social changes.
Keywords: risk management, internal audit, global challenges, adaptive strategies, risk map, business processes, strategic goals, resistance to threats.

Statement of the problem. Today's global macroeconomic and political instability, combined with military conflicts, pandemics and climate change, creates an unprecedented number of challenges and risks that significantly affect the ability of businesses to achieve their strategic goals. In these conditions, companies and their internal audit structures face the task of being ready for various threats that may arise at any moment. The development of an effective strategy and flexible tools for identification, analysis and monitoring of business threats should be among the priority areas of internal audit development, as a key component of an effective enterprise management system designed to diagnose threats. Accordingly, the introduction of system processes for risk management and risk mapping are among the top priorities for business.

Risk mapping is a systematized, visually adapted presentation of possible risks that an organization may face, classified by their probability of occurrence and potential impact on the business. This tool enables identification and ranking, helping managers develop effective risk management strategies. In the conditions of global challenges, when organizations must quickly adapt to changes, the risk map becomes an indispensable element of a systemic approach to management.

One of the key aspects of risk management is its role in internal audit processes. After all, the function of internal control at the enterprise is a kind of business immunity that ensures the stability of internal processes and systems against any external and internal challenges, and risk management is a conditional vaccination that can help prevent and minimize potential consequences from expected threats. The integration of this area of responsibility into internal audit processes allows auditors to quickly focus on the most relevant areas of economic activity, thus ensuring an increase in the efficiency and effectiveness of audit inspections. It serves as a basis for planning audit activities and developing recommendations for reducing risks, which, in turn, contributes to the improvement of the overall management system of the organization.

Analysis of recent research and publications. The scientific works of such researchers as M. Crouhy [1], M.V. Karminska-Belobrova [2], O.M. Polinkevich [4], I.S. Yakos [5] and others. The analysis of scientific sources on the topic of risk management in economic activity demonstrates a persistent need for new strategies for building risk-oriented management, in particular, due to the potential of internal audit structures at the enterprise.

Objectives of the article. The purpose of the article is to explore risk management as a key function of internal audit that allows businesses to effectively respond to global challenges such as macroeconomic instability, military conflicts, and climate change. The task is to analyze the processes of identification, assessment and classification of risks, as well as the development of effective strategies for their management with the help of internal audit structures to increase business sustainability.

Summary of the main material. The positioning of the role of internal audit structures in the risk management system has various implementations. Thus, in industries with normative and regulated risk management processes, their administration is a task for a separate structural unit, and the role of internal audit is to be responsible for verifying the actions of such structures and compliance with an agreed set of policies and procedures [1]. But in today's realities, most other industries assign the function of risk identification and management to various related structures or specialists, from the project manager to the financial director [5]. But, of course, given the presence in the organizational structure, of all the typical departments, internal audit will usually be the most successful choice. Being outside the operational contour of the enterprise, internal audit interacts with all divisions, has up-to-date information about business processes, areas of responsibility and existing problems in the company's work and, as a rule, has a sufficient level of authority. It is the internal audit unit, due to its functional capabilities, that perfectly resists the main threats to successful risk mapping. In particular, resistance to change, when employees may show resistance to the introduction of new management tools and methods, and auditors already have ready-made motivational tools. Lack of resources – internal audit is an existing department that is designed to work with project tasks and is easily scalable. Ambiguity of roles and responsibilities – internal auditors know the company at a deep level and can always identify centers of responsibility.

The process of creating a risk management system includes several main stages: identification of risks, their assessment, classification, visualization, development of management strategies and monitoring and review of the risk map. Risk identification involves identifying all possible threats that the organization may face. Risk assessment includes determining the probability of their occurrence and potential impact. Classification of risks allows you to allocate them according to the level of priority, which helps to determine the most critical risks. Developing risk management strategies includes identifying measures to minimize or eliminate risks. Monitoring and reviewing the risk map ensures its relevance and compliance with current conditions.

Risk identification is an ongoing process that may have scheduled sessions but should never stop completely. There are many different approaches to identifying risks, but with the help of internal auditors, the most appropriate will be: analysis of historical data; assessment of business processes; assessment of the environment; interviews and questionnaires.

Analysis of historical data by internal audit is a key tool for identifying and managing risks in the organization. Reports of internal audits, conclusions of external audits, historical data on the formation of the company, its resource, organizational and other features, all this is usually already stored in the internal audit unit, which gives the maximum ratio of speed and quality in the process of identifying risks.

The method of evaluating the organization's business processes is longer, but no less effective. It helps to identify weaknesses and potential threats that can affect the efficiency and safety of operations. The first step is to identify the key processes that have the greatest impact on the business. These can be processes related to production, finance, personnel management, etc. After that, you need to describe these processes in detail by creating their flowcharts in BPMN (Business Process Model and Notation) format, documenting the steps, resources and responsible persons. Next, you should check to what extent these processes meet established standards and requirements by comparing them with industry standards or internal policies of the organization.

The environmental assessment method takes into account various external and internal factors affecting the organization. The assessment begins with an analysis of the macro environment, which includes political, economic, social and technological factors. Political changes, such as new legislation or regulatory requirements, can create risks for the organization that need to be considered. Economic factors such as currency fluctuations, changes in interest rates or economic crises can also affect a company's operations. Social factors, such as demographic changes, changes in consumer preferences or social trends, can create both risks and opportunities. Technological changes, including the development of new technologies or changes in the availability of technological resources, can significantly affect the competitiveness of an organization. An important stage of the assessment is the analysis of the microenvironment, which includes the study of direct market participants, such as competitors, suppliers, consumers and partners. Analysis of competitors helps to identify their weaknesses and strengths, as well as potential threats from their side. Assessing relationships with suppliers allows you to identify risks associated with dependence on certain counterparties or changes in supply conditions. Analyzing consumers helps to understand their needs and expectations, which can help identify opportunities to improve products or services.

Interviews and questionnaires are effective risk identification methods that help gather qualitative and quantitative information from internal and external stakeholders of the organization. These methods make it possible to identify potential threats and problems based on the qualified expert opinion and experience of the process participants. Interviews and questionnaires can be used separately or in combination, depending on the needs of the organization and the specifics of the process.

Interviewing, as a risk identification method, involves conducting in-depth conversations with key stakeholders such as managers, employees, suppliers and customers. This approach allows you to get detailed information about the risks and problems faced by the organization. During the interview, you can ask open-ended questions that contribute to identifying non-obvious risks and understanding the context of their occurrence. Interviews also provide an opportunity to clarify and expand respondents' answers, which increases the quality of the information collected.

Questionnaires are another important method of risk identification, which involves distributing standardized lists of questions to a large number of respondents. Questionnaires can contain both closed and open questions, which allows collecting both structured and free information. Surveying provides the ability to quickly collect data from a large number of people, which is its main advantage. Using questionnaires, it is possible to assess the prevalence of certain risks and identify trends in respondents' answers. To conduct effective interviews and surveys, it is important to develop appropriate data collection tools. Preparation of questions for interviews and questionnaires should take into account the specifics of the organization's activities and potential risks that need to be identified.

Risk assessment. After completing the stage of risk identification, it is necessary to carry out their assessment. Using all the collected information about each risk: its nature, probability of occurrence, possible consequences and conditions affecting its implementation, you can begin quantitative and qualitative risk assessment. Quantification includes analysis of statistical data, calculation of probabilities and determination of potential financial losses. It is the statistical method that is a priority for internal audit, it consists in studying the statistics of losses and profits that took place at a certain enterprise, in order to determine the probability of the event, to establish the amount of risk [2]. It is also important to consider the impact of risks on the organization's reputation, which are often difficult to quantify, but at the same time cannot be ignored.

Qualitative assessment is based on expert judgment and includes the use of methods such as FMEA (Failure Mode and Consequence Analysis), where each risk is assessed according to three parameters: probability of occurrence, severity of consequences and detectability. Each parameter is assigned a rating and the overall risk is calculated. Another approach is a SWOT analysis, which allows you to identify internal and external factors that affect risks. It is also advisable to use Ishikawa diagrams to identify cause-and-effect relationships and understand the root causes of risks.

After assessing the risks, they need to be prioritized. For example, risks with high probability and high impact require immediate attention and the development of measures to reduce or eliminate them. Risks with low probability and low impact can be accepted or monitored on an ongoing basis. It is important to involve all interested parties in the risk assessment process in order to get the most complete picture and understanding of risks from different perspectives.

Classification of risks. The most common categories of risks include: strategic, operational, financial and reputational. Each of these categories has its own subcategories and specific characteristics that help to better understand the nature of threats and effectively manage them.

Strategic risks are related to the organization's long-term goals and strategy. They may arise from changes in market conditions, the competitive environment, technological innovations or political and regulatory changes. This category includes risks associated with the wrong choice of strategy, underestimation of market trends, or other unsuccessful decisions that, in one way or another, comprehensively affect all economic activity.

Operational risks are related to the internal processes, systems and people that carry out normal business activities on a daily basis. They can occur due to failures in technological systems, personnel errors, inefficient processes or a lack of adequate controls. This category includes risks related to manufacturing processes, supply chain management, information security and internal fraud.

Financial risks relate to the financial health of the organization and other aspects of the activity of financial instruments tied to specific functions. These risks may arise from adverse changes in securities, fluctuations in exchange rates, changes in interest rates or financial crises. This category includes risks related to cash flow management, financial reporting, liquidity, and financing of the organization's activities.

Reputational risks are related to the image and reputation of the organization. They can arise due to negative publications, scandals, dissatisfaction of customers, partners and staff, as well as due to ethical violations or problems with the quality of products or services. Reputational risks can have a serious impact on an organization's credibility, market position and financial results.

In addition to the main categories, risks can be classified according to other criteria, such as external and internal risks, managerial and technological risks, legal risks, etc. External risks include those beyond the organization's control, such as natural disasters, economic crises, and changes in legislation. Internal risks arise from internal factors such as management decisions, operational failures or internal conflicts.

Before compiling a visual analytical adaptation of risks, it is necessary to first collect all possible risks and classify them according to the specified categories. After that, each risk is assessed for probability of occurrence and potential impact on the organization. This allows them to be prepared for placement on a matrix where each risk is ranked according to its probability and impact. Such matrices are actually risk maps and can have several levels of detail, depending on the needs of the organization and the complexity of its operational activities.

The most common ways of visualizing the risk map are: matrix form, map of thermal zones, graphs and diagrams, from the specialized forms, it is worth highlighting the Ishikawa diagram.

The specified list is not exhaustive, there are many variations of visualization of the risk map, depending on the specifics of the risks and the mechanics of managing them. In the case of building a risk map

	Influence			
Probability	**Minor**	**Substantial**	**Critical**	**Catastrophic**
Very often				
Sometimes				
Rarely				
Very rarely				

Figure 1. Matrix form

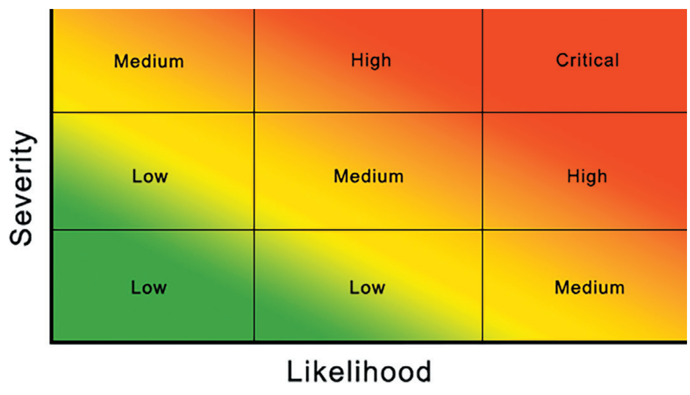

Figure 2. Heat Map

Source: [6]

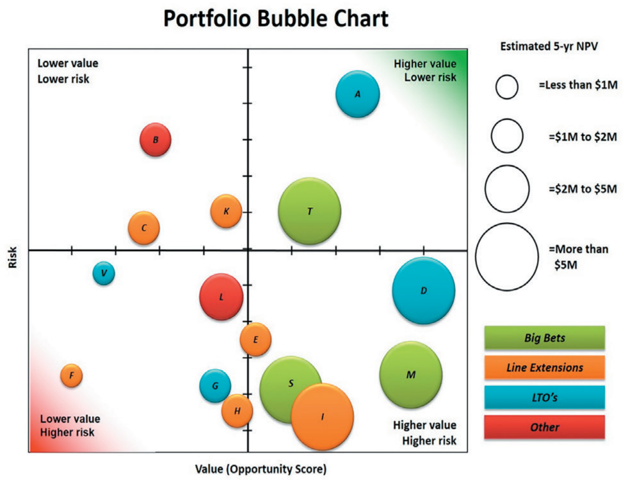

Figure 3. Graphs and charts

Source: [7]

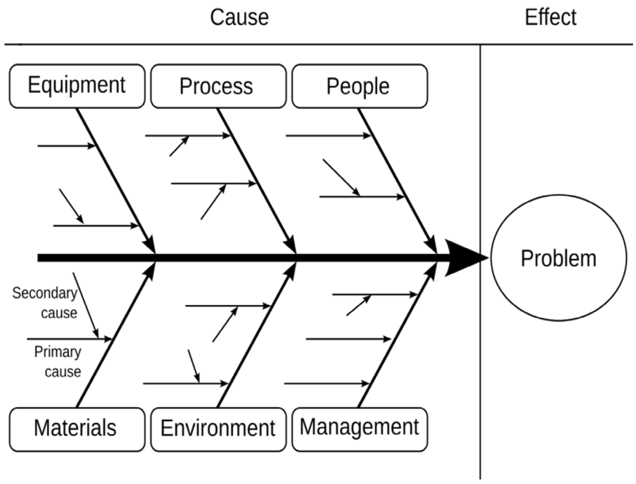

Figure 4. Ishikawa diagram

Source: [8]

by internal audit, the most appropriate method is a map of thermal zones. This approach provides a sufficient ratio of speed of formation, quality of filling and universality of application, while it has the possibility to modernize into bubble charts with increasing analytical depth and allows to comprehensively cover all areas of economic activity.

Risk management strategies. The next stage of the implementation of the risk management system includes the development of risk management strategies, which are divided into strategies of avoidance, reduction, transfer and acceptance. Before this, one of the most responsible stages, internal auditors must necessarily involve the entire management team, operational level stakeholders, according to their competences, and external experts.

Risk avoidance is one of the main risk management strategies, which consists in completely eliminating activities, processes or decisions that may lead to the occurrence of risk. This strategy becomes relevant when the potential negative impact of the risk is unacceptable to the organization or when the risk cannot be effectively controlled in other ways. Risk avoidance involves actively avoiding activities or situations that may lead to undesirable consequences. This requires careful analysis of business processes, the environment and potential threats to identify aspects of operations that may be too risky.

When the probability of a risk occurring is very high, and its impact can significantly disrupt the organization's operations, it is worth considering a risk avoidance strategy. If the consequences of taking a risk could be catastrophic for the organization, including significant financial losses, legal consequences or loss of reputation, avoiding the risk may be the only correct solution. Also, if the organization does not have effective means to control or reduce the risk to an acceptable level, avoiding the risk becomes appropriate.

An example can be the situation in construction, if the land plot for the project was obtained in violation of the law or has significant environmental threats, the company may refuse to participate in this project. Another example is the refusal to cooperate with unreliable partners. If a potential partner has a questionable reputation or a history of financial difficulties, the company may decide to avoid working with him to avoid the risk of default or financial loss.

The advantages of the risk avoidance strategy are that it allows the organization to completely exclude the possibility of the realization of certain threats. This can be especially important in industries with high security requirements, where even a small risk can have serious consequences. Avoiding risk also allows the organization to focus on safer and more stable opportunities.

However, risk avoidance has its drawbacks. It can limit opportunities for growth and development because the organization may miss out on potential opportunities. In some cases, risk aversion may lead to a loss of competitive advantage if competitors are willing to take those risks. Also, careful analysis of risks and making decisions about their avoidance can require significant resources and time.

At the heart of the risk reduction strategy is the desire to make risks more manageable. For example, in a manufacturing process, this may mean implementing additional safety measures or using more reliable equipment. In the financial sphere, this may include diversification of investments or the introduction of stricter credit policies. The main objective of risk reduction is to create conditions under which risks become less likely or less significant to the organization.

There are many ways to reduce risk, and they depend on the specifics of a particular organization and the nature of the risks it faces.

One of the main methods of reducing risk, which is especially inherent in internal audit structures, is the implementation of monitoring and control systems. Regular monitoring of key indicators and processes allows you to identify potential problems at an early stage and take measures to eliminate them before they turn into serious risks. For example, in the financial sector, this may include regular auditing of financial statements and transactions to detect possible fraudulent activities or errors. In the manufacturing sector, this may mean regular maintenance and inspection of equipment to prevent breakdowns or emergency situations.

Reducing risk may also include strengthening the internal control system. This involves the division of responsibilities between employees to avoid conflicts of interest and reduce the possibility of fraud, as well as the implementation of multi-level systems of checks and approvals for important decisions and operations. This approach helps ensure a higher level of control over key aspects of the organization's activities and reduces the likelihood of risk situations.

Implementation of new technologies is another effective way to reduce risk. Modern technologies can significantly increase the safety and efficiency of operations, reducing the likelihood of errors or emergency situations. For example, the use of automated control systems allows to reduce the human factor in production processes, and the introduction of modern information systems helps to ensure a higher level of data protection against cyber threats.

In addition, risk reduction may include the development of contingency plans. Such plans should include clear instructions for employees on actions in the event of risk situations, identification of responsible persons and resources that may be needed to eliminate the consequences of the risk. This allows for a quick and effective response to emergency situations, minimizing their impact on the organization's activities.

Risk transfer is one of the most effective risk management strategies, which is to transfer the responsibility for the risk to another party. This may include insurance, contracting with suppliers or partners, or outsourcing certain activities. The basic idea is to reduce the impact of potential negative events on the organization by transferring risks to external organizations or individuals who can better manage these risks or have more resources to compensate for them.

One of the most common methods of risk transfer is insurance. Insurance allows an organization to transfer financial risk to an insurer in exchange for payment of insurance premiums. This means that in the event of an insured event, the insurer assumes financial obligations to compensate for losses. For example, a company can insure its property against fire, theft or natural disasters. Thus, if one of these events occurs, the insurer will pay compensation, allowing the company to avoid significant financial losses.

Outsourcing is also an effective method of transferring risk. An organization may outsource part of its business processes or functions to third-party providers who specialize in those activities and can more effectively manage the associated risks. For example, a company can outsource IT support or logistics functions, thereby reducing the risks associated with managing these functions in-house. Outsourcing allows the company to focus on its core business, while transferring responsibility for supporting processes to specialists.

Contracting with suppliers or partners is also a common way to transfer risk. Contracts may contain provisions transferring responsibility for certain risks to the counterparty. For example, construction contracts may include terms requiring the contractor to provide insurance against property damage or an accident on the construction site. Thus, in the event of such events, the responsibility for compensation of damages will be borne by the contractor, and not by the customer.

The advantages of the risk transfer strategy are that it allows the organization to reduce the impact of potential negative events on its operations and financial condition. Risk transfer can be particularly useful for small and medium-sized enterprises, which may not have sufficient resources to manage large risks themselves. In addition, risk transfer allows a company to focus on its core business without being distracted by risk management that can be more effectively managed by other organizations.

However, risk transfer has its drawbacks. The cost of insurance or outsourcing services can be significant, and a company should consider these costs when deciding whether to transfer risk. In addition, risk transfer does not always guarantee full protection against negative consequences. For example, an insurance policy may have limitations or exclusions that do not cover all possible scenarios. Outsourcing can also create dependence on suppliers, and any problems with their performance can affect the organization's operations.

To successfully implement a risk transfer strategy, a company must conduct a thorough risk analysis and determine which of them can be transferred most effectively. It is also important to choose reliable partners and suppliers who have the experience and resources to effectively manage risks. The company must ensure that contracts and insurance policies are detailed and include all necessary provisions to protect against risks. Regular monitoring and review of these agreements is also necessary to ensure their relevance and effectiveness.

Risk acceptance is the conscious recognition and acceptance of the possibility of risk without taking active measures to avoid, reduce or transfer it. This strategy is used when the risk is assessed as acceptable, that is, its potential negative impact is not critical for the organization or when the costs of risk management exceed the potential losses from its implementation.

A risk-taking strategy may be appropriate in situations where the organization has sufficient reserves or resources to cover possible losses. For example, in a large company with high profitability, certain risks can be accepted without serious consequences for its financial condition. In addition, taking a risk can be justified when the probability of its occurrence is low and the possible losses are insignificant. In such cases, the cost of implementing risk management measures may not be profitable.

One example of risk acceptance is when a company decides not to insure certain assets because the cost of insurance premiums exceeds the potential losses from their loss. This may be particularly true for assets with low value or low probability of damage. The company can also accept the risks associated with new projects or innovations, understanding that some of them may not bring the expected results, but at the same time provide an opportunity for significant growth and development.

Acceptance of risk can also be justified when the organization has a plan of action in the event of the realization of the risk. This may include the creation of contingency funds or budgets to cover unforeseen costs, the development of disaster recovery plans, and other measures that enable a rapid response to the occurrence of risk and minimize its consequences. For example, a manufacturing company may have backup capacity or alternative suppliers that can be called upon in the event of major supplier disruptions.

The advantage of a risk-taking strategy is that it allows the organization to avoid the costs of managing risks that are low or acceptable. Risk acceptance can also facilitate greater flexibility and speed in decision-making because the organization does not have to spend time and resources developing and implementing measures to manage each risk.

However, the risk-taking strategy has its drawbacks. The main risk is that the organization may underestimate the possible impact of certain risks or incorrectly assess their probability. This can lead to significant losses if the risk materializes. In addition, acceptance of the threat may not be acceptable to some stakeholders, such as investors or regulators, who may require more proactive risk management measures. In such cases, the organization may face pressure from external stakeholders or lose the trust of investors.

Monitoring and viewing. Monitoring and reviewing the risk map is a key task for the internal audit department, because its high-quality performance will ensure effective risk management in the organization. These processes make it possible to detect changes in the threat environment in a timely manner, evaluate the effectiveness of implemented risk management measures and make the necessary adjustments to the risk map, ensuring its relevance and compliance with current conditions.

Monitoring of the risk map includes constant observation of identified threats and indicators that may signal changes in their status or probability of realization. The internal audit department performs this function by gathering data from various sources such as incident reports, financial performance, internal and external audits, and other relevant information. This allows you to identify trends, anomalies or potential problems at an early stage and take measures to solve them.

The review of the risk map is an integral part of the monitoring process and includes a regular assessment of the relevance and effectiveness of the risk map. The internal audit department should periodically review the risk map to ensure that all identified threats are still relevant and new ones have been identified and assessed. This includes checking the correctness of the assessment of the probability and impact of each risk, analyzing the effectiveness of the implemented management measures and determining the need for their correction or improvement.

The process of monitoring and reviewing the risk map begins with the identification of key indicators that help track changes in the risk environment. These indicators should be specific, measurable and correspond to the main threats of the organization. The internal audit department should regularly collect and analyze data on these indicators in order to identify and respond to potential threats in a timely manner.

An important element of monitoring is the use of automated risk management systems that allow digitization of data collection and analysis, increasing the accuracy and efficiency of the process. Such systems can provide real-time information on the state of risks, which allows internal auditors and management to quickly respond to changes and make informed decisions.

Regular review of the risk map includes conducting internal audits and assessments that allow checking the effectiveness of existing risk management measures. The internal audit department should hold regular meetings with management and other stakeholders to discuss monitoring results, identify new risks and determine the need to make changes to the risk map. This allows to ensure the state of awareness of all interested parties about the current state of risks and the measures taken for their management.

The review process also includes an analysis of external factors that may affect the organization's risk profile. This may include changes in legislation, economic conditions, technological innovations or other external factors that may affect the organization's operations. The internal audit department should consider these factors when reviewing the risk map to ensure it is relevant to current conditions.

Monitoring and reviewing the risk map also includes documenting all changes and assessment results. This allows you to save history, analyze trends and the effectiveness of implemented measures. The internal audit department must ensure adequate documentation and reporting to enable management to make informed decisions about risk management.

Conclusions from the study. Risk management is a critical function of internal audit, especially in the face of global challenges. Research shows that effective risk management can significantly increase the resilience of organizations to external and internal threats, enabling them to adapt to changing conditions and remain competitive.

Internal audit plays a key role in the risk management process, providing a systematic approach to the identification, assessment, monitoring and management of risks. An important component of this process is the use of modern methods and tools to identify potential threats and develop strategies to mitigate or eliminate them.

Historical data analysis, interviews and questionnaires, evaluation of processes and procedures, as well as other risk identification methods allow internal auditors to gain an even deeper understanding of the organization's risk environment. The use of various types of threat visualizations, such as risk matrices, heat maps, and decision trees, helps to more effectively present and communicate risks to management and other stakeholders.

Risk management in the face of global challenges requires from internal auditors not only a high level of professional competence, but also flexibility and the ability to quickly adapt to new conditions. Constant monitoring of the external environment, updating of risk assessments and development of adaptive risk management strategies are integral components of an effective internal audit. It is also worth emphasizing that the need to integrate risk management into the overall strategy of the organization, ensuring close cooperation between internal auditors and other functional units, as well as the use of modern technologies to increase the effectiveness of risk management is a guarantee of success. This approach will allow organizations not only to reduce the impact of negative factors, but also to use the opportunities that arise in the changing conditions of the global economic environment.

References:

1. Crouhy M., Galai D., Mark R. (2024) The essentials of risk management, 3rd edition. New York, NY : McGraw Hill.
2. Karminska-Belobrova M., Ignatova E. (Ed.) (2014) Risk management in entrepreneurship: study guide. Kharkiv: "Slovo". (in Ukrainian)
3. Moroz V. M., Moroz S. A. (2018). Risk management: academic. study guide. Kharkiv: NTU "KhPI". (in Ukrainian)
4. Polinkevich O., Volynets I. (2018) Justification of business decisions and risk assessment. Lutsk: Vezha-Druk. (in Ukrainian)
5. Yakos I. S. (2010) The risk map as an element of the risk management program. *Bulletin of Economic Science of Ukraine*, no.1 (17), pp. 160–162. (in Ukrainian)
6. Enterprise GRC blog. (2012) Heat maps: not quite so hot anymore? Available at: https://enterprisegrcblog.wordpress.com/2012/04/24/heat-maps-not-quite-so-hot-any-more/
7. PPM Execution (2014) Portfolio Bubble Chart. Available at: https://ppmexecution.com/five-uses-of-a-prioritization-scoring-model/portfolio-bubble-chart/
8. SafetyCulture (2024) Ishikawa Diagram: A Guide. Available at: https://safetyculture.com/topics/ishikawa-diagram/

Список використаних джерел:

1. Crouhy M., Galai D., Mark R. The essentials of risk management, 3rd edition. New York, NY : McGraw Hill, 2024.
2. Управління ризиками у підприємництві: навчальний посібник / Кармінська-Бєлоброва М.В., Ігнатова Є.М.. Харків : «Слово», 2014. 169 с.
3. Мороз В.М., Мороз С.А. Ризик-менеджмент: навч. посібник. Харків : НТУ «ХПІ», 2018. 140 с.
4. Полінкевич О., Волинець І. Обґрунтування господарських рішень та оцінювання ризиків: навч. посібник. Луцьк : Вежа-Друк, 2018. 336 с.
5. Якось І.С. Карта ризиків як елемент програми управління ризиками. *Вісник економічної науки України*. 2010, № 1 (17). С. 160–162.
6. Heat maps: not quite so hot anymore? *Enterprise GRC blog*. 2012. URL: https://enterprisegrcblog.wordpress.com/2012/04/24/heat-maps-not-quite-so-hot-any-more/
7. Portfolio Bubble Chart. *PPM Execution*. 2014. URL: https://ppmexecution.com/five-uses-of-a-prioritization-scoring-model/portfolio-bubble-chart/
8. Ishikawa Diagram: A Guide. *SafetyCulture*. 2024. URL: https://safetyculture.com/topics/ishikawa-diagram/

Масленніков Є. І.
Попенко О. О.
Одеський національний університет імені І. І. Мечникова

УПРАВЛІННЯ РИЗИКАМИ ЯК КЛЮЧОВА ФУНКЦІЯ ВНУТРІШНЬОГО АУДИТУ В УМОВАХ ГЛОБАЛЬНИХ ВИКЛИКІВ

Анотація
Досліджено процес управління ризиками як ключова функція внутрішнього аудиту в умовах глобальних викликів, таких як макроекономічна та політична нестабільність, військові конфлікти, пандемії та зміни клімату. Обґрунтована необхідність розробки ефективної стратегії та гнучкого інструментарію для ідентифікації, аналізу та моніторингу загроз бізнесу. Серед таких інструментів виділяється картування ризиків, що дозволяє візуально представляти ймовірні загрози та їх потенційний вплив на бізнес. Доведено важливу роль у цьому процесі внутрішньому аудиту, який забезпечує надійність внутрішніх процесів підприємства, і слугує основою для управління ризиками. Аудитори, через свої функції, ефективно ідентифікують слабкі місця, аналізують бізнес-процеси, історичні дані, проводять оцінку середовища та можуть безпосередньо впливати на усунення виявлених ризиків. З'ясовано, що система управління ризиками включає кілька етапів: ідентифікацію, оцінку, класифікацію ризиків, розробку стратегій управління та постійний моніторинг. Оцінка ризиків ґрунтується на кількісних і якісних методах, таких як аналіз статистичних даних, розрахунок ймовірностей, SWOT-аналіз та діаграма Ісікави. Класифікація ризиків охоплює стратегічні, операційні, фінансові та репутаційні ризики. Запропоновані стратегії управління ризиками включають уникнення, зменшення, передачу та прийняття ризиків. Обґрунтовано важливу роль внутрішнього аудиту в оцінці ефективності цих стратегій, шляхом забезпечення моніторингу і регулярного перегляду карти ризиків для підтримки їхньої актуальності та відповідності змінним умовам. Доведено необхідність інтеграції управління ризиками в загальну стратегію організації для підвищення її стійкості до зовнішніх і внутрішніх загроз, що особливо актуально в умовах глобальних економічних і соціальних змін.
Ключові слова: управління ризиками, внутрішній аудит, глобальні виклики, адаптивні стратегії, карта ризиків, бізнес-процеси, стратегічні цілі, стійкість до загроз.