DOI: https://doi.org/10.30525/978-9934-26-307-1-9

Olha Starenka
Candidate of Economic Sciences, Associate Professor,
Associate Professor at the Department of Accounting,
Analysis and Auditing
Odesa National Economic University

RISK ASSESSMENT IN THE INTERNAL CONTROL SYSTEM OF AN ENTERPRISE

Summary

The current state of enterprise development in Ukraine is characterized by a high level of uncertainty, dependence on internal and external factors, and increased influence of risks on their effective operation. This fact necessitates considering new approaches to the organization of a risk management system and the establishment of an effective internal control system for the enterprise as a means of risk identification. This can be done by identifying many risks arising from the enterprise activity; this necessitates creating a system of their management and imposes specific requirements for the internal control system. The study also analyzes different views of scientists on the risk essence, its influence on the activity of the enterprise and emphasizes that the opinions of researchers were generated in different approaches to its interpretation and developed towards detailing certain types of risks. The concept of risk assessment is formulated. It is noted that risk assessment creates the basis for identifying how risks will be managed. It is substantiated that the process of identifying risks in the internal control system that affect the efficiency of business processes, evaluating their effectiveness and building an internal control system in such a way that it is able to reduce the impact of risks on the functioning of an enterprise as a whole is of great importance. The nature of internal and external risks is clarified. It is also argued that the internal control system should be focused on identifying and assessing internal risks in terms of their impact and likelihood of occurrence. To achieve this, the criteria of risk assessment by directions of influence on the enterprise activity were developed. Risk assessment is proposed based on the criteria of probability of their occurrence and influence on the internal control subjects' ability to realize the operational goals according to the risk assessment matrix. It is proved that to improve the reliability of accounting and reporting information, it is necessary to timely predict the risks of displaying business transactions, identify weaknesses in the enterprise management process, diagnose manipulations with reporting; this will be possible only when creating an effective internal control system that will be able to detect all types of risks and ensure the successful development and stability of enterprises in a competitive *environment. The development and implementation of an effective risk management system will enable the enterprise to function steadily in the market and gain competitive advantages despite significant political, economic and social influences.*

Introduction

The current state of business development in Ukraine is characterized by a high level of uncertainty, dependence on a combination of internal and external factors of enterprise activity, as well as an increase in the impact of risks on an enterprise's effective operation. This is due to the instability of economic and political development, various crisis phenomena, significant inflation rates, the lack of a clear legal framework and its frequent changes, the use of worn-out equipment and outdated technologies, etc. Under such circumstances, the importance of risk management and the ability to assess the degree of influence of possible risks that become constant companions of entrepreneurial activity increase.

This fact necessitates considering new approaches to the organization of a risk management system and the establishment of an effective internal control system for the enterprise as a means of risk identification. This can be done by identifying many risks arising from the enterprise activity; this necessitates creating a system of their management and imposes specific requirements for the internal control system.

The ability to predict and correctly assess risks is important when conducting control measures at an enterprise. The internal control system should be focused on identifying and assessing internal risks and the factors that determine them, since the possibilities of control over them are higher than over external ones.

Managers and management personnel of enterprises need knowledge of the theory of risks and their practical application, timely consideration of risk factors in making management decisions, a well-organized process of assessing and reducing risks, aimed at quickly adapting enterprises' activities to the highly variable and unstable conditions of the external and internal environments of their functioning. To identify risks at an enterprise today, a modernized internal control system is needed, which will be able to identify various types of risks, ensure the stability and successful development of enterprises in a competitive environment, and also allow timely detection and minimization of risks in the management of financial and economic activities.

Currently, their successful development is directly related to the construction of an effective internal control system, the study of which is particularly relevant as a means of identifying organizational risks.

Part 1. Internal control as a component of the enterprise management system

Internal control occupies an important place in the enterprise management system. Considerable attention should be paid to improving its efficiency, because reducing the risk of asset loss and ensuring the reliability of financial reporting is possible only thanks to an effective internal control system that can assess risks in a timely manner.

Prospects for the development of the management system are related to internal control, since it is designed to ensure the performance of management functions directly related to the control function. The place of internal control in the management system is determined in the following areas: the internal control system processes information from internal (management) accounting for use in the management system, verifies accounting information for reporting to external users, processes information from external sources for forecasting purposes, provides information for making management decisions [1, p. 49].

Great importance is given to internal control in terms of accounting. The Law of Ukraine On Accounting and Financial Reporting in Ukraine, Article 8, paragraph 5, determines that an enterprise independently "develops a system and forms of internal (managerial) accounting, reporting and control of business operations, determines the rights of employees to sign accounting documents". Article 15 states that "control over compliance with the legislation on accounting and financial reporting in Ukraine is carried out by the relevant authorities within their powers provided by law" [2].

Recently, the importance of internal control has increased dramatically, in particular, in an environment where the responsibility of accounting services for the quality of reporting has increased. The organization of the internal control system at modern enterprises is one of the important tasks. But management attempts to organize it are not always successful. Very often, the measures taken are limited to documenting the necessary provisions and instructions and do not lead to the desired results. The main reason for this is the complexity of the organization of the internal control system, a laborious and lengthy process. It includes the study of regulatory documents; analysis of the activities of enterprises and their structural divisions; development of a system for setting goals and evaluating their achievement; development of regulatory documentation; implementation of a system of interacting and interrelated processes of an enterprise; planning activities for the further development of an enterprise.

The identification of many risks arising from an enterprise’s activities necessitates the creation of a management system for them and establishes certain requirements for the internal control system. It can provide information that allows you to predict possible risks that may adversely affect the future activities of an enterprise.

A study of the economic literature has shown that most scholars consider the system of internal control using the main components of such a model proposed by The Committee of Sponsoring Organizations of the Treadway Commission (COSO). This model contains five interrelated components, such as the control environment, risk assessment, control tools, information and communications, monitoring [3; 4, pp. 4–5]. It reflects the main concepts, definition of internal control and meaningful content of the main components. Namely, internal control is a process, a means to an end, and not an end in itself; internal control depends on people. It represents not only politics, management, and forms, but people at all levels of the organization; internal control can give a company's management and council only sufficient confidence, but not absolute guarantees [4].

According to the COSO model, internal control is a process carried out by the highest body that determines an enterprise's policy (for example, the supervisory board representing the owners of the enterprise), its top management personnel (management) and all other employees, which sufficiently and justifiably ensures achievement of enterprise goals [5, p. 365].

The International Standards for Quality Control, Auditing, Review, Other Assurance and Related Services (hereinafter referred to as ISA) provide a definition of internal control [6, p. 14–15], which meets COSO requirements.

Scientists define an internal control system as a set of organizational measures, procedures and methods used by the leaders of an economic entity to effectively and orderly manage business activities, ensure the safety of assets, correct, detect and prevent errors and misrepresentations of information, and also to prepare reliable financial information. They emphasize that effectively functioning control should have strategic orientation, result orientation, business relevance, flexibility, timeliness, simplicity and economy [7, p. 244]. Therefore, in order to figure out what and how to control, you need to find out what is not working as planned, and identify the source of the problems.

The direct solution of these issues leads to three main aspects of the management process: setting achievable goals; comparison of the results of economic activities with the current standard; evaluation of the results with subsequent adjustments to business operations or regulation of activities based on measurement results.

In practice, any control process consists of ten stages, namely: setting the standards that an organization plans to achieve in matters of internal control; the choice of time and place for collecting the necessary information on economic activities that are planned to be monitored and measured; monitoring the progress of the process or collecting samples; registration of collected information; measuring the results obtained, comparing them with expected indicators or existing standards; assessment of satisfaction with activity results; a report to the appropriate management level about detected deviations from established procedures or problems; implementation of changes in the relevant process or system; bringing change implementation processes to their logical conclusion and checking the effectiveness of the results; consideration and verification of performance standards as necessary [7, pp. 244–245].

The structure of the internal control system is based on the following components: reviews of results (reviews and analyses of actual results in comparison with budgets, forecasts and results for previous periods; linking different sets of data, operational or financial, with each other) with analysis of relationships and actions to investigate and correct shortcomings, comparison of internal data with external sources of information; review of functional indicators or performance indicators); information processing (two large groups of information system controls are application controls, which are used to process individual applications, and general IT controls, which are policies and practices that apply to many applications and ensure the effective functioning of application controls helping to ensure the further correct operation of information systems); physical measures (covering the physical protection of assets, including appropriate security measures such as secure facilities from access to assets and records, providing access to computer programs and data files, periodically counting and comparing with the amounts indicated in the control records); separation of duties (appointment of different persons responsible for issuing permits for transactions, registering transactions and ensuring the safety of assets. The segregation of duties is intended to reduce the possibility for any person to hold a position that enables him/her to commit and conceal errors or fraudulent acts in the ordinary course of his/her duties); assistance in ensuring the proper operation of the information system (general information technology controls: control procedures for information centers and networks; acquisition, change and maintenance of system software; access security; acquisition, development and maintenance of application systems; software change control procedures; control procedures limiting access to programs or data; control procedures over the introduction of new versions of the complete software; control procedures over system software that limit access, monitoring or use of system support programs that can change financial data or records without the possibility of their tracking during internal control) [7, pp. 244–245].

Improving the functioning of the internal control system, bringing it in line with the scale and nature of business transactions, will contribute to the improvement of business processes, which will achieve a positive effect in the form of increased profitability, saving resources, increasing confidence, strengthening reputation and related business success, and will also improve the level of enterprise management.

Part 2. The essence of risk in the internal control system of an enterprise

One of the main elements of the COSO model is the risk assessment process, which allows you to identify and, if necessary, eliminate the identified risks of a company's activities. Of great importance is the definition of a method for identifying risks, their assessment, management and elimination.

It should be noted that there is no normative, legally established definition of entrepreneurial risk in Ukraine. But the term «risk» is found in legislative and by-laws, resolutions and congresses of various ministries, departments and services of Ukraine, international organizations and unions. In particular, the regulations of the state and regional customs services, the Ministry of Labor and Social Policy, the National Bank of Ukraine, the Ministry of Health, the State Tax Service, the State Committee for Financial Services Markets and others, the Economic Code of Ukraine do not contain a definition of «entrepreneurial risk», although «entrepreneurship» itself is defined as risky [8].

It is quite obvious that risk is universal in the economic system. It is generally accepted that all types of risk associated with uncertainty should be borne by the owner of an enterprise. However, the desire to reduce risk has led to the creation of a number of economic entities that allow redistributing the burden of risk, but never, however, eliminating it completely.

Currently, there is no consensus on the definition of risk. The study of different views on the essence of risk and its impact on a company's activities allows us to conclude that the opinions of scientists were generated in different approaches to its interpretation and developed towards detailing certain types of risks. A large number of types of risks has led to the emergence of various interpretations of them.

Thus, economic risk is defined as an objective-subjective category associated with overcoming uncertainty and conflict in a situation of inevitable choice and reflecting the degree of achievement of the expected result, the impossibility of deviating from the set goals, taking into account the influence of controllable and uncontrollable factors [9].

Risk is interpreted as the probability of not achieving the desired result of the activity [10]; an action (deed) carried out under conditions of choice in the hope of a favorable outcome, when in case of failure there is a danger of being in a worse position than before the choice [11].

Lopatovsky, for a better understanding of the essence of the concept of «risk», presented his own definition, according to which «risk is an objective-subjective category, which, due to the influence of a number of factors, characterizes the multidimensional results of the activity of an economic entity or its inaction, moreover, in the presence of uncertainty in achieving one or another option» [12].

The most appropriate definition of risk is based on the fact that it is the probability of an adverse situation that can affect the positive result of management decisions and the result of an enterprise's economic activity as a whole.

Entrepreneurial risk can also be defined as the possibility of an undesirable event, as a result of which an enterprise suffers certain losses, a decrease in income received, and additional expenses. This event is both subjective and objective (natural disasters, accidents, illegal actions of contractors or government agencies, etc.). The possibility of its occurrence may cause the need for insurance to compensate for the damages caused in the future. Therefore, the presence of numerous factors of a political, economic and legal nature that can affect business activity does not allow predicting possible consequences and final results. In such a situation, the desire of the head of an enterprise to reduce entrepreneurial risks to a minimum is understandable. It should also be noted that risk is inherent in all aspects of a company's activity. When solving a risky situation, one of the properties of risk is manifested, such as alternativeness, when there is a choice of several possible solutions. If there is no choice, then this indicates the absence of risk: where there is no choice, there is no risk.

The essence of risk can be determined by the fact that it can arise from events of both an objective and subjective nature, which cannot be influenced. In this way, the definition of entrepreneurial risk can be formulated as the possibility of losses caused by the uncertainty that accompanies the activities of an enterprise.

To manage and control risks, it is necessary to classify them according to certain characteristics, which will allow them to be structured, make a choice, and determine the sequence of decisions based on classification characteristics. This will form the basis for the following risk assessment.

Thus, the following types of risks can be distinguished:

− Business risks – risks associated with the possibility of a deterioration in the overall financial condition of an enterprise, a decrease in the value of its capital; risks of insufficient information provision, risk of loss of liquidity.

− Organizational risks – risks caused by the errors of the management personnel of an enterprise; poorly developed regulations and rules of work; problems of the internal control system; improperly selected personnel; lack of qualified personnel; other risks related to the internal organization of an enterprise.

− Market risks – risks associated with the instability of the economic environment: increased competitive pressure; the risk of financial losses if there is a change in the market price or demand for goods; uncompetitive cost level;

entering the market of a new highly competitive product; inadequate level of marketing research.

− Financial risks – risks of improper banking services or bankruptcy of a settlement institution; currency change in international settlements; currency risk of the transfer.

− Credit risks – the risk that the counterparty will not fulfill its obligations on time; bankruptcy of a counterparty.

− Legal risks – risks of losses associated with changes in legislation or insufficient legal protection of an enterprise; risks of industrial injuries; the application of high financial sanctions by regulatory authorities to an enterprise; non-compliance with government regulations.

− Technological, man-made risks – risks of the consequences of inappropriately developed business processes, improper organization of production; risk of untimely technological support; risk of equipment failure; risk of man-made accidents.

− Natural, environmental risks – the risk of material losses due to natural disasters, fires and climatic conditions; the risk of damage to the environment.

− Reputational risk – the risk of a message appearing in the media, which can adversely affect the business reputation of an enterprise, cause negative events for the development of the enterprise's business, such as the loss of customers and suppliers; outflow of client resources, non-receipt of funds [7, pp. 192–193].

The presented classification clearly interprets the belonging of risks to a certain group, which allows for the unification of risk assessment, and also covers the types of risks as much as possible. This makes it possible to competently approach the problem of identifying risk formation factors.

According to the generally accepted definition of risk as a threat that some event or negative action will affect the ability of an enterprise to successfully achieve its goals or implement its strategies, risk can only be spoken of in the context of specific goals. Therefore, it is possible to classify risks according to the threat to specific targets.

However, in addition to the goals that a company sets for itself, it is also necessary to take into account the obligations that the company has to the state and investors. Therefore, it is necessary to take into account the relationship between the responsibilities and possible risks of an enterprise:

– Provision of reliable information: a company is obliged to provide information to interested parties (the state, investors, creditors) for them to make a decision on interaction with the company. The company is responsible for the accuracy and reliability of the information. An example of a risk is the accidental or intentional misrepresentation of information due to employees' unrestricted access to the company's information systems.

– Compliance with internal policies, plans, procedures, and external laws and regulations. Compliance with national laws is the responsibility of an enterprise. Also, an enterprise can establish its own internal standards, for example, a collective agreement or a code of business conduct. This includes legal and internal requirements for production safety. When an enterprise sets its own internal standards, it strives to meet them in order to maintain the consistency of production processes. An example of a risk for this type of goal is the non-compliance by a separate subdivision of the schedule for shipping semi-finished products to another, untimely submission of internal information, etc.

– Asset protection: investors (owners) provide the enterprise with its own assets in order to make a profit. The enterprise, for its part, is obliged to protect assets. Examples of risk for this type of purpose are theft of working capital, non-current assets, losses in the securities market due to unbalanced investments, etc.

– Economical and efficient use of resources: an enterprise's management is obliged in its current activities to create the necessary conditions for the organization of the work process, in which all types of enterprise resources, such as stocks, cash, fixed assets, and labor resources, will be used efficiently. An example of a risk for this type of purpose is damage to finished products or the expiration of their sale due to erroneous forecasting of sales volume. Such risks can lead to overuse of resources.

– Achieving the goals set for current activities and special programs: current plans for production, implementation, quality assurance of products and services, introduction of new software. An example of a risk for this type of purpose is an increase in the number of claims from buyers due to the acceptance of orders for goods that are not available, or the shipment of goods that are of inappropriate quality, the loss of a partner, etc. [7, pp. 150–151].

In order for an enterprise to function effectively, management must create a risk management system, which should consist of the following elements: identification of possible risks in accordance with each goal; description and qualitative characteristics of risks; risk measurement; risk management. After all, any enterprise is somehow exposed to various risks. The task of management personnel is to timely identify, assess risk and effectively allocate resources for its leveling. The main principles of risk management are the best risk management, that is, the ability to predict the conditions for their occurrence and the timely implementation of preventive measures, and an effective information system created at the enterprise should ensure timeliness and prerequisites for high-quality risk management; the risk management process should be ongoing; each employee must complete a training program to understand what potential risks to the enterprise are associated with his/her actions.

A simple definition of risk management is given in the COSO ERM standard. According to it, risk management is «the processes of identifying critical risks, assessing their impact, developing and implementing a comprehensive solution to manage them, combining strategy, personnel, processes and technology». Based on this definition, a risk management system is a system for collecting data on risks, analyzing them and making decisions that allow an enterprise to avoid random events that negatively affect the results of an enterprise or individual areas, as well as create conditions for the occurrence of events that improve these results. That is, each employee of the enterprise must be able to identify risks that may affect the performance of his/her unit, as well as know how to resist them and ensure stable operation.

Risk management activities consist of the following stages: identification, measurement, and control. Risk identification is a systematic identification and study of risks specific to the enterprise. It is necessary to establish and rank the hazards, risk factors, resources, etc. that may be affected. Risk measurement is a determination of the degree of its probability and the size of the potential loss. Damage is calculated, the size of which is expressed by the possible impact of the risk on resources. Often, a manager conducts a probabilistic assessment and ranks losses according to their degree of probability and size. This makes it possible to divide risks into three groups: damage that occurs frequently, is small in size and does not pose a serious threat; damage that occurs less often, but is more significant in size, its occurrence can cause serious financial difficulties; and catastrophic loss, characterized by low probability, but capable of jeopardizing the very existence of an enterprise. Such an assessment of risks allows deciding on the forms of control over them. Control comes in two forms, physical and financial. Physical control involves the use of various methods capable of reducing the probability of damage or its size. The application of physical control measures is associated with certain costs (wages, purchase of equipment). Financial risk control consists in the direct search for sources of compensation for possible losses in cash (reserving resources, risk insurance, etc.).

Risk assessment is the determination of the degree of risks by internal control subjects based on the criteria for the probability of risk occurrence and their impact on the ability of internal control subjects to perform tasks and functions to achieve the set goals [13]. Risk assessment forms the basis for determining how risks will be managed.

Scientists give the following definition of risk management: «a process that involves well-defined steps and tools that enable managers to clearly understand the risks facing their organization». It is emphasized that in the case of integrating risk management into various business processes, it is necessary to use different methods of risk assessment [14].

The search for other approaches to organizing the risk management system and creating an effective system of internal control of enterprises is connected with the fact that it is difficult to achieve complete elimination of risk. It can only be possible to manage risks and, by identifying areas of increased risk, prevent their occurrence and carry out systematic control.

To identify areas of increased risk, it is necessary to establish and analyze their possible causes and sources of occurrence. Business entities are exposed to various risks in their activities. They must be identified and evaluated using professional judgment to assess the factors affecting the magnitude of the risk.

The consequences of incorrect management decisions may affect the financial results of an enterprise or in future periods, when it is almost impossible to correct errors. Therefore, the wrong actions of managers are considered the main risk factor of a latent nature. The main task of the controller is to timely assess and provide the necessary information about the effectiveness of management at all levels, including the assessment of the effectiveness of economic processes. Therefore, identifying risks in the internal control system that affect the efficiency of business processes, assessing their impact and building an internal control system in such a way that it is able to reduce the impact of risks on the activities of an enterprise as a whole are of great importance.

Risks in the internal control system arise because unreliable, incomplete information about the controlled object is provided. This affects the amount of risk. Therefore, the risk in the internal control system can be defined as the possibility of an event that may affect the achievement of the goal, the probability of incorrect information for managers about the results of the inspection. Internal control risks can be divided into internal and external. Internal risks associated with the influence of factors caused by the management process are presented in Table 1.

It is appropriate to highlight the main external risks that may arise in the activities of enterprises: general economic (a sharp change in legislation in the field of taxation, hyperinflation, a change in regulations and legal relations, a sharp fluctuation in the prices of energy and materials, an increase in interest on loans), natural disasters (earthquake, fire, etc.) that may change the terms of performance of works and other force majeure circumstances that may be recognized as such on the basis of current legislation; the risk associated with the general economic and political situation in the country and the world, the increase in resource prices, the general market drop in them for all assets, changes in the interest rate, the drop in general market prices, inflation; the risk associated with the financial condition of a specific client, late payment by clients for services rendered; liquidity risk associated with a possible delay in the implementation of services on the market; sectoral risk associated with a change in the state of affairs in a separate economic sector; the risk of reducing resources, demand for products; financial risk associated with unprofitability and bankruptcy.

Table 1

The essence of internal risks of the internal control system

Internal risks	Essence of risk
Risk of incompatibility of an enterprise's organizational structure with the size and complexity of business processes	Improved economic processes (complication, expansion) at an enterprise with an unchanged organizational structure will contribute to slowing down the development of management
Risk of improper distribution of powers	Delegation of authority to implement control procedures in the field will not allow management to ensure effective control in the cost centers for the timely detection of errors and the formation of operational information about deviations
Risk of unreliability of accounting data and non-compliance with internal operational reporting schedules	Lack of a clear organization of the accounting system and operational reporting in the implementation of business processes is a source of unreliable information
Risk of inconsistency in the level of professional skills of employees performing control functions	The quality of control depends on the competence and professionalism of management personnel and specialists responsible for the implementation of control procedures; the ability to organize the accumulation of information about the current results of the functioning of economic processes in order to identify deviations and make management decisions
Risk of incorrect selection of means and timing for control procedures	The result of inspections depends on the methods used and the time of the inspection
Risk of not detecting errors on the controlled object	The correct execution of control procedures and the use of reliable information will prevent the detection of existing errors and deviations due to subjective and objective factors

Source: based on [15]

To reduce risks and protect activities, it is necessary to plan and create the necessary reserves and stocks of material, financial and time resources in a timely manner. These measures are especially important in the conditions of shortage of financial resources observed in Ukraine. Therefore, it is necessary to form the volume and structure of the necessary material reserves and reserves for unforeseen expenses, reserve funds to cover unforeseen expenses associated with the operation of equipment, changes in natural conditions, and the behavior of personnel.

Part 3. Risk assessment process to identify and eliminate the risks in the internal control system of the enterprise

The ability to predict and correctly assess risks is important when conducting control measures at an enterprise. The internal control system should be focused on identifying and assessing internal risks and the factors that determine them, since the possibilities of control over them are higher than over external ones.

The use of the software may affect the risk of deviations and errors. Among them, one can highlight technical risks (unsatisfactory operation of controls, use of unlicensed software, lack of maintenance); risks associated with the organization of accounting and control (the occurrence of errors due to improper training of employees to work with the data processing system, organization of control, lack of separation of employees' responsibilities and duties); risks associated with the data processing system (the occurrence of errors in the development of the system and when it is used for other purposes); risks associated with the professionalism of internal controllers (the occurrence of errors due to the incorrect construction of tests, incorrect assessment of the data processing system) [15, p. 358].

Therefore, the construction of a reliable internal control system should contribute to increasing the efficiency of management and protecting shareholder interests. Internal controllers can professionally assess its effectiveness and recommend improvement measures.

Internal control entities take and maintain effective internal control measures to ensure an acceptable level of risk. Their task is to continuously manage risks and prevent them by identifying areas of increased risk and systematic controls.

The internal control system can provide information that will allow predicting possible risks that can negatively affect an enterprise's further activities. It should be focused on the identification and assessment of internal risks in terms of their impact and probability of occurrence. There are no specially developed requirements, so the unit that performs control actions at an enterprise independently conducts such an assessment, taking into account needs and its own experience. For this, criteria for assessing risks by spheres of influence on a company's activities are being developed. In terms of the impact on the ability of internal control entities to achieve operational goals, risks can be assessed according to the criteria presented in Table 2.

According to the probability of occurrence, risks can be assessed according to the criteria presented in Table 3.

Table 2

Internal control risk assessment criteria

Influence level	Essence
Low (1)	Limited or minimal reduction in capacity that prevents the continuation of tasks in one line of business. Quick recovery at work
Average (2)	Significant reduction (loss) of capacity that prevents the continuation of tasks in one or several areas of activity. Slow recovery at work
High (3)	Significant decrease (loss) of legal capacity that prevents the continuation of tasks in two or more areas of activity. Slow recovery at work
Very high (4)	Not being able to continue with tasks. Failure in all areas of activity. Significant loss of capacity. Slow recovery at work

Source: based on [13]

Table 3

Risk probability criteria

Probability criterion	Probability level	Probability, %
Very low	Rarely (almost impossible)	0–20
Small (unlikely)	Distant	21–40
Average	A possibility of a rare occurrence in the future	41–60
Possible	Within 1-2 years	61–80
Frequent (expected)	Happening or expected	81–100

Source: based on [13]

Risks are assessed based on the probability of their occurrence and impact on the ability of internal control entities to achieve the set operational goals in accordance with the risk assessment matrix presented in Table 4.

Table 4

Risk assessment matrix

Level (point)			Probability				
			Rarely	**Unlikely**	**Average**	**Maybe**	**Often**
			1	2	3	4	5
Influence	Low	1	1	2	3	4	5
	Average	2	2	4	6	8	10
	High	3	3	6	9	12	15
	Very high	4	4	8	12	16	20

Source: based on [13]

Risks that have the highest probability and level of impact on the ability to achieve the set operational goals are significant. Accordingly, the least significant are the risks that have a lower probability and a lower level of such an impact. The most attention should be paid to the risks with the highest likelihood and level of impact.

Reducing risk means taking action that will reduce or eliminate the likelihood of risks and their impact.

In the process of implementing the internal control system, risk probability assessment can have a large error. But in the future, when it is already implemented at an enterprise and a large amount of data on errors that occur will be collected, the composition of risks and their significance can be assessed with high accuracy.

It is also necessary to define risk assessment procedures, that is, audit procedures that are performed to gain an understanding of an enterprise's activities and its environment, including the enterprise's internal control, the identification and assessment of the risks of material misstatement due to fraud or error at the level of financial statements and assertions. However, risk assessment procedures alone do not provide acceptable and sufficient audit evidence on which to base the auditor's opinion. Gaining an understanding of the business and its environment, including internal controls, is a dynamic and ongoing process of gathering, analyzing, and updating information throughout the audit. This understanding forms a system of criteria within which the auditor can plan the audit and make professional judgments during the entire audit, in particular, when assessing the risks of material misstatement of financial statements; consideration of the acceptability of selecting and applying accounting policies and the adequacy of information disclosure in financial statements; identification of areas that may require special consideration by the auditor (transactions with related parties, acceptability of management's use of the assumption of operation continuity; formulation of expectations for the use in performing analytical procedures); taking actions in response to assessed risks of material misstatement; assessing the sufficiency and acceptability of audit evidence obtained, such as the acceptability of assumptions, oral and written assurances of management personnel. Information obtained as a result of performing risk assessment procedures and related measures can be used by the auditor as audit evidence to support assessments of the risks of material misstatement. Also, the auditor can obtain audit evidence about classes of transactions, account balances or disclosures and related assertions, and about the operating effectiveness of controls, even if such procedures are not separately planned as substantive procedures or tests of controls. The auditor may choose to perform substantive procedures or tests of controls at the same time as risk assessment procedures because it is effective. The auditor uses professional judgment to determine the degree of understanding required.

Therefore, it is necessary to highlight the Risk Assessment Procedures at an enterprise, which include the following:

1. Submission of inquiries to management personnel and other employees of an enterprise who may have information that may help identify risks of material misstatement due to error or fraud. Much of the information that the auditor obtains when making inquiries is provided by management personnel and those responsible for financial reporting. However, the auditor can obtain information when identifying risks of material misstatement by making inquiries of other employees of the enterprise with different levels of authority. These may be persons with higher authority, they can help the auditor understand the environment in which the financial statements are prepared; staff of the internal control unit, who will provide information on internal control procedures that were performed during the year regarding the effectiveness and structure of the company's internal control; employees who initiate, process or record complex or unusual transactions can help evaluate the acceptability of choosing and applying certain accounting policies; the company's internal legal consultant can provide information on compliance with laws and regulations, court cases, knowledge of fraud that may affect the enterprise, arrangements with business partners and the meaning of contractual terms; marketing staff can provide information on changes in the company's marketing strategies, contractual arrangements with its customers, and implementation trends.

2. Analytical procedures. Performed as risk assessment procedures, they can identify aspects of the company's operations that the auditor was unaware of. They can help in assessing the risks of material misstatement in providing a basis for developing and implementing actions in response to those assessed risks. Analytical procedures performed as risk assessment procedures include financial and non-financial information. They help identify the existence of unusual transactions or events and amounts that may require audit. Identified unexpected or unusual relationships can assist the auditor in identifying risks of material misstatement, especially risks of material misstatement due to fraud.

3. Observation and verification. They can accompany submission of requests to management personnel and other persons, as well as provide information about the enterprise and its environment. Examples of such audit procedures may include observation or verification of various operations of the enterprise; documents (business plans and strategies), instructions and internal control records; reports prepared by the management (quarterly reports of the management staff and interim financial statements) and those entrusted with the highest powers (minutes of the meetings of the board); production and administrative premises of the enterprise.

4. Analysis of information obtained in previous periods. When the auditor intends to use information obtained in the course of his past work with the entity

and in the course of audit procedures in previous audits, he should determine whether there have been changes since the previous audit that could affect the relevance of such information for the current audit. The previous experience of the auditor's work with an enterprise and the audit procedures that were performed during previous audits can provide the auditor with information about previous distortions and their timely correction; the nature of the enterprise's activity and its environment, as well as its internal control (including deficiencies in internal control); significant changes that the entity or its operations have undergone since the previous financial period that may help the auditor obtain a sufficient understanding of the entity to identify and assess the risks of material misstatement.

5. Discussion with engagement team members. The engagement partner and other lead members of the audit team should discuss the sensitivity of the reporting entity's financial reporting framework to the entity's facts and circumstances. The engagement partner must determine what matters to communicate to members of the engagement team who are not participating in the discussion. Discussing with members of the engagement team on the project the sensitivity of the entity's financial statements to material misstatement, which will allow more experienced members of the engagement team, including the engagement partner, to share their opinion based on their knowledge of the entity; will enable members of the engagement audit team to share information about the business risks faced by the entity and how and at what stage the financial statements may be susceptible to material misstatement due to error or fraud; helps members of the audit team better understand the possibility of material misstatement of the financial statements in certain areas assigned to them and understand how the results of the audit procedures they perform may affect other aspects of the audit, including decisions about the nature, timing and scope of further audit procedures; provides a basis for communicating and sharing new information obtained throughout the audit that may affect the assessment of the risks of material misstatement or the audit procedures performed to address such risks among the members of the engagement team.

6. Other procedures. The auditor is not required to perform all of these procedures with respect to every aspect of understanding the entity. Other procedures may be performed and the information obtained from them may be useful in identifying risks of material misstatement. Examples of such procedures include checking information obtained from external sources such as trade and economic journals, analytical reports, banks or rating agencies; or from regulatory or financial publications; making inquiries to the external legal advisor or valuation experts the company has used [7, pp. 211–214].

Also, the auditor should gain an understanding of whether the enterprise has a process for identifying business risks that are relevant for financial reporting purposes; risk significance assessments; estimates of the probability of their occurrence; making decisions about the mechanisms for considering these risks. The enterprise risk assessment process provides a basis for management to determine the risks that should be managed. When appropriate to the circumstances, including the size and complexity of the entity and its nature, this process may assist the auditor in identifying risks of material misstatement. If the enterprise has established such a process, then the auditor should gain an understanding of such a process and its results. If the auditor identifies risks of material misstatement that management failed to identify, then the auditor should assess whether any material risk exists that the auditor believes should have been identified by the entity's risk assessment process. If such a risk exists, the auditor should understand why the process was unable to identify it and evaluate whether the process might be acceptable in the circumstances, or determine whether there are significant deficiencies in the internal control of the entity's risk assessment process.

In case the enterprise does not establish such a process, or the process is not systematic, the auditor should discuss the business risks with management personnel and find out how they have been taken into account. The auditor should evaluate whether the absence of a documented risk assessment process is acceptable in such circumstances, or determine whether this is a significant internal control weakness [7, p. 214].

To increase the reliability of accounting and reporting information, it is necessary to timely forecast the risks of displaying business operations, identify weak points in the process of managing the enterprise, diagnose manipulations with reporting, which will be possible only with the creation of an effective internal control system, which will be able to identify various types of risks, ensure the successful development and stability of enterprises in a competitive environment, and will also allow timely identification and minimization of risks in the management of economic activities.

Thus, the developed organizational and methodological measures for the functioning of internal control at an enterprise are aimed at creating an effective and efficient internal control system, which, if implemented, will increase the efficiency of the management system as a whole.

Conclusions

Based on the analysis of current practice, it can be concluded that in order to identify risks in an enterprise, a modernized internal control system is needed today, which can identify various types of risks, ensure stability and successful development of enterprises in a competitive environment, and also allow timely identification and minimization of risks in the management of financial and economic activities.

Trends in the development of regulatory and legal support of the internal control system are in the need for a systematic modernization of existing regulatory and legal documents relating to the internal control system. It is necessary to expand the list of internal control objects and strengthen the requirements for its implementation, as well as clarify the content of internal control. Currently, the role of the internal control service is undergoing significant changes, namely, it not only evaluates the control procedures of a company's activities, but also contributes to its management in the field of risk management.

In the process of implementing the internal control system, the assessment of possible risks may have a large error. However, in the future, by introducing an internal control system and accumulating a sufficient amount of data on the errors that have occurred, the composition of risks and their significance can be assessed with high accuracy To increase the reliability of accounting and reporting information, it is necessary to forecast the risks of displaying economic transactions, diagnose manipulations with reporting, identify potential weaknesses in the process of managing the organization, which will become possible when creating an effective internal control system.

Achieving the goals of the existence and development of any enterprise is related to the effective implementation of the risk management process. The more effectively it is carried out, the more stable the enterprise becomes and the better it resists internal and external challenges. The development and implementation of an effective risk management system will enable a business entity to function stably on the market, gain competitive advantages, despite the significant influence of political, economic and social factors.

An important direction in the context of risk management is also the further study of the criteria for assessing the levels of damage and the likelihood of risk events occurring in various areas of an enterprise and specific economic processes.

References:

1. Sharovska, T.S. (2010). Organizatsiino-metodychni zasady vnutrishnogo kontrolu realnyh investytsii [Organizational and methodological principles of internal control of real investments]. Candidate's thesis. Odesa, 224 p. [in Ukrainian]
2. Zakon Ukrainy Pro bukhgalterskii oblik ta finansovu zvitnist v Ukraini. 1999, № 40, st. 365. [Law of Ukraine "On Accounting and Financial Reporting in Ukraine"]. Available at: https://zakon.rada.gov.ua/laws/show/996-14. [in Ukrainian]
3. Components of an internal control system. Available at: https: //www.accountingtools.com/articles/components-of-an-internal-control-system.htm [in English]
4. Internal Control – Integrated Framework: Executive Summary. Committee of Sponsoring Organizations of the Tredway Commission, 2013. 12 p. [in English]
5. Kamenska, T.O. (2010). Vnutrishnii audit: suchasnyi pogliad [Internal audit: a modern look]. Kyiv: DP «Inform.-analit. agenstvo», 449 p. [in Ukrainian]

6. Mizhnarodni standarti kontrolu yakosti, audytu, ogliadu, inshogo nadania vpevnenosti ta suputnih poslug (2017) [International standards for quality control, audit, review, other assurance and related services]. Part 1, 1142 p. Available at: https://www.apu.net.ua/attachments/article/1151/2017_часть1.pdf. [in Ukrainian]

7. Kamenska, T.O. (2015). Vnutrishnii control I audit v upravlini [Internal control and audit in management]. Kyiv: DP «Inform.-analit. agenstvo», 375 p. [in Ukrainian]

8. Semenova, K.D., Tarasova, K.I. (2017). Ryzyky diialnosti promyslovyh pidpryemstv : integralne otsiniuvania: monografiia [Risks of activity of industrial enterprises: integral estimation]. Odesa: FOP Guliaeva V.M. », 234 p. [in Ukrainian]

9. Vitlinskyi, V.V., Nakonechnyi, S.I. (1996). Ryzyk u menedzhmenti [Risk in management]. Kyiv: Borisfen-M, 336 p. [in Ukrainian]

10. Goncharov, I.V. (2002). Ryzyk ta pryiniatia upravlinskyh rishen [Risk and management decision making]. Harkiv: NTU HPI, 16 p. [in Ukrainian]

11. Ivchenko, I.Yu. (2004). Ekonomichni ryzyky [Economic risks]. Kyiv: Tsentr navchalnoi literatury, 304 p. [in Ukrainian]

12. Lopatovskiy, V.G. (2008). Upravlinnia ryzykamy pidpryemstv za umov nestabilnogo zovnishnogo seredovyshcha [Enterprise risk management in an unstable environment]. Extended abstract of candidate’s thesis. Kyiv, 21 p. [in Ukrainian]

13. Kryvoviaziuk, I.V. (2018). Ryzyk-menedzhment logistychnoi systemy mashino-budivnyh pidpryemstv: monografiia [Risk management of logistic system of machine-building enterprises]. Available at: http://er.nau.edu.ua:8080/handle/NAU/33937 [in Ukrainian]

14. Duka, A.P. (2017). Kartografuvania ruzykiv u systemi integrovanogo ryzyk-menedzhmentu organizatsii [Risk mapping in an organization’s integrated risk management system]. *Efektyvna ekonomika*, vol. 10. Available at: http://www.economy.nayka.com.ua/?op=1&z=5794 [in Ukrainian]

15. Petrenko, S.M. (2013). Vnutrishnii control: problemy informatsiinogo, organizatsiinogo ta metodologichnogo rozvytku: monografiia [Internal control: problems of information, organizational and methodological development]. Donetsk: Svit knygy, 503 p. [in Ukrainian]