CHAPTER 3
MODERN MANAGEMENT TECHNOLOGIES

RISK MANAGEMENT AND COMPLIANCE CONTROL AT ENTERPRISES: THEORETICAL BASIS

Yulia Ilkiv[1]

[1]*Ph.D. Researcher, Lviv State University of Internal Affairs, Lviv, Ukraine. e-mail: yulya_ilkiv@ukr.net*

Citation:
Ilkiv, Y. (2020). Risk management and compliance control at enterprises: theoretical basis. *Economics, Finance and Management Review*, (4), 71–77. https://doi.org/10.36690/2674-5208-2020-4-71

Received: November 15, 2020
Approved: December 03, 2020
Published: December 07, 2020

Abstract. *The article provides a theoretical analysis of the organization of security activities in enterprises, which is proposed to mean activities to ensure the most efficient use of available resources to protect their interests from the effects of internal and external threats, as well as adaptation to existing conditions with minimal losses. Theoretical bases of essence of safety activity of the enterprises as bases for maintenance of effective functioning of the enterprises in the conditions of competition are substantiated. It is proposed to position security activities as a management technology in the enterprise, which contributes to the achievement of strategy and a high level of competitiveness in the market. Currently, businesses face an increasing number of risks and threats that arise from a significant level of uncertainty in the environment, as well as illegal intentional or unintentional actions of employees. The impact of such threats has significant negative consequences on the results of enterprises, their image, market position and so on. Therefore, special attention is paid to the details of the process of risk management and compliance control in order to achieve a high level of economic security of the enterprise. Using methods of analysis, scientific abstraction, formal logic and logical generalization to determine the essence of the main categories in the field of security activities of enterprises and risk management. A comparison of risk management and a comprehensive enterprise risk management system is made. The advantages of using a comprehensive risk management system are analyzed. The ERM concept is characterized as an approach to enterprise management that integrates strategic planning, operations management and internal control and is based on risk accounting. Comparisons were made and differences were established between compliance control and internal audit at the enterprise.*

Keywords: *risks, threats, enterprise management, security activities, economic security of the enterprise, risk management, compliance control.*

JEL Classification J11, J21, M21, M5

Formulas: 0; fig.: 1; tabl.: 1; bibl.: 17

Introduction. Security activities are activities to ensure the most efficient use of available resources in order to protect their own interests from the impact of threats to the internal and external environment, as well as adaptation to existing conditions with minimal losses. We consider it expedient to use such wording, because it allows you to reflect the security activities in terms of management technology, rather than a set of individual actions.

The author's approach to the formation of a model of security activities of the enterprise is presented in Fig. 1.

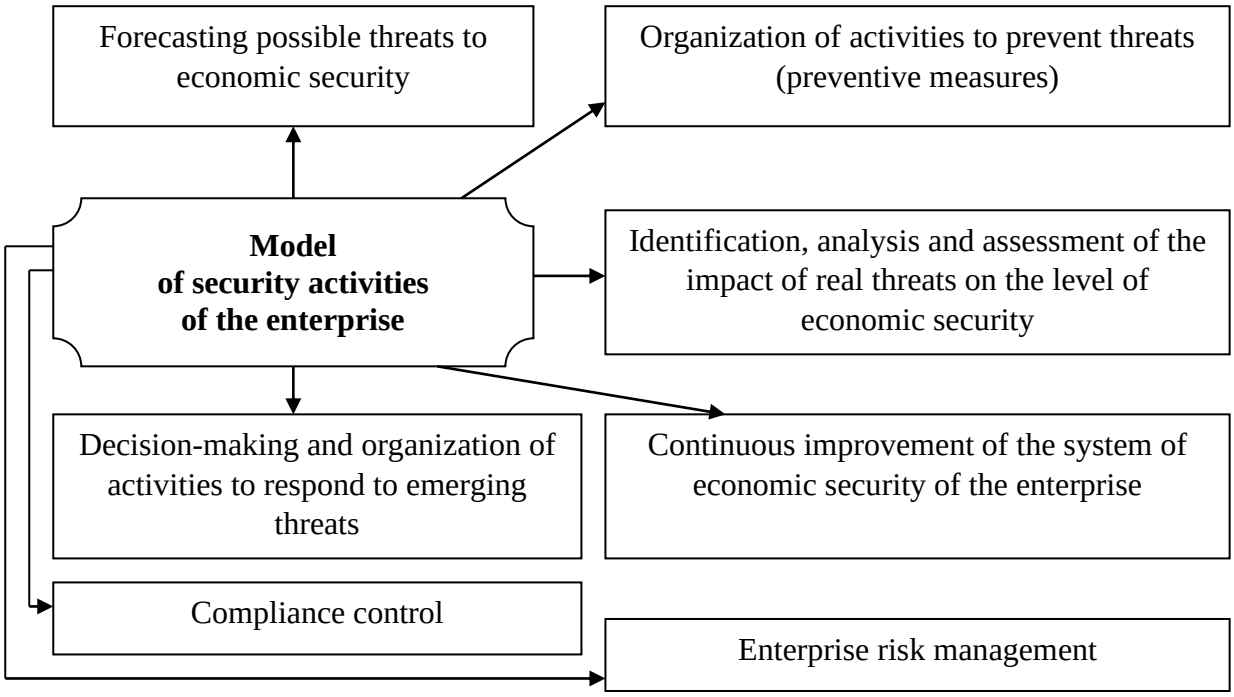

Figure 1. Model of security activities of the enterprise

Source: author's development based on [1, 2]

Analyzing fig. 1. we see that 6 functions of security activity out of 7 belong to the detection, prevention, forecasting of impact, minimization of the consequences of destabilizing factors, which include risks, threats and dangers.

In [3], Baker Tilly expert Roman Grinevsky notes that "if a company does not know and manage its risks, it knows nothing about its future." Therefore, the priority for each company is to develop its own, adapted to the specifics of the activity, the process of identifying risks and threats, which will be the first step to effectively manage them to help achieve the goal of the activity.

Therefore, special attention should be paid to the study of the features of the process of risk and threat management to increase the level of economic security of enterprises.

Literature review. To understand the essence of risks, it is advisable to agree with T.Yu. Feofilova, who notes that negative influences are a set of all influences that can damage the economic system of a certain level with varying degrees of probability [4]. The scientist believes that the basis of the grouping of negative impacts is the probability of the moment when the economy will be caused real damage. She further clarifies that “if we quantify the possibility of damage from 0 to 1, the risk is in the range from 0.3 to 0.5, the threat - from 0.7 to 0.9. The range from 0.5 to 0.7 will be a risk that creates a threat, ie such an impact has no clear "intention" to cause harm, but this trend is clearly visible "[4]. It is no less important that T.Yu. Feofilova gives the concept of negative impact assessment: “negative impact assessment is a process by which the compliance of the expected results is determined - damage to the economic system, specific forms and intensity of the impact on the economic security of negative impacts. Algorithm for assessing negative impacts provides:

"First, the identification of negative impacts;

secondly, determining changes in the strength of the impact of negative impacts on economic security in the period;

third, identifying possible changes in the economic system adequate to the effects of negative influences "[4].

There is a belief among scientists [5-7] that risks are sources of threats; so N.N. Poida-Nosyk [8] believes that this statement is true for the financial security sector of businesses, because it is the risks that generate the potential for harm to the business entity.

Correlates the concept of "risk" and "threat" K. Goryacheva [9], who formulated the following statements:

- risk in relation to the threat - the primary category, while the threat - the secondary and arises from the risk;

- risk - a category of general, non-specific, it is something that has not yet been identified, a threat - is something that has been identified, ie a specific category;

- risk is always present when there is financial activity, while the threat - no, it may or may not be, and arises only under certain conditions;

- the relationship between risk levels and financial security is inverse: the higher the level of financial risk, the lower the level of financial security and vice versa.

Aims. Investigate the features of risk management and compliance control in order to identify areas of security to improve the economic security of enterprises.

Methods. The main research methods were scientific abstraction, formal logic and logical generalization to determine the essence of the main categories in the field of security activities of enterprises and risk management.

Results. Identifying or identifying risks is the first and most important step in the risk management process. If an error was made in identifying a certain risk, ie the risk was identified inaccurately, incorrectly or was not taken into account at all, then other steps in risk management will not be implemented in relation to this risk. This means that it will not be possible to analyze this risk and minimize losses from it.

In order to manage risks, an organization must know what risks it may face in its activities and be able to assess them. Identifying risks is the first step in creating an organization's risk profile. There is no single correct option for compiling a risk profile of the organization, but the availability and application of this document in the enterprise is crucial for effective risk management. Risk identification can be divided into two separate stages:

• primary risk identification - for organizations that have not previously identified their risks in a structured way, as well as for new organizations, a new project or activity within the organization;

• continuous identification of risks, which is necessary to identify new risks, previously forgotten, as well as changes in existing risks, or risks that existed before, but now become relevant to the organization [10].

The most common methods of risk identification are: brainstorming, Delphi method, SWOT-analysis, checklists, the method of building flowcharts.

After identifying the risks, an important step is to assess the level of their impact. The level of impact can be determined both by quantitative methods (expert evaluation, statistical methods, analogy methods, etc.) and qualitative methods, the peculiarity of which is manifested in identifying sources and causes of risks, identifying types of risks and areas of influence, analysis of potential negative impacts or practical benefits, etc. . The most common method of qualitative risk assessment is the method of expert assessments.

The risk management process in the enterprise is multicomponent. Until recently, leading researchers and professional managers used risk management to identify and overcome the effects of risks and threats to the enterprise. But this approach loses its position in favor of a comprehensive system of enterprise risk management (ERM - Enterprise risk management). The differences between risk management and integrated enterprise risk management system (ERM) are given in table. 1.

Table 1. Differences between risk management and integrated enterprise risk management system (ERM)

Risk management	Integrated enterprise risk management system (ERM)
1. Risk management by individual fragments - each department at the enterprise guided by its own functions carries out risk management. 2. Risk management by episodes - risk management occurs when there is an awareness of its need. 3. Limited risk management - is carried out in relation to financial risks and risks to be insured	1. Integrated risk management - the process of risk management is organized and coordinated by senior management, the responsibilities of each employee include the functions of risk management. 2. The risk management process is continuous. 3. Extended risk management - all risks in the process of enterprise activity are taken into account.

Source: author's development based on [11]

An integrated enterprise risk management system is a concept that contains the methods and processes used by organizations to manage the risks and opportunities associated with achieving their goals. ERM forms the basis of risk management, in particular, determines the ability to identify events or circumstances that can affect the achievement of enterprise goals, assess the likelihood of adverse effects or benefits, form a response strategy, as well as to monitor the level of efficiency. This work protects and creates value for stakeholders, including owners, employees, customers, regulators and society at large. The concept of ERM can also be described as a risk-based approach to enterprise management that integrates strategic planning, operations management and internal control [12].

ERM focuses on risk management for the company as a whole. At the same time, attention is paid to all risks that may arise in the activities of the enterprise at different stages, regardless of the place of origin, features and control. The advantages of using ERM are the ability to:

- to build a single risk management strategy for the company taking into account the level of riskiness of the company's managers;
- optimize the level of subjectivity of decisions;

- to form a unified methodology for assessing the level of risk impact;
- set thresholds for assessing the level of risk impact;
- to form an integrated risk indicator based on the composition of the impact of all identified and assessed risks;
- increase the level of confidence in the stability of the level of activity of top managers and owners;
- improve the quality of corporate governance and the quality of decisions;
- increase the efficiency of internal control and internal audit systems;
- will lead to an increase or stabilization of the value of shares due to more positive expectations of investors;
- ensure compliance with the requirements of regulators when placing securities [11].

Consider in more detail the process of compliance control in enterprises from the standpoint of the structural element of security activities.

International Compliance Association compliance is ensuring compliance with established requirements and standards. Compliance is interpreted by domestic scholars from different positions, so professors Pererva PG, Kotsyski D. believe that the ideology of "compliance" calls for compliance with internal policies and procedures of the company and is implemented by creating conditions in which persons representing the organization will act in accordance with high professional and ethical standards [13].

The primary purpose of compliance control is to minimize an entity’s risks to events that could cause not only financial loss but also loss of trust by supervisors, shareholders, investors, and customers.

In today's business world, the leading place in the field of risk management belongs to risks that are difficult to quantify, they include, in particular:

- operational risk,
- risk of loss of image and business reputation,
- risks caused by political and legal changes in the country or region,
- risk of force majeure,
- risk of conflict of interest,
- the risk of activities related to the prevention of participation, which contradicts the requirements of current legislation (financing of illegal activities, including terrorism, money laundering through securities transactions, money laundering for the purpose of introducing them into financial traffic, the use of prohibited practices doing business) [14].

In summary, you can group compliance risks into the following categories:

- reputational: publication of negative information about the organization or its employees, shareholders, members of management bodies, affiliates in the media;
- legal: non-compliance with the law, which is the reason for prosecution by supervisory authorities;
- operational: violation of internal rules and documents of the organization, which caused losses; non-compliance by affiliated persons and shareholders with the legislation, constituent and internal documents of the economic entity.

Important for the effective operation of the enterprise is the implementation of corporate compliance. Corporate compliance is a set of procedures (processes) in the company that regulate the behavior of staff in compliance with legal and ethical standards [15]. These procedures include:

1) combating corruption, money laundering and terrorist financing;

2) regulation of the process of accepting and giving gifts, invitations to events;

3) notification of violation of ethical standards;

4) regulation of conflicts of interest;

5) non-disclosure of data related to confidential information in the organization, as well as the organization of storage and compliance with certain standards in the processing of personal data, etc. [15];

6) counteraction to violation of the ecological legislation;

7) regulation of the processes of safety and minimization of injuries in the workplace;

8) compliance with the principles of corporate social responsibility;

9) compliance with the proper quality of products, provision of services;

10) prevention of operational risks, etc.

When distributing compliance control functions between different departments, it is necessary to provide a mechanism for cooperation between departments and managers of the compliance control function as a whole. The distribution of compliance functions between services can be recommended as follows:

- the function of internal audit is an independent audit of the internal control system;

- the function of the compliance control structure (or enterprise security service) is to organize the current control of compliance risk management procedures.

Another important difference is the time aspect of the object of control and the compliance of the unit. The role of compliance control as an element of risk management is to coordinate compliance risk control at the level of individual functional units and aggregate the results of compliance control in the assessment of aggregate risk. Compliance monitoring works in a precautionary mode, while auditors analyze what has happened and whether it meets the requirements at the moment. It is worth emphasizing that, despite the similar purpose of internal control and compliance control, they can not be performed by the same unit [16].

Discussion. It can be noted that many Ukrainian companies consider internal control and compliance not too important for successful business, so they do not want to spend time or money on compliance control. At the same time, Western firms in practice demonstrate that competent compliance control is able to generate added value. Control in the field of compliance is customer loyalty, interest and trust of shareholders, trust of society as a whole. When entering global capital markets, the presence of a compliance function in the organization is viewed in a positive light by both international regulators and investment financial institutions, and institutional investors. For potential investors, effective compliance control increases the level of investment attractiveness of the organization. Moreover, the current legislation of the

United States and the United Kingdom requires foreign partners to have an effective compliance unit within the organization.

Conclusion. Thus, the theoretical foundations of the essence of security activities of enterprises as a basis for ensuring the effective functioning of business in a highly competitive environment. It is proposed to position security activities as a management technology in the enterprise, which contributes to the achievement of strategy and a high level of competitiveness in the market.

It is determined that the basis of security activities should be upavlin measures to identify, prevent, minimize the impact, eliminate the consequences of risks and threats to the activities of enterprises.

Particular attention is paid to the benefits of using a comprehensive risk management system and compliance control in the process of enterprise activity.

References:

1. Kopytko, M.I, Prikhodko, S.M. (2018), "The specifics of the use of management technologies in the process of private security structures". *Scientific notes of KROK University*. University of Economics and Law "KROK". Issue. 49. pp. 74-77 [in Ukrainian].
2. Franchuk, V.I, Prigunov, P.Ya., Melnyk, S.I. (2017), "Security activities: a systematic approach". *Scientific Bulletin of Lviv State University of Internal Affairs*. № 1. pp. 154–163 [in Ukrainian].
3. Grinevsky, R. Do not let problems drift: 4 reasons to manage risks URL: https://bakertilly.ua/news/id47296
4. Feofilova, T.Yu. (2010), Risks and threats to economic security: identification, assessment and counteraction to influence. *Business, Management and Law*. №1. pp. 19-23 [in Russian].
5. Mihus, I., Koval, Ya., Laptev, S., Bala, O., Kopytko, M. (2020), "Monitoring in the system of state anti-crisis management of economic security of the banking institution of Ukraine". *Business: Theory and Practice*/ 21(2), pp. 804–812. https://doi.org/10.3846/btp.2020.12985
6. Kopytko, M.I, Ilkiv, Yu.I. (2020), "Management of security activities of innovative enterprises". *Socio-legal studies*. Issue. 3 (9). pp. 162-172. https://doi.org/10.32518/2617-4162-2020-3-162-172 [in Ukrainian].
7. Laptev, S.M., Alkema, V.G., Sidak, V.S., Kopytko, M.I. (2017) "*Complex support of economic security of enterprises*" Kyiv: University of Economics and Law" KROK. 508 p. [in Ukrainian].
8. Poida-Nosyk, N.N. Risks and sources of threats to the financial security of joint stock companies in modern conditions URL: www.teologia.org.ua/20110920172/statti/dokladi/riziki-i-djerela-zagroz-finansoviie-bezpeci-akcionernix-tovaristv-u-suchasnix-umovax-1.html.
9. Goryacheva, K.S (2006), "*The mechanism of management of financial safety of the enterprise*". Kyiv: Kyiv National University of Technology and Design. 17 p. [in Ukrainian].
10. Sizyakov, E.S Modern methods of risk identification URL: https://novainfo.ru/article/4019
11. Organization of the risk management system at the enterprise URL: https://slide-share.ru/organizaciya-sistemi-upravleniya-riskom-na-predpriyatii-147295
12. ERM. URL: https://www.cfo-russia.ru/glossariy/detail.php?ELEMENT_ID=1929
13. Break, P.G., Kotsiski. D., Vereshne Shomoshi M., Kobeleva, T.A. (2019), *"Compliance program of an industrial enterprise"*. Kharkiv-Miskolc: NTU "KhPI". 689 p. [in Ukrainian].
14. Kovalchuk, O. (2010), "The concept of compliance-control system and features of compliance risk in Ukrainian banks". *Youth and the market*. №7 - 8 (66 - 67). pp. 153-157. [in Ukrainian].
15. Ermakova, N.A, Akhunyanov,a Ch.F. (2014), "Compliance control in the corporation's internal control system". *Accounting problems*. 3 (297). pp. 2-10. [in Ukrainian].
16. Compliance control URL: http://www.iccwbo.ru/blog/2016/komplaens-kontrol-chto-takoe-i-dlya-chego-nuzhen/.
17. Herasymenko, O. (2020). Theoretical and methodological aspects of integration rational approach to business process management. *Economics, Finance and Management Review*, (1), 71-79. https://doi.org/10.36690/2674-5208-2020-1-71-79