Security management in economic organizations

Ivanka Nikolova [*] [1] [A]

*Corresponding author: [1] PhD student, e-mail: nikolovav20@gmail.com, ORCID: 0000-0002-7605-9354

[A] Higher School of Security and Economics, Plovdiv, Bulgaria

Received: November 2, 2022 | Revised: December 05, 2022 | Accepted: December 30, 2022

DOI: 10.5281/zenodo.7401557

Abstract

The selected topic examines security management as part of integrated management systems. The security policy, approaches and methods, management environment, and objectives pursued. The relationship between components and objectives and the standards that accompany them.

Key words: security management, security policy, standards.

Introduction

Modern security management in an organization that develops a business for private benefit and whose ultimate goal is to achieve profit and legitimate business interests begins with the responsibility and commitment of management. Security management is a part of integrated management systems, responsibility and commitment include one main document – the security policy. A company's top management should state what its security priorities are and what it is committed to following them. The security policy must be clear and understandable for the entire company and be known and followed by all employees. The organization's security management is based on this document and such a security system should be built that corresponds to the interests of the company.

Results and Discussion

Security management in economic organizations

When it comes to security management and the approaches we will follow, the resources that logical management should have can be presented in the following order:

- Employees possessing the necessary knowledge, skills and qualifications
- Facilities to meet the needs of the company and the assets to be protected
- Technologies to protect assets and prevent risks
- An internal organization to assist the security department
- Information
- Budget

In 1992 in the USA, the concept of increasing internal control in organizations is created **"Internal control – Integrated Frame Work",** developed under the guidance of the **Committee of Sponsoring Organizations of the Treadway Commission (COSO).** Originally established in 1985, COSO is a joint initiative of five private sector organizations and is dedicated to providing thought leadership through the development of internal control frameworks and guidelines for enterprise risk management (ERM) and fraud prevention. The integrated framework defines internal control for the first time. Its concept and methodology based on internal control can be used in any organization or in the private sector.

The Integrated Framework methodology defines internal control as "a comprehensive, complex process, carried out by management and other personnel of the organization, which is designed to provide a reasonable level of assurance regarding the objectives related to the performance of proper, economical, efficient and effective activities and operations, fulfillment of commitments regarding accountability and reliability of financial and non-financial information,

compliance with applicable laws, regulations, contracts and protection of resources and information" (Donkova, 2022).

"The definition reflects certain basic concepts. Enterprise risk management is:

- A process, ongoing and flowing through an entity;
- Effected by people at every level of an organization;
- Applied in strategy setting;
- Applied across the enterprise, at every level and unit, and includes taking an entity level portfolio view of risk;
- Designed to identify potential events that, if they occur, will affect the entity and to manage risk within its risk appetite;
- Able to provide reasonable assurance to an entity's management and board of directors;
- Geared to achievement of objectives in one or more separate but overlapping categories" (Enterprise Risk Management: Integrated Framework: Executive Summary, Framework, 2004).

Strategy is a method of determining the organization's mission, in the form of long-term goals, action programs and priorities in the allocation of resources at its disposal.

The management of the company forms the strategic goals and chooses a strategy corresponding to the activity of the enterprise. "This enterprise risk management framework is aimed at achieving the objectives set out in four categories:

- **Strategic** – high-level goals aligned with and supporting its mission;
- **Operational** – effective and efficient use of resources;
- **Reporting** – reliability of reporting;
- **Compliant** – compliance with applicable laws and regulations" (Enterprise Risk Management: Integrated Framework: Executive Summary, Framework, 2004).

Objectives related to reporting responsibility and compliance with laws and regulations are under the management of the entity and the organization's risk management can be expected to provide reasonable assurance of their achievement. However, the realization of strategic and operational goals is subject to external events that are not always under the entity's internal control. It would be appropriate for these objectives to ensure rational certainty for enterprise risk management, so that management and the board of directors are informed, in a timely manner, of the extent to which the enterprise is moving towards achieving them.

Enterprise risk management consists of eight interrelated components (HAYES, 2022). They are derived from the way management runs the enterprise and are integrated by the management process. These components are:

- **Internal environment** – The internal environment of an organization is a collection of its resources and integrated management systems and mechanisms and sets the basis for how risk is viewed and directed by people in the enterprise. Includes a world view of risk management and propensity to risk, integrity and moral values, as well as the environment in which they work.
- **Setting goals** – Objectives are the results that the organization wants to achieve and must be in place before management can identify potential events that relate to their achievement.
- **Event identification** – Identification is the determination of the events or factors that threaten the achievement of the company's goals and strategies. These are internal and external events that affect the results of a given entity, objectives must be established, distinguishing between risks and opportunities.
- **Risk assessment** – A process where risks are analyzed in order to determine the likelihood of them occurring and their potential impacts, which is the basis for determining how they should be managed. Risks are assessed based on which are acceptable and tolerable for the organization and which are not.
- **Response to risk** – Process of selecting and applying control actions and measures to deal with the risk, which includes: avoiding, accepting, reducing or sharing the risk.
- **Control activities** – Activities aimed at minimizing risk and increase the possibility that the company's goals and objectives will be achieved. They can be preventive or corrective.

- **Information and communication** – The availability of effective and reliable information and communication systems is a necessary condition for the organization to manage and control its activities. Effective communication results when identifying, gathering and disseminating reliable and credible information, horizontal and vertical communication from and to all levels of the enterprise are included. The information must be appropriately shaped, structured and content, be up-to-date, be provided in a timely manner upon request, be reliable and available to the authorized persons.

- **Monitoring** – Monitoring is a comprehensive review of the organization's activities, risk management is also monitored, and changes are made if necessary. The objective is to assess the state of internal control and to provide the management team with assurance that the control activities are functioning according to their functions and remain effective over time.

There is an interdependence between the goals that the organization seeks to achieve and the enterprise risk management components that are actually all that is needed to achieve them.

Important for effective control in the organization are the concepts of building control systems by using **a system and architectural approach, the process model and control consistency.** For this purpose, it is appropriate to use the theories of the systems to ensure the necessary efficiency of the control system.

The theory of open systems – the open system is characterized by interaction with the external environment, provides an assessment of the influence of external uncontrolled sources of influence on the activity of the control system. An open system has the ability to adapt to changes in the external environment and must do so in order to continue functioning, and **the theory of closed systems** explains its functioning in conditions without the intervention of external uncontrollable factors for it.

The theory of adaptive systems provides the mechanisms for adapting the control system to the changing environment and training of the organization, the flexibility of the control system is ensured while preserving or increasing the efficiency of the economic properties of the object. They are open systems and learn from their mistakes.

Control systems to be capable of corrective action, leading to the use of **corrective systems theory.** The types of systems are of two types: open and closed, functioning only according to the algorithms embedded in them and not having the opportunity to learn from their mistakes.

The architectural approach helps to build the structures necessary for quality control in the organization.

In this line of thinking, the control systems in the organization should be adaptive or corrective, which should be able to be designed as open or closed type, have qualities of adaptability to changes in the environment and function mainly in accordance with their established control algorithms.

The process model is based on the theory of the process approach in management and monitors the current state of the values of the set processes in the enterprise, comparing them with the standards and, in case of deviations, sends signals to the relevant body. Processes in organizations are characterized by resources, process resource input, process, output, and control. To implement the process, resources are needed, which may be material, human, financial or other assets available to the enterprise.

The sequence of control processes is carried out by repetition in time and space of precisely defined activities in their logical and technological sequence. These activities are the following: establishment of standards, measurement, analysis and assessment of deviations. The selection of a standard determines the values of the quantities in the control system.

External standards are requirements in the form of laws, regulations, decrees, tax system, insurance parameters, banking policy, market situation, trade restrictions, etc. **Internal standards** are documents establishing internal normative and regulatory values, such as technological and technological standards, quality standards, contracts, internal regulations, etc. The development of

the organization is determined by the complexity of its vision, goals, strategies, functions, tasks, organizational structure, plans, programs, etc.

The measurement aims at reporting the results of the activities and performs a function of comparing the measured parameters with the set ones. The measurement methods, in turn, are quantitative, qualitative, value, and others, being determined depending on the requirements regarding the control system. The algorithm of the measurements is determined depending on at what exact moment in time, in what sequence and where the measurements will be performed. The obtained results are compared with the requirements set in the standard, in which case we have two options: to meet or not to meet the standard. An evaluation of deviations is then determined and corrective actions are determined if the situation requires them.

We actually distinguish two types of controls, which are known as soft and hard controls. Softs are based on the broader authority of employees in the enterprise, which is dependent on their skills, competence and authority in relation to the managed processes, activities, functions or operations. An effective system of internal control is characterized by economy, content, relevance, compliance and thoughtfulness of the need to make a precise assessment. Information should be timely and simplified, while being comprehensible to the officials of the organization.

This approach provides certain advantages in the operation of internal control systems, such as reliability, traceability and identification of processes, as well as continuous control and monitoring by the governing bodies of the control system.

Conclusions

The application of the applied approaches in the conditions of uncertainty of the functioning and development of enterprises, organizations and companies, allows choosing such a variant of implementation and development, which adequately and reliably ensures the realization of the tasks with minimal deviations from their efficiency, under any conditions of work and ability to withstand economic threats.

The use of standards provides organizations with the opportunity to prevent risks and errors related to their activities, saving time and additional costs for their elimination.

An additional advantage is that businesses are provided with much-needed security and stability.

References

Denchev, S. (2019). *Information and Security.* Ed. about the letters. Sofia, pp. 153-160.

Defense Planning Risk Management Model and armed forces. (2011). Retrieved from: https://www.mod.bg/bg/doc/programi/20110516_ModelRisk.pdf

Donkova, V. (2022). *Good internal control in the company – a guarantor for achieving the set goals.* Retrieved from: http://trudipravo.bg/kompyutarni-produkti-epi/kompyutarni-informacionni-produkti-epi/epi-schetovodstvo-i-danatzi/podbrani-statii/1034-062010epif

Enterprise Risk Management: Integrated Framework. Executive Summary. Framework. (September 2004). Retrieved from: https://egrove.olemiss.edu/cgi/viewcontent.cgi?article=1037&context=aicpa_assoc

Enterprise Risk Management, Integrating with Strategy and Performance. Executive Summary. (June 2017). Retrieved from: https://www.coso.org/Shared%20Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

Hayes, A. (September 07, 2022). *Enterprise Risk Management (ERM): What Is It and How It Works.* Retrieved from: https://www.investopedia.com/terms/e/enterprise-risk-management.asp

Internal control efficiency in light of COSO. (2013). Retrieved from: https://www.ides.bg/media/1242/04-2015-valeria-dineva.pdf

Mladenov, Yu., V. Terziev. (2011). *Fundamentals of Management.* University of Applied Sciences. Retrieved from:

https://www.researchgate.net/profile/VenelinTerziev/publication/309512953_Osnovi_na_upravlenieto/links/58145d9608aeb720f682ade2/Osnovi-na-upravlenieto.pdf

On the risk assessment process as part of an understanding of internal control. Retrieved from: https://www.ides.bg/media/1774/03-2020-vasil-bozhkov.pdf

Petkov, A., A. Nedyalkov. (2015). *Integrated Management Systems.* Retrieved from: file:///C:/Users/Admin/Downloads/51383751.pdf

Radev, K. (2018). *Strategic Management.* Ed. NBU. Retrieved from: https://e-edu.nbu.bg/pluginfile.php/1399362/mod_resource/content/1/Uchebnik%20SM_K.%20Radev_2018.pdf

Security and Management Guidelines of information and communication technologies. Retrieved from: https://www.eiopa.europa.eu/sites/default/files/publications/eiopa_guidelines/eiopa-gls-ict-security-and-governance-bg.pdf

Systems Theory Approach. Retrieved from: *https://saylordotorg.github.io/text_mastering-public-relations/s07-02-systems-theory-approach.html*

The organization as an open management system. Models of the organization as a closed, open, partially open system. Retrieved from: https://amikamoda.ru/bg/organizaciya-kak-otkrytaya-sistema-upravleniya-modeli-organizacii.html