

Prof. Galina Kurteva, PhD*

INTERNAL CONTROL OF THE ORGANIZATION THROUGH RISK MANAGEMENT

Internal control is defined as a comprehensive process integrated in the activity of the organization and implemented by its management and employees. It aims to provide a reasonable confidence level of achievement of the set goals. The main elements of the internal control according to COSO model are five - control environment, risk management, control activities, information and communication, and monitoring. The internal control system in every organization is different and unique as it reflects the specifics, the size, the organizational structure, the complexity and scope of activities, the administrative and business environment, the level of regulation, the management style, etc. However, in order to control its activities, every organization needs all of the five elements of internal control. The article focuses on one of the five elements of internal control – the risk management. Well-managed risk-taking is seen as a prerequisite for sustainable improvement of the activities of the organization.

JEL: M 290; G320

Keywords: internal control system, risk management

The contemporary business organizations could not rely on guaranteed development in the uncertain internal and external environment which generates a variety of dangers and threats requiring a specific approach and a particular pattern of behavior. All entrepreneurs and managers are aware that in order to be competitive they need to learn to take risks. Awareness of the risk as objective and permanent for the organization implies focusing of the management's efforts on the detection of the determinants of individual types of risk, a research on possible adjustments of these determinants as well as establishment of a system allowing elimination of the existing risks.

The role of risk management in the internal control system of the organization

One of the first steps in the process of risk management is assessment (made by the manager) of the organization's risk appetite and capacity to take risks. In other words, it should be clarified the nature and extent of acceptable risk by the organization.

The main causes of the risks are associated with the threats arising from the uncertainty and variability of the external and internal environment of the organization. When risk events occur, especially when they have not been foreseen and assessed,

* Free University of Burgas, galiap@abv.bg

the managers are obliged to take measures and sometimes to spend significant further financing in order to eliminate the consequences of those risk events. In terms of the vulnerability of the business of risk events, most companies acknowledge that the issues related to overcoming the negative consequences can be placed on a professional basis. In other words, the risk can be managed professionally when taking into account both the positive and the negative effects of its influence on the organization.

Therefore, risk management can be characterized as a combination of methods, approaches and activities that allow to a certain extent to predict the occurrence of risk events and to take the necessary measures for exclusion or reducing of the negative consequences of these events. The main task of every manager in the process of risk management is to find a course of actions securing the optimum balance between costs and benefits for the organization from the occurrence of a risk event.

One of the internationally recognized core concepts of risk management in the corporate sector – „Enterprise Risk Management” (ERM)¹ introduces the following definition of risk management on organizational level: *Risk management in the company is a comprehensive process conducted by the Executive Board, the Management Board and the employees. According to the ERM concept, the process starts with defining the organization's strategy and covers all of its activities. This process is intended to:*

- Identify the possible events which can influence the organization;
- Manage the risks according to the organization's risk appetite;
- Provide reasonable assurance of achieving the organization's goals.

The implementation of adequate and effective process of risk management is essential for achieving the organization's goals of the company, which according to the ERM concept can be divided into the following four categories:

- Strategic goals - they are adopted by the management board of the organization and are associated with implementing the mission of the organization;
- Operational goals - they are related to the effective and efficient utilization of the organization's resources;
- Goals, related to financial reporting and accountability, intended to ensure a fair picture of the financial position of the organization;
- Goals, related to adequate enforcement of the legislation, designed to ensure consistency between the organization's activities and applicable laws and regulations.

Through the process of risk management reasonable assurance is to be provided that the management board has established an adequate procedure to define the organization's goals and their compliance with the mission and risk appetite of the organization.

¹ For more information see www.coso.org/publication.htm

Risk management is related to the so-called tolerance of the organization to risk, i.e. acceptable level of deviation related to the achievement of organizational goals. The tolerance can be measured by using the criteria of the respective goals.

If a systematic approach to risk management is applied, then two subsystems will be distinguished: *Controlling subsystem* (subject of control) and *Managed subsystem* (object of management)².

The process of influence of the subject on the object is a management process, formed under the exchange of information between the managed subsystem and the controlling subsystem. The provision of such information requires an appropriate information system. Such system should provide and guarantee the process of risk management in the organization and to contain modern technical means, methods, technological procedures, software and personnel. This system must be set up as a continuously operating structure of the organization. Its main purpose is to gather, process, store and transmit complete, accurate, expedient, reliable and relevant information which can be used by the management board of the organization in the decision making process regarding the risk management within the organization.

Risk management is distinguished by certain specifics and characteristics, expressed as specific management actions and functions. Based on the subsystems which have already been pointed out, the following functions could be distinguished:

- The functions of the managed subsystem refer to the identification of the risk, risk investments, risk reduction activities, risk insurance, economic relations and links between the subjects of the economic processes.
- The functions of the controlling subsystem refer to activities such as forecasting, organization, regulation, coordination, stimulating and controlling in the process of risk management.

Without going into any details only the main features of the functions of the subject (the controlling subsystem) will be outlined. *Forecasting* in risk management is associated with the development of specific predictions about the future behavior of the factors (sources) of risk. The forecasting is often an extrapolation of past into the future, although numerous new mathematical methods for forecasting are very popular. The function *organization* is related to the creation of specific management bodies which implement the program of risk management in the organization on the basis of certain rules, regulations, procedures, norms and methodologies. The

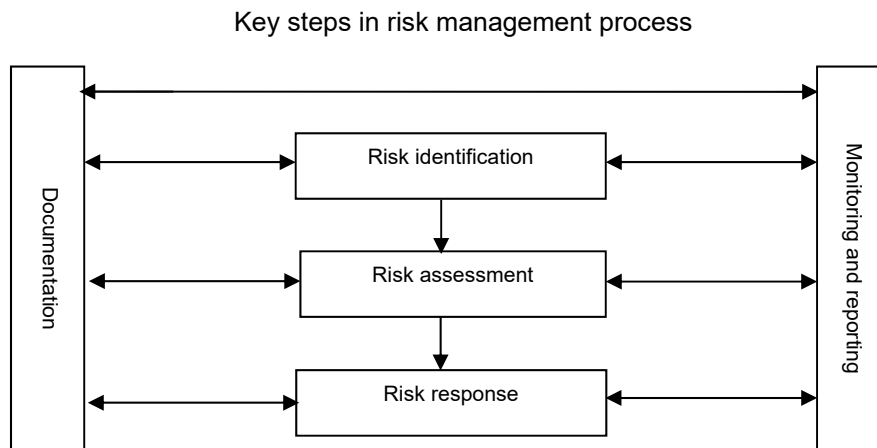
² In the present case we will make the following clarification - "object" means the risk and economic relations between the entities in the process of implementation of a particular action. For example, those are the economic relationships between a creditor and a debtor, an insurer and an insured, competitors, partners; as well as actions related to the purchase of new technology, a release of a new market, offering a new product, etc. "Subject to control" means the person or group of people, specialists in financial management, risk management, insurance, investment management, etc., who by different methods and tools affect the object of management (the managed subsystem) and implement targeted functioning of this object.

actual impact of the controlling system over the managed subsystem reveals the content of the function *regulation*. Through it a steady state of the object (managed subsystem) can be reached in case of deviation from the set parameters. On the other hand, the *coordination* function ensures coherence of the activities in the entire management structure of the organization. Accordingly, the *stimulating* function refers to the specific impact on the persons defined as elements of the subject (the controlling subsystem). That impact stimulates the interest of those persons on the results of risk management. Foremost special attention should be paid to the controlling function as a typical management function. It is related to the risk reduction.

Specifics of the steps in the risk management process

In accordance with the functions of the controlling and managed subsystems in the process of risk management the following steps can be distinguished (see the Figure).

Figure



Source: Stoykov, 2005.

Risk Identification

Risk identification is the first step in the risk management process. A prerequisite to risk identification is exploration of the risk circumstances which adversely affect the normal operation of the organization. In that sense, the initial step is a thorough analysis of the strategic and operational goals of the organization and the activities related to them.

Part of the risk identification is examination and clarification of the events that threaten the achievement of the goals of the organization or the execution of

specific activities. Generally not more than 20-30 risks to the organization could be identified and managed. Therefore, only the most important (essential) risks should be identified. They are the risks which are most likely to occur and have the greatest possible impact on the process of realization of strategic and operational goals of the organization.

The results of the risk identification are correct if the risk sources (internal and external) are correctly identified. Most common among them are:

- Wrong position of the owners of the organization in view of the development, expansion or change in the business;
- unfavourable natural and/or climatic conditions preventing or restricting the implementation of the organizational goals;
- Unforeseen changes in the domestic or the international political and economic situation;
- Insufficient qualification of the personnel to deal with introduced new technologies and associated risks in the production process or services, etc.

It is necessary to identify the effects of the detected risks, which in most cases are loss of capital, fixed assets, finished products, major suppliers, regular customers, qualified employees, confidential information illegally exported and supplied to the competitors.

The relevant specialized literature indicates the following *research methods for identifying risk and risk areas*:

- Traditional research methods:
 - *Desk research* – own/external databases, personal experience, work experience of other organizations in similar situations.
 - *Field studies* – through surveys, experts, observations, experiments.
- Expert research methods:
 - *Brainstorming* – the results are: list of the most probable sources of risk; list of the intrinsic risks; qualitative assessment of the possible cooperation; list of the results at risk.
 - *Delphi method* – an expert assessment with a greater focus (inclusion of questionnaire), greater independence from the initial statements, protection of extreme assessments and more precise determination of the prevailing assessment. Suitable for standard problems.
 - *Mind Mapping* – graphical method for displaying associative thinking and revealing of the relationship between things, in particular - the relationship and interaction between the different risk sources.

Analysis and assessment of the identified risks

In most of the cases in the previous step an extremely large number of diverse risks is identified in the risk management process. Therefore, the so identified risks need to be analyzed in order to determine which of them have a distinct

impact on the business or could cause the greatest negative consequences. In this context, the risk analysis is based on the combination of the possible effects of the risk and the likelihood of its occurring (Stavrev, 1991, p. 14). For more convenience the formula $P = E \times B$ could be used, which determines the level of risk (P) as a product of the presumed consequences/effects of the risk (E) and the likelihood the risk actually to occur (B).

The methods for forecasting the probability of risk events are objective and subjective. Using the *objective* methods, the probability is based on calculations of the frequency with which an event occurs. It should be noted that the mathematical methods and tools of probability theory, the theory of risks and statistics can be used for quantitative assessment of the risks with material and financial consequences. The *subjective* methods are used in determining the probability by subjective criteria which are based on various assumptions derived from the assessor's personal experience, expert assessments, and financial advisors' opinions.

The most appropriate subjective assessment of the probability of an event is considered to be the expert assessment. It is performed by different methods (logical, mathematical, statistical, etc.) based on which the expert processes and analyzes large amount of information (Danailov, 1995, p.53). The essence of the techniques of expert assessments is to obtain answers from experts on issues concerning the development of a risk situation. To minimize errors and the effect of subjective factors, the information obtained from the experts is processed in the specific logical and mathematical procedures (Semerdzhiev, 2007, p. 46). The expert assessments are used in complex situations of choice, without sufficient information and when it is more likely to take a wrong decision. Moreover, many problems requiring a decision generally or partially defy quantification and therefore do not allow the techniques of mathematical modeling and optimization to be used (Georgiev, 1995, p. 95).

According to the purpose of risk management, expert opinion can be used both for determining the probability of a risk event to occur and for forecasting of the trends in its development. Application of the expert opinion is appropriate in the following situations:

- *In determining the strategic goals of the organization.* On one hand, the generation of strategic alternatives is connected to the demand for opportunities for overcoming the weaknesses of the organization in order to reduce its vulnerability to the existing threats in the external environment. On the other hand, the generation of strategic alternatives refers to looking for options for "implementation" of the organization's strengths in mastering the chances conferred upon it by the external environment. Thus, the strategic alternatives are risky in their nature, because the predictions about the behavior of the factors from the external environment are not binding. In such situations, an expert opinion on the likelihood to realization of one or another behavior allows the management board to rank the strategic goals. In some complex situations the so-called 'method of the goals' could be applied in order to establish a hierarchical structure of the goals.

- *In forecasting the trends.* In analyzing alternative management decisions often there is a lack of information in order to make an optimal choice. In such cases, the expert opinion can be used for determining the results and for assessing the trends among the alternatives.

- *In developing scenarios for the future development of the organization.* These are the situations when not all of the parameters for the future are identified and the risk of having an inaccurate estimates and unrealistic analyzes is high. The experts develop three possible scenarios for the future development of a situation that presumably can be defined as a risk: pessimistic, optimistic and probable (real). In the area of their competences, the experts are trying to anticipate the possible scenario for development of the risk situation in order to be able to take the most successful decision. It is important to ensure a practical realization of the principle of consistent reduction of uncertainty as procedures and methods for consistent clarification in time and space of the behavior of the factors from the external and internal environment (Neykova, 2008, p. 383).

- *In generating alternative actions in solving a new problem.* Expert assistance is also very important in cases of changes or when a new problem occurs and the management board does not have a ready solution.

- *In determining ratings.* In many cases, the decision making is based on comparative preferences towards the assessed alternatives/objects (ratings of banks, insurance companies, politicians, athletes, etc.) measured by using a special methodology. This also requires the involvement of experts.

A variation of the method of expert assessments is the *method of commissions*. It involves regular meetings of experts over a problematic situation during which is produced (formed) agreed solution.

Another way for risk assessment with the help of expert techniques is the *KYT³ method*, created and used by the Japanese company "Simitomo Kindzoku" (see Semerdzhiev, 2007, p. 64). According to this method, the result is achieved through debate and discussion of the risk situations in a team of experts who seek a solution to eliminate any negative consequences or to minimize them. The essence of the method is consisted in completing four activities: analysis of the current situation; concretization of the most likely threats; identifying alternative solutions for eliminating or minimizing the risks; discussing criteria for making choices and adopting the optimum of the many variations of decision. The adopted decision is discussed in detail and communicated to the personnel who have to realize it.

Another method which could be applied when an expert report for particular risk event is needed is *the brainstorming method*. It is appropriate in situations when a new, unknown so far event occurs or when a new, non-trivial solution is needed. Variation of the brainstorming method is *the Delphi method*, which is characterized by the following specifics:

³ KYT in Japanese means "training for forecasting dangers".

- Anonymity of the experts - during the conduct of the expert assessment participants are unknown to each other and their interaction in the process is completely off. That could be achieved with the use of special surveys and other means for individual consultation, such as a computer.

- Controllable feedback - a several rounds of consultations are undertaken, on each of which the experts fill in their quantitative assessment of the parameters of the compared alternatives (e.g. deadline for realization of the investment project or level of risk). Then the results are communicated to the experts.

- Statistical processing of the results of the consultation - on this basis, experts recommend version of the decision that reflects, or more precisely corresponds to the views of the majority of the group.

The analyzed risks could be measured, i.e. the frequency and the effects of their occurrence could be assessed. The purpose of the assessment is to answer the following two questions: are these risks acceptable, and if not, what means of protection should be used. From a great importance is a development of criteria for measuring the risk its impact and consequences and, accordingly, adoption of adequate solutions for restricting or even overcoming the risk.

Very important are also the results about the level of the effects of the risk and the risk frequency. According to those results could be defined if *the risk is tolerable, acceptable, or not*. If the risk is unacceptable, it is subject to special monitoring. Risks with measured low level of effects or rare frequency are acceptable to the organization. It accepts them as they are, without interfering. Another important criterion for measuring the risk is whether the cost of the risk treatment is justified or not. If it exceeds the benefits from the treatment such should not be made. The third criterion is *distinguishing between the acceptable risk and other risks*.

Any risk is acceptable and, therefore, is not subjected to a risk treatment when:

- the level of influence and the effects of the risk are low enough and no special attention is required;
- the favourable opportunities for profit-making are greater than the chances of loss;
- the risk sources are external factors where the business cannot intervene (e.g. natural disasters, unforeseen economic and political transformations, etc).

It can be concluded that the risk assessment is a prerequisite for making a decision on how the risk to be controlled and what influence should be exerted on them, i.e. whether the risk is or is not subjected to a treatment and what exactly to be this treatment.

Obviously, the risks cannot be eliminated completely, but they can be significantly reduced by taking the appropriate actions.

Risk Response

Once the identified risks are analyzed and assessed, the manager of the organization needs to consider an appropriate response. Despite the taken specific

measures and actions in most of the cases continues to exist the so-called residual risk. This proves that the risk intrinsic for the organization's activities cannot be removed completely. It is manager's responsibility to assess whether the level of residual risk is acceptable or further actions for its reducing need to be taken. The possible responses to risk, intended to minimize the consequences of events with negative effects or respectively to maximize those with positive effects, are the following:

- *Reducing (mitigating) the risk.* This is most frequently used response to risk because the risk can rarely be entirely avoided or transferred. It is therefore necessary to conduct a periodical monitoring and analyzing of the risk areas within the organization's activity. This will allow, depending upon the extent of the risk and the cost which need to be done, promptly taking action in order to restrict the risk within acceptable parameters.

- *Transferring the risk.* This response is undertaken when the manager considers that the risk is too high and it is better to "transfer" it to a third party. The classic way to transfer risk is the insurance. In this case extra costs are incurred, but on the other hand the "risk impact" indicator is significantly reduced. Another possibility is an agreement with another organization under which by mutual consent the implementation of a particular activity is transferred together with its risks. It should be emphasized that the risk cannot be completely transferred to another party. Therefore, the risk-sharing is a way of taking some of the potential consequences in accordance with the terms of the obligations under the signed contract for this purpose.

- *Accepting the risk.* Such reaction is possible only if certain risks have limited (minor) impact on the achievement of organization's goals or if their avoidance would cost more than just taking them. Such risks are a normal part of the business activity, but they must be continuously monitored because various external or internal factors could have an impact on their occurrence and future influence, and so to shift them to another higher category.

- *Avoiding the risk.* Some risks can be reduced or limited to an acceptable level only through the suspension or avoidance of activities accompanied by huge negative and unsolvable problems for the organization. However, in a hasty or reckless termination or avoidance of an activity benefits could be omitted and subsequently new threats may arise. On the other hand, the management board's inactivity can also be risky because it could prevent achieving the goals pursued by the organization.

The selected actions for risk response should be analyzed in terms of costs and the effects thereof, i.e. the effectiveness of the chosen response, its duration, the cost of implementation and the level of residual risk after the implementation phase should be assessed.

In the context of choosing a risk response a security program (within the organization) needs to be developed. In the process of implementation of the security program specific activities and actions are conducted, associated with the

specified measures for determination of the needed resources for countering the risk and financing preventive measures; deadlines for implementation; units and persons responsible for them; identification of deviations and losses in project activities; determining the persons who will take the decision to remove or offset these losses; impact on the subjective risk, etc.

Monitoring and reporting

Ensuring the efficiency of the process of risk management requires ongoing monitoring at every stage and periodic reporting of the identified risks and the taken actions (responses). Monitoring activities are undertaken via daily ongoing operational activities or via separate periodic evaluations of the risk management process. Both types could be applied simultaneously.

The daily ongoing monitoring should be integrated into normal routine (operational) activities of the organization, to be performed in real time in order to react to the changing conditions. Therefore, it is more effective than the separate periodic evaluations because they are obtained after the risk event.

Separate periodic evaluations vary in scope and frequency, depending on the degree of influence of the risks and the importance of the responses to them. The high risk areas and responses are usually measured more frequently. Usually the evaluations take the form of self-assessments when the persons responsible for a unit or function, establish the effectiveness of the process of risk management in terms of their own activities.

The aim of the monitoring and reporting process is *to observe the changes in the risk profile of the organization (the probability and the impact of identified risks) in order to create confidence in the management board that the risk management process remains effective over time and the necessary actions to reduce the risk to an acceptable level have been taken*. For the successful implementation of this process it is necessary to develop *internal rules/procedures* as a part of the overall strategy for risk management in the organization. These internal rules/procedures need to describe:

- The communication and exchange of information (regarding the identified risks) between all levels and employees within the organization;
- The procedure and terms for conducting regular reviews of the risk - register;
- The procedure and terms for reporting all significant risks, the undertaken actions and their effects, as well as informing about the newly arisen events;
- The responsible departments and employees for the implementation of the necessary actions.

The ways in which the management board will apply these rules and procedures and organize the process of risk management depends on the particular circumstances associated with the organization (whether its administration has a high degree of self-government, or is centralized; what activities are carried out and from what nature are the risk which the administration faces).

Internal control of the organization through risk management

To sum up, the scope of the risk management in the organization includes the following activities:

- Identification, assessment and prioritization of the risks which threaten the achievement of the organization's goals;
- Implementation of activities to control the risks which reduce or somehow lower down the levels of the risks to acceptable;
- Conducting ongoing daily monitoring and periodic re-evaluation of the risk, as well as the efficiency of the activities related to its management;
- Preparation of periodic reports providing information on the results of risk management;
- Taking corrective actions based on the information from the monitoring and reporting.

In the process of implementation of the risk management activities, the managers could require additional specialized assistance by a working group within the organization or by external consultants, specialists in risk management.

The employee entrusted with coordinating the risk management process works together with the employees at various management levels in the organization and assists them with identifying, evaluating and selecting the appropriate responses to risks events. Every manager detects and identifies on his own the possible risks related to his unit of the organization and later on together with the employee responsible for this process they create a risk-register. When choosing such an approach, the head of the organization is responsible to determine: the frequency of the meetings between the employee who is coordinating the process of risk management and the employees at managerial positions; the procedure and method for communication between them; the documenting of the taken decisions; the procedures for reporting to the head of the organization.

In relation to the coordination of the process of risk management in the organization a *working group* could be set up, with carefully selected personnel. The participants in this working group are selected not only with regard to the specific position they occupy, but also with regard to their personal qualities and competence - their knowledge of specific areas of activity for the risk management process, etc. Important requirement for the successful activity of the working group is the precise defining of the responsibilities of each of the participants as well as the clear instructions for communication within group and with other employees from the organization. Thus, an adequate response and assessment by the working group will be guaranteed in cases of changes in the circumstances. The working group follows the best practices in the risk management process, communicates and exchanges information with organizations or individual departments in which this process is considerably advanced; organizes training for employees where the nature and benefits of the risk management process is explained in a clear and structured way. All this leads to significant improvement of the effectiveness and efficiency of the risk management process in the organization.

*

The conclusion that can be made is that the risk management is a dynamic process that requires constant and thorough attention until it becomes an element of the managerial life of the organization. Establishment of a risk management system is a mission and a goal that must become a top priority for the senior management of the organization. Successful risk management within the organization is crucial for the success of the organization's activities on the market and an integral part of its organizational structure and strategy. It should be adopted by the management board of each organization as a culture, processes, structure and solutions that are a prerequisite for an effective management.

References:

Georgiev, I. (1995). Rudiments of investments. Sofia: Open Society Foundation Publishing House (in Bulgarian).

Danailov, D. (1995). Corporate business analyses. Sofia (in Bulgarian).

Draganov, Hr. (2003). Risk Management. PH „Trakia“ (in Bulgarian).

Kurdi, Dzh. (2009). Business strategy. Efficient decision-making process. Sofia: PH „Classics and Style“ (in Bulgarian).

Neykova, R. (2008). Risk and risk management in industries. Gabrovo: PH „Express“ (in Bulgarian).

Semerdzhiiev, Tsh. (2007). Strategic management and leadership - leader. Sofia: PH „Soft Trade“ (in Bulgarian).

Stavrev, Sv. (2005). Economic management methods. Svishtov: APH „Tshenov“ (in Bulgarian).

30.IX.2016