RISK MANAGEMENT – BETWEEN NECESSITY AND OBLIGATION

Ion CROITORU, PhD Associate Professor
Athenaeum University, Bucharest, Romania
ion.croitoru.ag@gmail.com

Viorica NEACȘU (BURCEA), PhD Student
University of Valahia Targoviste, Romania
viorica.burcea@yahoo.com

Abstract: *Risk management is a process designed and set by the leadership of economic organizations and implemented by all staff to avoid or minimize losses, protect resources, and patrimony. Good process management ensures the achievement of organizational goals, efficient use of resources and achievement of expected profitability levels. In order for the risk management process to be effective, it is necessary for the organization to develop appropriate risk strategies and policies, specific rules and procedures to help identify and assess risks. The effectiveness of the risk management process is ensured if the organizational culture is appropriate to the risks, the staff knows the risk strategy developed by the organization and is aware that the good risk management ensures the achievement of the organizational objectives. The risk management process needs to be integrated with objectives and activities and involves identifying and assessing risks, risk control, risk monitoring and review.*

Keywords: *exposure to risk, impact, objectives, risk management, likelihood, inherent risks, organizational risks, residual risks, strategic risks*
JEL Classification: *M00, M40, M41*

Risk management - objective of management

Up to now, no risk definition has been formulated, which is unanimously accepted by all specialists in the field. In practice, concepts such as:

„Risk is the threat to an event or action with an unfavorable impact on the entity's ability to successfully achieve its goals" (Renard 2014). The definition highlights that risk poses a threat that something may happen, or an event to occur if it is not sufficiently controlled and will have an impact on the organization.

„The risk is the threat that an action or event will adversely affect an organization's ability to achieve its goals and to successfully implement its strategy. Griffith (1998)." This definition, simple and easy to understand, appreciates the risk of being a chance for a positive or negative event to happen and affect the achievement of goals.

„Risk is the possibility or opportunity for something to happen that will have an effect on achieving the goals Griffith (1998)." This definition highlights that risk can have a negative impact on the achievement of objectives if it poses a threat but can also have positive connotations that can be used by the organization. The analysis shows that risk may be a threat or an opportunity. Risk is also the uncertainty about achieving the desired results and should be seen as a combination of probability and impact.

Probability is the extent to which risk can be manifested and can be judged by high, medium or low probability. **High probability** exists when risk is not controlled and its manifestation can not be prevented by the organization. **Low likelihood** can be attributed to a risk if it is well managed by the organization, ie the internal controls implemented maintain the risk in the accepted levels.

The impact of risk is the consequence of the results (objectives) if the risk materializes. If the risk poses a threat, the consequence is a negative one, and if the risk is an opportunity, the consequence is a positive one.

The impact of risk can be assessed by high impact, medium impact and low impact. **The high impact** implies that the materialization of the risk implies a high degree of severity. **The low impact** implies a reduced severity if the risk is manifested.

From the analysis of risk concepts, it can be appreciated that risk management involves identifying, evaluating, managing and controlling risks in order to ensure that organizational goals are achieved.

In relation to the presented, it is found that the risk is a result of the vulnerability of the organization and its inability to adapt to the environment

in which it operates. In practice, problems related to the identification and assessment of risks are attributed to the ability to identify the risks and then manage them.

Risk management is a process designed and established by the leadership of economic organizations and implemented by all staff. This involves identifying and assessing risks, establishing risk tolerance and treating uncontrolled risks.

The implementation of a risk management process at the level is due to the uncertainties of the nature of the threats that may affect the achievement of the objectives and the environment in which the organization operates.

The overall objective of risk management is to manage risks in order to ensure the efficient and effective use of resources, the protection of patrimony and employees.

In this sense, the implementation of the risk management process involves:

a) risk management as the responsibility of management;
b) creating a positive culture of risk;
c) knowledge and management of threats that prevent the achievement of goals;
d) prioritizing risk decisions.

To meet these requirements, the organization sets out actions, implementation measures, responsible and reporting systems at the level of functional structures.

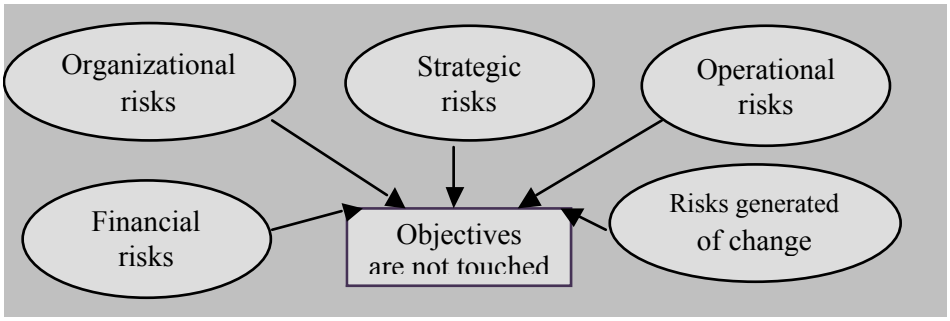
A proper risk management process ensures:

a) efficient and effective use of resources;
b) change in driving style;
c) achieving the objectives in an efficient and effective manner;
d) building a healthy internal control system.

The risk management process is continuous and the results are materialized by the decisions taken regarding the acceptance, reduction or elimination of the risks that affect the achievement of the objectives. The goal is to optimize the organization's risk exposure to prevent losses, avoid threats, and exploit opportunities (Vasile & Croitoru 2011).

Classification of risks

At the level of an economic organization there are several categories of risks, controlled or uncontrolled, that have an influence on the achievement of the objectives, depending on the nature of the operations they generate, namely:



Source: Own projection

Strategic risks are directly related to the organization's development strategy and are associated with strategic goals.

Organizational risks are associated with the organizational process, the implementation of operational activities and procedures.

Financial risks are caused by interest rates, inflation, insurance, taxes and taxes, protectionist policies, regional policies, the need to reduce losses.

The risks of change are caused by legislative changes, professional ethics, the level of culture and training of staff, the needs and needs of staff, and the fluctuation of staff.

Operational risks are directly related to the functional compartments of the organization and are associated with the specific objectives defined at the level of the functional structures.

Organizational changes, the existence of poorly trained, unmotivated, unskilled staff, as well as changes in the work environment or in doing business lead to increased exposure to risk. The approach approaches the following approaches:

• The procedural approach involves taking into account the characteristics and requirements for achieving the operational processes, management processes, processes that characterize the organization's support functions, activities and actions;

• The causal approach implies taking into account the changes in the human resources structure, the professional training of the personnel, the structure of the indicators defined for the performance measurement, as well as the application of the internal provisions of the organization.

In order for the risk to be minimized and controlled, it is necessary: „the internal control system to be adapted to the nature and complexity of the activities carried out and to ensure at least the following actions: delegation of competence and responsibility, separation of functions, protection of assets and internal audit function (Iovu 2005)."

In our opinion the characteristics of the risk can be as follows:

a) exposure to risk, there are various ways of risk exposure of the organization, such as staff, patrimony or organizational environment;
b) the risk factors are related to the characteristics of the organization and the applicable legislative framework;
c) the potential impact, represents the consequences of the organization, as a result of the risk manifestation.

Risk exposure is the level at which risk can be accepted if it materializes. The outcome of the risk assessment is as follows:

a) if exposure to risk is greater than the accepted level, the risk is assumed to be inherent, uncontrolled. Internal controls implemented are insufficient or inoperative, which requires that risks be mitigated to limit their level;
b) if the risk exposure is lower than the accepted level, it is assumed that the risk is a residual, controlled and no need for intervention.

The factors that determine the risk exposure of an economic organization can be defined as follows:

a) structural changes, major changes made on the basis of internal decisions;
b) fitting into available financial resources;
c) limited staff training and motivation programs;
d) setting tasks for employees in accordance with their nature and qualification;
e) insufficient procedures.

Taking into account that risk poses the threat that an event or action adversely affects the ability of an organization to achieve its goals, we believe that achieving the set goals may be under uncertainty if management decisions and actions taken to implement they do not take into account the existing realities and risks. Also, given that risk is assessed based on probability and impact, it is the responsibility of the management to identify, assess and treat the risks and, depending on the results, establish the appropriate control tools that need to be implemented to maintain the risks in accepted levels.

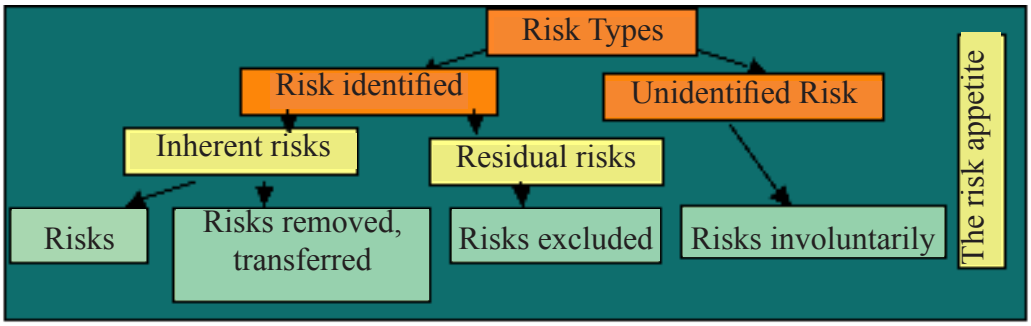
Types of risks

Risks identified in an organization may fall into two categories, namely inherent risks and residual risks.

The inherent risks are the risks that normally exist in any business carried out and are defined as „the risk existent prior to the application of internal control measures to reduce it", or „the entirety of the risks that lie on

the entity/organization and may be internal risks or external, measurable or unmeasurable (Vasile & Popescu 2004)." Thus, inherent risk is the possibility of errors or discrepancies in management and financial statements before the impact of internal control measures.

Residual risks are „exposure due to a certain risk after measures have been taken to mitigate it. Risk mitigation measures belong to internal control. For this reason, residual risk is a measure of the effectiveness of internal control, which is why some countries have replaced the term residual risk with the control risk." Thus, residual risk is considered as the risk that remains after the implementation of internal control measures. Applying internal control measures should have the effect of limiting inherent risk to a level that is acceptable to the organization.



Source: Own projection

Inherent risks and residual risks are considered as two hypostases of the same risk. Thus, the inherent risks exist prior to the introduction of internal control instruments, and the residual risks exist after the introduction of internal control instruments.

The degree of risk identification is influenced by a number of factors, including: organizational culture vs. risk, training and knowledge in the field, methods and tools used to identify and assess risks, complexity and volume of activities.

Apart from the inherent risks and residual risks, other types of risks identified at the organization level are the control risk and the risk of non-detection. The control risk is the risk that the organization's internal control system fails to prevent or detect timely errors, irregularities or fraud. These risks may appear in the balance of an account or in a category of transactions and may be individually significant or aggregated with other information. The

risk of undetectability is the risk that a particular threat can not be identified and managed.

Taking into account the fact that the risks can not be avoided or eliminated, the opinion of the specialists in the field is that „economic organizations must be concerned about risk assessment and keeping them within the limits they can accept and tolerate."

The link between the risk management process and the COSO model

The COSO Risk Management Framework Model is recognized as a key element for good governance. The internal control implementation methodology presented by COSO has been embedded in policies, rules, procedures and regulations and used by various organizations to ensure control over the way in which the planned activities are carried out and the achievement of the objectives.

COSO defines risk management as „the process of the board of directors, management, and others, applied in strategy setting and throughout the organization, to identify potential events that may affect the entity and manage risk within the risk appetite to provide a reasonable assurance of achieving the objectives of the organization" (Tomoiala & Mare 2012).

The COSO framework manages risk to the risk appetite, which implies that the inherent risks are „evaluated and treated by implementing control devices that act on the impact and likelihood of occurrence of risks so that they become residual risks."

Thus, the implementation of the process is influenced at the level of each organization's organizational culture against risks, the philosophy of risk management disseminated among staff, and the way in which the negative effects of risk are attained at all levels of the entity.

The need for risk management is determined by the fact that uncertainty is a reality, and the reaction to uncertainty is a permanent concern. Because, acquiring a risk management system, unanimously accepted at the level organization becomes indispensable for the practice of financial-accounting activity (Vasile & Croitoru 2012).

Conclusions

In our opinion, the implementation of the risk management process should be structured according to the following components (Vasile & Croitoru 2011):

A. The internal environment within this specific component is the activities carried out on the establishment of the organizational structure, the tasks and responsibilities, the setting of the conditions in which the activities can be carried out and the requirements for the future development of the organization.

B. Establishing the objectives, this component is characterized by the fact that the implementation of a risk management system involves identifying and assessing the risks that affect the achievement of the objectives. Objectives must be defined so as to pose a challenge to management and staff, regardless of the level at which they are set.

C. Identifying events, this component involves identifying internal and external events that may affect the achievement of objectives. Depending on the consequences, the identified events are categorized into risks or opportunities.

When defining risks, the following rules should be considered: risk is uncertainty, difficult issues are assessed, problems that do not occur are not risks, problems that arise are certain, risk must not be defined by its impact on objectives, risks are identified by correlation with objectives , the risks have a cause and an effect, the differentiation between the inherent risk and the residual risk.

An adequate risk management process involves identifying risks at any level where there is a threat that may adversely affect the achievement of objectives, their assessment and appropriate risk mitigation measures.

D. Risk assessment, which involves assessing the likelihood of materializing risks and the impact of risk, based on a risk analysis matrix. The likelihood of materialization of risk is determined by the sufficiency and functionality of internal control. The impact of risk is the consequence of risk if it materializes.

The risk assessment should follow if the proposed control tools for implementation are the most appropriate.

E. Response to risk is the decisions taken by the management of the public entity following the risk assessment process and aiming at reducing the likelihood of the occurrence of the risks and their impact. In relation to the outcome of the risk assessment, the response to risk may be as follows:

a) accepting risks in the form and size they exist, without any mitigation measures. These situations are specific to residual risks, characterized by the existence of sufficient internal controls that limit the likelihood of risk exposure and make it impossible to manifest it.

b) treating risks, involves identifying and implementing appropriate control measures to limit the probability and impact of risk. These situations are specific to the inherent, uncontrolled risks of the entity and require control measures to reduce their level.

c) avoiding risks, involves eliminating risks by reducing or ending the activities to which those risks are associated. These situations are specific to risks with high exposure to the accepted level and can not be treated or treatment costs are higher than the results obtained.

d) the transfer of risks, implies that certain risks can not be controlled by any control measures which require their transfer to other structures.

The control tools used to handle the risks can be as follows (Ghita et al. 2010):

a) preventive control instruments are used to limit the effects of the risks that may arise, and to ensure that unwanted results do not materialize;

b) corrective control instruments are used to correct unwanted results if the risks materialize;

c) directional control instruments are used to obtain a particular result or transfer a risk to another area within the entity where it can be tolerated;

d) detective control instruments, are used to identify new emergencies as a result of materializing the risk.

F. Risk control is designed to ensure that the set objectives are met and the significant risks are properly managed.

G. Information and communication, involves measures initiated by management to communicate to staff the responsibilities of those involved in the risk management process. For staff to make an effective contribution to the risk management process, it is imperative that the information be communicated in a timely manner so that it can carry out its tasks within the deadlines set.

H. Risk monitoring and surveillance is intended to track the profile of risks, whether they persist, new risks have emerged, impacts or probabilities have changed, internal control instruments put in place are effective, or certain risks need to be redefined.

Risk oversight involves knowing the concepts and mechanisms with which the entity operates in the process of risk management, implementation modalities, and assessing the effectiveness of risk management implementation.

In our opinion, the effectiveness of risk management largely depends on the quality of the internal control system implemented, ie whether the expected controls correspond to the existing controls. In general, organizations have implemented a risk management system, but they are very little focused on identifying and managing risks (Croitoru 2014).

References

Croitoru, I. (2014). Operational Risk Management and Monitoring. *Internal Audit & Risk Management*, No. 4(36), pp. 21-31.

Ghiţă, M., Croitoru, I., Popescu, M. and Ţogoe D. (2010). *Corporate Governance and Internal Audit*. Galati: Europlus Publishing House.

Griffiths, P. (1998). *Risk-Based Auditing*. England: Gower Publishing Limited.

Iovu, G. (2005). Procedures Manual, Internal Control and Advanced Method for Operational Risk Management according to the Basell II Agreement, *Conference on IT & C Markets and Financial-Banking*, Bucharest.

Jacques, Renard. (2004). *Theory and practice of internal audit*, Fourth edition. Bucharest: Print Art Graphics.

Popescu M. and Vasile E. (2004). *Internal control and audit*. Bucharest: Ben Publishing House.

Tomoială, M. and Mare E. (2012). *Internal-Managerial Control*. Iasi: Ştef Publishing House.

Vasile E. and Croitoru I. (2011). Integrated risk management system - key factor of the organization's management system, Chapter in the *Risk Management Book,* Croatia: Tech Publishing House.

Vasile E., I. Croitoru. (2012). Risk Management in the Financial Accounting Activity. *Internal Auditing & Risk Management* No. 1 (25), pp. 13-24.

Vasile, E. and Popescu, M. (2004). Internal Control and Auditing. Bucharest: Bren Publishing House.