DOI: 10.5281/zenodo.4058375

RISK MANAGEMENT IN PUBLIC ENTITIES – MANDATORY ELEMENTS

Viorel BULMEZ, PhD Student
Athenaeum University Bucharest
bulmez_v@yahoo.com

Abstract: *In its historical dimension, risk is a young concept while being one of the few business terms with direct origins within the commercial and financial field, and not derived from the military, psychologically or scientifically vocabulary. A general response to the following question: "why is it necessary a risk management?" is induced by the observation which proves that in any organization, or field that this one takes action into exists uncertainties seen as threats in accomplishing the given objectives. Therefore, to implement functional politics of management of risk in the public entities it is necessary to follow some mandatory steps: Understanding the concept of risk by the management of the public entities; Awareness of internal and external factors of risk; Identification of risks which may negatively affect necessary activities for accomplishing the objectives of public entities; Evaluation and ranking of risks; Establishment and implementation of countermeasures of risks; and Periodic evaluation of risk's level.*

Keywords: *public sector audits*
JEL Classification: *H83*

1. What is risk? Concepts regarding risk

The word "risk" is derived from the Italian "risicare" which stands for the verb "to dare". Therefore, *risk is a choice, not a fate* (Spencer Pickett, 2006, pag. 54). From this definition we can understand that we are truly exposed to risks in our daily lives, we have control over them because we can change different variables if we have the time and the necessary inclination.

Generally, risk is a part of every humanly effort. From the moment we leave home to when we are back we are exposed to all kinds of risks. The

significant fact is that on one hand some risks are completely up to us, and on the other hand we create the risks through our daily activities.

We can say that there is a risk in everything we do, in any kind of activity, in every decision we make. These manifest in one way or another, even if we do not want to admit it.

It is wisely recommended to us that we should understand the risks and try to deal with them.

In the present time, there is no unanimously accepted definition of the concept of risk by all specialists in the field. Among the most commonly used definitions are the following:

"Risk represents the possibility of obtaining favorable or unfavorable results in a future action expressed in probabilistic terms."

"The risk is the possibility that a future event will materialize and may cause some losses."

"The risk is the threat that an event or action will negatively affect an organization's ability to meet its objectives."

The following conclusions can be drawn from the analysis of these definitions of risk:

a) Probability versus consequences. While some definitions of risk focus only on the probability of an occurring event, other definitions are more comprehensive, including both the probability of occurrence of the risk and the consequences of the event.

b) Risk and threat. In defining the concept, some specialists put the sign of equality between risk and threat. We specify that a threat is an event with a low probability of manifestation, but with high negative consequences, given that the probability of manifestation is difficult to assess in these cases. A risk is an event with a higher probability of occurrence, for which there is sufficient information to make an assessment of the probability and consequences.

c) Comparing only negative results. Some concepts of risk focus only on adverse events, while others consider all variables, both threats and opportunities.

d) Risk is related to profitability and loss. Obtaining the expected result of an activity is under the influence of random factors, which accompany it in all stages of its development, regardless of the field of activity.

The term “risk” taken singularly is meaningless, as long as it is not supplemented by the type of loss, from which it is calculated (the entity subject to the loss) and the type of conditions or circumstances for which the assessment is made (exposure to danger).

2. Risk Categories

For example, below are the risk categories identified by the English Ministry of Finance (Treasury) to support organizations in verifying that they have considered the full range of risks that may arise:

A. External risks arise from the external environment and cannot be fully controlled by the organization, but for which mitigation measures can be taken, as it follows:

- political
- economical
- socio-cultural
- technological
- legal
- environmental

B. Operational risks are related to the current activities, both the current way of carrying out the activity, and the construction and maintenance of the capacity and capability, respectively:

- related to the development of the activity:
  a) the possibility to provide a product / service
  b) carrying out activities / projects
- related to capacity and capability;
  a) resources (active, human, financial, informational)
  b) relationships
  c) operations (obtaining results)
  c) reputation
- related to the way and capacity of risk management
  a) governance (regularity and fairness)
  b) exploration (ability to identify risks and opportunities)
  c) flexibility and adaptability
  d) security (active, social, informational)

C. Change are the risks related to objectives, strategies and policies, respectively:

- new strategies
- new politicians
- new programs
- new projects

3. Inherent and residual risks

The inherent risk is the risk arising within an entity in the absence of any management actions to change / transform the probability or impact of events.

Residual/remaining risk is the risk that remains after the existing management response has been taken into account. The technology for assessing the two types of risks is the same reason why, previously, reference was made to risk assessment in general and not to the assessment of one type of risk.

The inherent risk and the residual risk are two hypostases of the same risk: before the introduction of an internal control instrument and, respectively, after the introduction of an internal control instrument. Therefore, the inherent risk exposure is a measure of the "amount" of risk to which the organization is exposed if the internal control system does not work, and the residual risk exposure is a measure of the amount of risk remaining after the internal control instruments have been implemented.

The inherent risk, where there is no instrument of internal control, is not the most common case in organizations. They have internal control systems for many risks, even if the situations or events that are kept under control are not perceived (realized) as risks.

Internal control systems can be said to be adequate or not, but it cannot be argued that they do not exist. Because of this, the inherent and residual risk are relative and not absolute.

When the internal control implemented at a given time in the organization in relation to a certain risk results in an exposure to risk exceeding the tolerability limits, the previous residual risk is considered an inherent risk in relation to adjustments and developments of the existing internal control system. The internal control system adjusted and developed to capture changes in circumstances is completed by a new residual risk.

It is important that the response to relevant risks is proportionate to their impact and likelihood of occurrence.Providing a response to a risk is therefore a matter of optimizing risk management and not a simple attempt to eliminate or reduce the risks.

4. Public entities facing typical risks

Reasonable assurance reflects the view that the uncertainty and risk associated with the future cannot be predicted by anyone. In addition, factors beyond the control or influence of the entity, such as policy, may impact the ability to achieve its own objectives. In the public sector, factors beyond the control of the entity may even change major objectives in a short time. An important component of the internal control environment is the senior management of

the institution, significantly influencing the organizational climate. "Top tone" can establish or fatally undermine organizational culture. The independence of senior management from executive management, the experience and quality of members, the degree of involvement and research and the timeliness of activities play a very important role. Executive management may be part of senior management, but for the efficiency of the internal environment, the senior management team must include independent, non-executive members.

The attribution of authority and responsibility implies the level to which individuals and teams are authorized and encouraged to take the initiative to solve problems, while also setting the limits of their authorization. The support of the human resources department on practices related to the employment and promotion of appropriate people, professional training and concern for unsatisfactory performance is required. Management must specify the level of competence for particular tasks and transpose them in the job description for those special positions.

It is necessary to ensure that staff understand the entity's objectives and how their actions contribute to those objectives. Responsibility is as important as authority.

Limitations also result from the following realities: human judgment in making decisions can be imperfect; failures can occur due to human errors such as simple mistakes or deviations; the decisions that must react to the risks and the establishment of the necessary controls to take into account the costs and benefits; controls may be circumvented by secret agreements between two or more persons and management may disregard the control system.

5. The benefits of implementing a functional, efficient and performant system of risk management in public entities

Any manager must pay more attention to threat management because otherwise it jeopardizes the realization of its objectives. Also, a competent manager takes advantage of the opportunities for the benefit of the organization, proving his efficiency. If uncertainty is an everyday reality, then the reaction to uncertainty must also become a permanent concern. By implementing a risk management system, public sector organizations in Romania can achieve the following objectives:

a) making informed decisions;

b) planning the management system based on the hierarchy of specific risks;

c) more efficient allocation and use of available resources;

d) obtaining a high level of transparency of the management and decision-making process;

e) ensuring a greater degree of flexibility for alternative actions, as a result of a better understanding of the sources of risk;

f) compliance with the requirements of the relevant legislation;

g) substantiation of an approach regarding the uncertainty management mode;

h) ensuring a better identification and enhancement of opportunities.

The long-term benefits of these organizations include:

a) ensuring an increased degree of preparation for highlighting the positive consequences;

b) effective strategic planning, as a result of the high level of knowledge and understanding of the key risk exposure factors;

c) reduction of costs, as a result of forecasting undesirable effects and adopting appropriate measures to prevent them;

d) improving the audit processes and increasing the degree of capitalization of the results of internal and external evaluations;

e) better results in terms of efficiency, effectiveness and adequacy of the programs; for example, improved management and better allocation of available resources (human, financial and material);

f) ensuring an efficient communication base between the organizations and the affected / interested parties, in order to formulate the directions and design the priority action programs.

6. Risk management process

One of the most important standards that make up the Code of Internal Control, approved by the O.S.G.G. no.600 / 2018 is the standard regarding risk management (Standard 8).

According to the standard mentioned above, each public entity has the obligation to establish and implement a risk management process that facilitates the efficient and effective achievement of its objectives.

This practice has migrated from the private to the public sector, so that more and more governments in European Union member countries have integrated risk management into public management reforms in recent years.

Risk management is a preventive attitude regarding the elimination or limitation of damages, when there is the possibility of materializing a risk, respectively a process of identifying, analyzing and responding to the potential risks of an organization.

Under these conditions, the role of risk management is to help understanding the risks to which the organization is exposed, so that they can be managed. This role differs depending on when the analysis is performed, as follows:

- if the risk assessment is performed before the risk materializes, the purpose is to avoid the occurrence of the event;

- if the risk assessment is performed after the risk has materialized, the purpose is to ensure the performance of the activities and the continuity of the organization's activities.

The advantage of implementing the risk management system within the organization is to ensure the efficiency and effectiveness of operations. In order to achieve this requirement, the management of the organization has the responsibility to make known the risks it faces and to manage them properly, in order to avoid the consequences, in case of their materialization.

Risk management is the responsibility of the organization's management, and the central objective of this process is to manage risks so that resources are used efficiently and effectively to maximize results and minimize potential threats, while protecting the interests of employees and beneficiaries.

In order to ensure an efficient risk management, it is necessary to create organizational structures adequate to the organization's strategies and policies. In this regard, the organization must adopt appropriate policies in terms of organization, so as to effectively monitor each risk or risk category and in an integrated manner, the entire system of risks that accompanies the activities of the organization.

The policies and strategies that can be adopted in terms of organization are related to:

- establishing and elaborating its own system of norms and procedures, which put into practice to ensure the avoidance or minimization of risks;

- establishing the appropriate functional structure based on a clear design, which must ensure adequate compartments that contribute to the identification and monitoring of risks. Risk management is required because organizations face a multitude of internal and external factors of influence, and the biggest challenge for management is to determine what level of risk it is prepared to accept in carrying out its mission, so as to add value to activities and achieve their goals.

7. Techniques of risks identification

The risk identification process aims to discover all possible sources of risk in order to eliminate or reduce the effects they may produce.

Following the risk identification process, analysts can quantify these risks and establish ways to approach them in order to avoid situations in which the manager or organization is caught by unknown events.

Risk identification can be achieved through several methods such as:

• Internal questions;
• Brainstorming;
• Activity logs;
• Process and flow charts;
• Regular meetings with the staff involved.

Achieving the objectives of integrated risk management within an organization involves the fulfillment, in a logical sequence, of specific and necessary activities, as follows: setting objectives; identifying risks; risk assessment, establishing the risk response; implementation of control measures, information and communication and monitoring.

Once the risks have been identified and assessed and after the tolerance limits have been defined within which the organization is willing, at some point, to take risks, it is necessary to establish the type of risk response for each risk.

The risk response depends on the nature of the risks considered from the perspective of control (control) possibilities.

In fact, it is the answer to the following questions:

• can the risks be controlled by the organization?
• if so, can the organization control the risks to a satisfactory level?
• if not, can the organization outsource the risks or risk-generating activities?

Risk management is a process designed and established by management and implemented by all staff within the entity.

The implementation of an integrated risk management system involves the identification and assessment of risks that threaten the achievement of objectives.

This category includes the risks related to the activities and actions related to the entries, the risks related to the actual processes carried out within the organization, the risks that prevent the achievement of the planned results, as well as the risks related to the impact of activities.

Setting goals is an exclusive task of the institution's senior management. Their source is found in the current activity plans, multiannual planning, attributions and essential functions of the respective institution, the legislation that regulates its operation, orders, methodologies, production plans, procurement programs, etc.

Once the objectives are established, they are transmitted to the line management (heads of services, offices, compartments, similar), their task being to establish the subsequent activities necessary to achieve them, the tasks and responsibilities of subordinates, deadlines.

Execution staff must understand in detail the activities they are to carry out, assume their responsibilities and deadlines. At the same time, it is very useful for them to hierarchically signal the limitations and obstacles encountered in carrying out the established activities, to sensitize the management on the deficiencies and non-conformities identified.

Among the factors that constitute the risk environment and that public institutions must take into account are the following:

a) the legislative framework: the organization must identify those norms under whose incidence it falls; the rules are nothing but constraints that limit the way organizations act (for example, the risk of staff not performing their tasks satisfactorily cannot be fully controlled by internal control tools; the organization must take into account labor law in order not to is exposed to the risk of incurring legal sanctions);

b) political conditions: a factor of the risk environment, especially for public organizations, is the Government itself; public organizations exist to implement the policies of the Government and its ministries; for this reason, the approach of some risks by the leaders of these organizations is often conditioned by political decisions;

c) material and financial resources: in the case of public institutions the material and financial resources are generally limited, so that activities such as modernization of infrastructure, equipment, technology, computer systems, are usually delayed or canceled, the decision-making process is complicated and time consuming.

d) human resources: in the conditions of a less developed economy, the budgetary constraints affect the possibility of public bodies to attract qualified labor force, an internal control tool that would allow to better manage the risk of non-fulfillment of tasks by employees.

The risk management activity cannot be started without identifying the sources of risk. The identification process consists in looking for all the sources generating events that can negatively affect the activity of the organization having at its disposal a series of tools.

In practice, these tools are used either in combination or successively, the main purpose being not to overlook any risk that may affect the proper conduct of the organization's activities.

Once a source of risk has been identified, it must be analyzed, the probability of generating a risk event and the impact that this event may have must be established.

Depending on the values thus determined, a hierarchy of risks will be made, following that those at the top of the ranking will pay immediate attention to the proper management so that the consequences of their manifestation are diminished and eliminated as much as possible.

The risk assessment process involves taking into account the following characteristics:

- the probability of materialization of the risk is determined by the fact that, at a certain moment, in carrying out the activities, there may be conditions that favor the occurrence of the risk. Under these conditions, the analysis of the causes that favored the appearance of the risk can lead to an appreciation of the chances of its materialization;

- the impact of the risk on the objectives, represents the consequence of the materialization of the risk, respectively how the achievement of the objective is affected by the risk that has manifested itself.

8. Risk control and monitoring

Risk control is the policies, procedures, controls and other practices established by the organization's management for prudent risk management, as well as for ensuring the performance of activities as provided. Also, the purpose of risk control is to ensure the management of the institution that the set objectives are met and the significant risks are properly managed.

The management of the institution, depending on the risk assessment, will establish the risk response. In order to avoid conflicts, it is advisable to ensure an independence of risk control from the functional structures of the organization performing the activities in which the risk is identified. Any measures taken to control the risks must be included in the well-known "internal control system", for which the management of the organization is responsible for implementation.

Risk control assumes that, at the level of the functional structure where the risk exists, the continuous monitoring of the risks and the appropriate attenuation of the probability of materialization or of the risk impact are performed. Otherwise, the risks are uncontrollable and there are no ways to intervene to limit the likelihood and impact of the risk. Risk monitoring involves reviewing them and monitoring whether the risk profile changes as a result of the implementation of internal control instruments.

Review processes are implemented to examine whether: the risks persist; new risks have arisen; the impact and likelihood of risks have changed; the internal control instruments put in place are effective or certain risks need to be redefined.

Risk monitoring involves following the knowledge of the strategies applied for risk management, the ways of their implementation and the evaluation of the performances obtained after the implementation.

Risk sensitive areas are continuously monitored and the results are transmitted at the initial stage in order to re-evaluate, identify and implement appropriate internal control tools or apply other means to reduce risk exposure.

Delays in dealing with risk can diminish the chances of effective risk management in the future. Therefore, the application of the permanent risk monitoring strategy must be preceded by a serious analysis of the duration of the implementation of risk management measures.

If this duration is long, it is preferable that the time of onset of risk management is not delayed. Such an analysis must be subject to risks with a low probability of occurrence, but with a high impact if the affected objectives are of a strategic nature.

References

Internal Managerial Control, Romanian Government's General Secretariat. https://sgg.gov.ro/.

Spencer Pickett, K. H. (2006). *The Internal Auditing Handbook*, Second Edition. John Wiley & Sons, III, River Street, Hoboken, NY USA.

OSGG 600/ 2018 - Code of Internal Control, approved by the O.S.G.G. no.600 / 2018. The government secretary published: Oficial Monitory no. 387 / 7 mai 2018.