PREVENTION OF COMPANY RISKS

SUCIU GHEORGHE
Associate professor, "Dimitrie Cantemir" Christian University Braşov, Romania,
ucdc.suciu.g@gmail.com

TRIFAN ADRIAN
Associate professor, University Transilvania from Braşov, Romania, adrian.trifan @unitbv.ro

Abstract: *A company's manager has to create and maintain a healthy internal control system. An efficient internal control system implies the implementation in the company of risk management. Each company, but also each individual, who tries to attain certain objectives, establishes the activities which lead to the achievement of goals and, at the same time, tries to identify as many "threats" as possible, in order to take the necessary measures to eliminate them. Thus, even if one is not familiar with the concepts of risk and risk management, one acts, consciously or not, for that purpose.*

Key words: *risk, risk exposure, risk management, risk tolerance.*
JEL classification: *G32*

1. Introduction and context of the study

This article aims to provide new insights into the identification, control, monitoring and reporting of risks. Even if one takes all the necessary measures, risks cannot be fully eliminated, but some can be influenced positively. Risks must be identified by looking first at the management's objectives. Risks are acceptable, if the measures that try to avoid them are not justifiable in the financial plan. Significant risks appear and develop because of an inappropriate management of the rate between the company and the environment in which it acts or of some excessively centralized management system. This work is a result of scientific research, based on the analysis of literature and legal regulations regarding company risks.

2. Risk management

Risk management refers to ensuring a global control of risk, which allows maintaining an acceptable level of risk exposure, with minimum costs.

Risk management is tightly related to the internal control system. Internal control is conceived and put into practice by the shareholders, executive leadership and other employees in order to give a reasonable insurance about the achievement of the established goals. According to the International Audit Standards, an **internal control system** has the following components:

- ✓ Control environment;
- ✓ The process of risk evaluation by the company;
- ✓ The informational system, including the related activity processes, relevant for communication and financial reporting;
- ✓ Control activities;
- ✓ Controls' monitoring.

Risk can be defined as a problem (situation, event) which had not occurred yet, but which might occur in the future, which would threaten the achievement of the established results. Risk represents an uncertainty in obtaining the desired results and must be seen as a combination between probability and impact.

The probability of risk materialization shows the possibility or eventuality of a risk to materialize. It represents a measure of risk occurrence probability, determined by appreciation or by quantification, when the risk's nature and available information allow such an evaluation.

The impact represents the consequences on the results, in case the risk materializes.

Risk exposure signifies the consequences, as a combination of probability and impact that an organization can experience in relation to the pre-established objectives, in case the risk materializes.

Risk materialization represents the transposing of risk from the domain of uncertainty to the certainty one. The materialized risk is transformed from a possible problem into a difficult problem, in case the risk represents a threat, or in a favourable situation, if the risk represents an opportunity.

Risk attenuation shows the measures taken to diminish the probability of the occurrence of risk and/or to diminish the impact on the results (objectives), if the risk materializes.

Risk evaluation represents the evaluation of the consequences of risk materialization, in combination with the evaluation of probabilities of risk materialization.

Risk profile analyses the specific range of risks with which the company is confronted.

Risk strategy represents the general approach of the organization towards risks. It must be documented and easily accessible in the organization.

Risk tolerance represents the "quantity" of risk that the organization can tolerate or to which it is willing to be exposed to at a certain point.

Inherent risk shows the exposure to a certain risk, before any measure to attenuate it is taken.

Residual risk (control risk) shows the exposure caused by a certain risk, after taking measures to attenuate it. The measures to attenuate risks are part of the internal control. Because of this, residual risk is a measure of the internal control's efficiency.

Risk administration (according to the Francophone literature) or risk management (according to the Anglo-Saxon literature) encompasses all the processes related to the identification, evaluation and assessment of risks, establishing responsibilities, taking measures to attenuate or anticipate them, periodical revision and monitoring progress.

In public entities, risk management is implemented through the Order no. 946/2005 of the Ministry of Public Finance. Thus, the public entity analyses systematically, at least once a year, the risks related to its activities, elaborates corresponding plans to limit the possible consequences of these risks and nominates the employees who will be responsible with the implementation of these plans. Any action or lack of action represents a risk of not achieving the objectives.

Risk management can be characterized through the following **features**:

a) Risk management promotes action and forecast

Management must identify the possible threats, before they materialize and produce unfavourable consequences on the established objectives. Risk management is based on the principle "it is better to prevent, than to ascertain a fait accompli". The managers of an organization should not confine themselves to only deal with the consequences of some events that have already occurred. Managers should adopt a reactive management style, which means that they should implement measures to attenuate the risk manifestation.

b) Risk management facilitates to attain in an efficient and effective way the organization's objectives

Knowing the threats allows one to group them according to how likely it is for them to materialize, and also according to their impact on the objectives and the costs of the measures meant to reduce the likelihood of their occurrence or to limit the undesired effects. The measures taken by the entity must take into consideration the correlation "cost-benefit" or "effort-effect".

c) Risk management ensures the basic conditions for a healthy internal control

A healthy internal control implies the existence of risk management. The activities which must be done to attain the objectives must be completed by measures meant to reduce the risks and by ways to react in case of difficult situations. If one wants to consolidate internal control, risk management must be implemented. In risk management, the models or techniques are not the most important, but the attitude towards risk is.

3. Risk evaluation

Risk evaluation is an activity which aims to define the objectives and conditions which must be taken into account, keeping in mind the dynamics of the factors that influence the activities and the processes of an entity. The company operates in the context of factors that are specific to the sector of activity that it is a part of, regulation factors and other internal and external factors. In order to react to these factors, the entity's management defines the **objectives**, which represent the entity's general plans. Just like the external environment changes, in the same manner the operations of the entity are dynamic, and its strategies and objectives change in time. An efficient risk management is a constant preoccupation of the administration, and it implies that it knows where the risk might occur in the entity.

When doing risk evaluation, one must take into consideration the following aspects:

- If the risk is a fraud risk;
- If the risk is related to recent economic, accounting or other evolution;
- The transactions' complexity;
- If the risk implies transactions with affiliated parties;
- The degree of subjectivity in the evaluation of information;
- The accounting principles used for the accounting estimates;
- If the risk implies significant transactions for the entity.

In case of entities with complex structures and which have a high number of employees, there should be a **risk department**.

Risks do not disappear completely not even after implementing an internal control. Uncertainty cannot be eliminated, it can only be controlled. Each entity should implement a system of internal control for managing risks up to a level considered acceptable. Residual risk (what remained of the inherent risk as a result of a good functioning of the internal control) must be situated in the risk tolerance.

A model of risk management has 4 components:

A) Identifying the risks;
B) Evaluating of risks;
C) Controlling and monitoring the risks;
D) Reviewing and reporting the risks.

A) **Identifying the risks** is the first step in risk management. Risks are related to the entity's objectives. If objectives are not clearly identified, the risks will not be clearly identified either. An identified risk can be related to more than one objective in the organization, and its impact can vary depending on the objective. Risks should be identified permanently, not only at the beginning of the company's operations.

Risk is a problem (situation, event) which can appear, but which has not appeared yet. Risk is a possibility, not a fact. Risks are situations, probable events which would have consequences on the objectives, if they materialized. A lack in the entity's management is not a risk, but a certainty. If the internal control system had worked very well, then there wouldn't have been a lack in management. Because there are no two identical entities, risks are specific to each entity and cannot be generalized to all the companies.

Inherent risk is a specific risk which is related to the achievement of the objective, without intervention through measures meant to attenuate risk (internal control).

Residual risk is the risk that remains after implementing the measures to attenuate inherent risks. Residual risk is a consequence of the fact that inherent risks cannot be totally controlled. The magnitude of the measures taken to control the inherent risk is limited, because the resources that can be possibly used are themselves limited.

The identification of risks can be done through **2 methods**: self-evaluation of risks and appointing a team external to the entity. **Self-evaluation** has as an advantage the fact that the internal group knows much better the problems that the company is confronted with when wanting to attain its objectives. The disadvantage is that being involved directly in the activity, the subjectivity in perceiving the risks is a lot higher. **Appointing an external team** to analyze all the operations and activities in the organization has the advantage of correlating risks on multiple levels and ignoring subjectivism. The disadvantage is that certain risks, seemingly unimportant, can be ignored.

B) Risk evaluation implies the evaluation of the probabilities of materialization of risks and the impact on the objectives, in case in does materialize.

Risk evaluation means following the following **stages**:

a. evaluation of the probability of materialization of the identified risk; for example, if from 200 verified invoices, one notices that 5 have been filled out wrong, the accounting risks will be at 10%; the probability of risk materialization can be grouped into 3 levels: low, medium and high;

b. evaluation of the impact on the objectives, in case the risk materializes; impact can have only a single value component, but in some cases other components might appear (deterioration of the work climate, delays in the performance of the assigned tasks, unfaithful financial pictures); impact can be grouped into 3 levels: low, medium and high;

c. evaluation of risk exposure as a combination between probability and impact; risk exposure is a probabilistic concept, because it expresses a combination between probability and impact.

Risk exposure (E) can be established according to the formula:

$$\mathbf{E = P \times I}$$

where: P = probability of risk occurrence;

I = impact on the objectives, if the risk occurs.

If the organization adopted three-step scales to evaluate the probabilities and the impact, the scale to evaluate the risk exposure would have 9 values (3 x 3). It can be represented as follows [8]:

		PROBABILITY		
		LOW	**MEDIUM**	**HIGH**
IMPACT	**LOW**	**L x L**	**M x L**	**H x L**
	MEDIUM	**L x M**	**M x M**	**H x M**
	HIGH	**L x H**	**M x H**	**H x H**

If the scales are numbered as: low = 1, medium = 2 and high = 3, the evaluation of risk exposure will have the following values:

		PROBABILITY		
		LOW = 1	MEDIUM = 2	HIGH = 3
IMPACT	LOW = 1	1	2	3
	MEDIUM = 2	2	4	6
	HIGH = 3	3	6	9

According to this scale, we can interpret the data as follows:

- A low exposure for the values 1 and 2;
- A medium exposure for the values 3 and 4;
- A high exposure for the values 6 ad 9.

C) Risk control implies the attenuation of the materialization probability or of the impact in case the risk materializes or of both. Risks cannot be controlled if the organization does not have the possibility to intervene directly to attenuate the probability and/or impact (risks due to the external environment). Managers can adopt the following **alternative strategies** as a response to the entity's risks:

a) Accepting (tolerating) the risks. This implies taking no measures to control risks and it is adequate for inherent risks whose exposure is lower than the risk tolerance (the costs related to control measures are higher than the benefits).

b) Permanently monitoring the risks means accepting the risk and constantly monitoring it. The supervised parameter is the probability, because the monitoring strategy is applied in case of risks with a significant impact, but with a low probability of appearance.

c) Avoiding risks means eliminating the activities that generate risks.

d) Transferring (externalizing) risks means entrusting the risk management to a third party who has the necessary expertise to manage that risk, and signing a contract to this end. By using this strategy the company wants, on the one hand, to diminish the organization's exposure and on the other hand, to manage the risk in an efficient manner by a specialized third party. This option is suited especially in case of financial and patrimonial risks (for example insurance contracts).

e) Treating (attenuating) risks is the most frequently used approach for the majority of the risks in an organization. The option of attenuating the risks means that the company will continue to carry on activities which generate risks, but it will take measures (implements internal control instruments) in order to keep the risks at acceptable levels. Attenuating risks can be done by using procedures. Many risks are caused by the lack of procedures.

Procedures are those instruments of internal control through which the risks generated by the unawareness of processes and rules are controlled. To work without formalizing the way in which each must proceed, means that there is no efficient internal control, which is meant to keep under control the risks and thus to obtain a reasonable assurance that the objectives will be met. For example, the lack of formalized procedures for the circuit of the relevant supporting documents might lead to the risk that other people than those authorized will approve them, this possibly leading to frauds in the company's management.

In order for the procedures to become efficient internal control instruments, they must abide by certain **requirements**:

- To refer to all the important processes and activities;
- To be written;
- To be permanently updated;
- To be acquainted to the implementers;
- To be simple and easy to comprehend.

The information system is the group of devices used in internal control, operationalized as a result of the measures taken to make an information system that is complete, reliable, exhaustive (to contain all relevant information), pertinent and useful (which satisfies the decision making necessities), opportune (to provide the information when it is necessary) and non redundant (useless overflow of provided data).

Supervising groups the instruments (devices) of internal control, meant to keep under control the risks that are a result of the anomalies in the exercise of hierarchical control. To supervise does not mean doing the work of the subordinates, to seek for errors at all costs or to supervise permanently the processes. To supervise means, first of all, to coach (coordinate), to encourage and only lastly, to check.

All the identified risks must be included in a registry of risks, which will have the following structure:

Registry of risks

Risk zone (domain, compartments)	Objectives	Description of risks	Causes of risks	People responsible for risk management
1	2	3	4	5

Inherent risks				Instruments of internal control
Probability	Impact	Exposures	Adopted strategy	
6	7	8	9	10

Residual risks			Possible secondary risks	Observations
Probability	Impact	Exposures		
11	12	13	14	15

D) Revision and reporting of risks. The revision processes must be put into effect to analyze if: the risks persist; new risks appear; the impact and probability of risks have modified; the instruments of internal control put into practice are efficient; certain risks must be escalated to higher management levels. The results of the revisions must be reported in order to ensure a continuous monitoring of the risks' situation and to notice the major changes that impose the modification of priorities.

4. Conclusions

Risk evaluation at the level of a company's financial management is a complex demarche, because of the multiple ways to determine the risk, the diversity of sources and risk factors. Risk management contains a wide range of activities, strictly defined and organized, starting from the entity's conditions of existence and fundamental objectives, and also the analysis of risk factors in an optimal and efficient functioning conception.

When evaluating risks, one should always start from the entity's objectives. There is a cause for each risk and an effect in case it materializes. The effect is the impact. The cause is a situation which exists and which favours the appearance of risk. The management must always keep in mind the risk exposure, which is influenced by the probability of appearance and impact if the risk materializes.

5. Bibliography

[1] **Bârsan Pipu-N., Popescu I.**- *Managementul riscului. Concepte, metode, aplicaţii*, Transilvania University's Publishing House, Braşov, 2003;

[2] **Brealey R., Myers S.,** - *Principles of corporate finance*, 7th Edition, McGraw-Hill/Irwin Series in Finance, Insurance, and Real Estate, Boston, 2003;

[3] **Denzil Watson and Antony Head,** *Corporate Finance, Principles & Practice,* fourth edition, Sheffield Hallam University, 2007;

[4] **Dragotă V., Obreja Braşoveanu L., Dragotă I.M.,** - *Management financiar, ediţia a doua, Vol I, Diagnosticul financiar al companiei*, Editura Economică, Bucharest, 2012;

[5] **Ross S., Westerfield R., Jaffe J.** – *Corporate finance*, 8th edition, Ed. McGraw – Hill/Irwin, 2008;

[6] **Stancu I., Stancu D.**, *Finanţe corporative cu Excel*, Editura Economică, Bucharest, 2012;

[7] **Suciu G.** – *Diagnostic financiar*, Editura Universitară, Bucharest, 2013;

[8] *** www.fonduri-ue.ro, Elaborarea analizei de risc în cadrul analizei cost-beneficiu a proiectelor finanţate din FEDR şi FC, january 2012;

[9] *** Ministerul Finanţelor Publice, Metodologie de implementare a standardului de control intern „Managementul riscurilor", Bucharest, 2007.