sciendo

Proceedings of the 5th International Conference on Economics and Social Sciences (2022), ISSN 2704-6524, pp. 722-730

The 5th International Conference on Economics and Social Sciences
Fostering recovery through metaverse business modelling
June 16-17, 2022
Bucharest University of Economic Studies, Romania

Importance of Information in the Risk Management Process

Anca BĂNDOI[1], Costinel Cristian MILITARU[2],
Mariana Paraschiva OLARU (STAICU)[3], Alina Mădălina BELU[4*]

DOI: 10.24789788367405072-068

Abstract

Risk management is a systematic process for optimizing resources in accordance with the organizational policy of risk management. In the risk management process, information on potential risks should be documented and structured, thus facilitating decision-making for their proper treatment. Risk management must be integrated into day-to-day activities through defined roles and responsibilities in all areas of activity. The identification, analysis, and evaluation of risks must be reviewed periodically or when the situation requires it: when changing the business model of the organization, at any adjustment of the organizational structure and activities or working procedures within the organization, when changing information processing technologies, to major changes in the system, following incidents, following the application of risk controls. Risk management helps to include risk management issues in management practices and to make decisions throughout the life cycle of activities. Risk management can help maximize overall results, if carried out in an integrated manner, in areas such as: controlling the consequences of operational risks generated by information systems; management, costs, and planning of information systems activities. The main objective of the study is to analyze the information related to the main risk assessment methods and to manage the risk management process.

Keywords: information, risk, management, objectives, evaluation.

JEL Classification: M15.

1. Introduction

All economic organizations, no matter how big or small, face internal and external factors that create uncertainties about their ability to achieve their own goals. The effect of this uncertainty is the risk, which is inherent in all activities. The reduction of barriers and accelerated technical progress lead to major developments

[1] University of Craiova, Craiova, Romania, anca.bandoi01@yahoo.com.
[2] University of Craiova, Craiova, Romania, cristianmilitaru2005@gmail.com.
[3] University of Craiova, Craiova, Romania, mariana.staicu@icloud.com.
[4] University of Craiova, Craiova, Romania, alina.bbelu@gmail.com.
* Corresponding author.

in terms of security and stability of systems. In addition, in such a dynamic world, where the degree of uncertainty is constantly increasing, risk management associated with the activities of organizations requires a good knowledge of the context through timely and good quality information. The success of organizations operating in different areas of economic and social life depends on the ability of managers to know the environment in which they operate, but also anticipate future events, based on the analysis of present information. Information is the sector that is getting increasingly important. There is a tendency to move sources from the area of productive activities to the sphere of use of intelligence.

Risk management must operate in a management structure that provides the fundamentals and organizational arrangements that will incorporate it throughout the organization at all levels. The risk management structure helps the organization manage risks effectively, by applying the risk management process, at different levels and in specific organizational contexts. Risk management, as an important component of strategic management, is intended to address the appropriate risk response, using various methods and analytical and operational means to identify, prioritize, and adopt appropriate measures to avoid losses and achieve the organization's objectives. At the strategic level, it is important for the manager to identify, through intelligence analysis, the potential risks to which the organization is exposed, so that the decision achieves the intended purpose. The correct evaluation of the context, the realization of the appropriate scenarios, and the prediction of the result that will be obtained following the decision constitute the main performance criterion according to which it should be evaluated.

The process of risk identification is the initial stage in the risk management process. Its goal is to identify all potential sources of risk in order to remove or lessen the likelihood of their occurring, as well as the impacts or impact they may have. The risk is related to uncertainty and is associated with a probability of materialization. The risk is not certain and does not refer to a difficult problem that has already materialized. Risks must be identified and managed at any level where it is perceived that there may be consequences in relation to the achievement of the organization's objectives.

Risk management is an important means by which an efficient internal management control system is implemented. Risk management includes identifying and assessing risks, as well as identifying and implementing risk responses in order to reduce the likelihood of risks materializing, as well as the consequences that come from the materialization of risks. Risk identification is a continuous activity that allows the company to relate to the process of change and adaptation, according to effective risk management.

Each employee must understand the value and importance of the risk management process in the current activity, as well as the ramifications it may have on accomplishing the organization's goals. In order to manage risk effectively and to avoid an excessive and uncontrolled volume of risks, it is important that any organization manages the risks that really affect its objectives. It is necessary to provide an information framework to make known to all staff the risk management

process by creating a section on the organization's intranet in which experiences are learned and communicated to those who can benefit from them.

The risk management process has a special importance and a high impact on the achievement of the objectives of any organization and requires adequate protection regarding the access and provision of information to unauthorized persons from the external environment.

2. Problem Statement

In the process of identifying risks, the objectives and activities that contribute to their realization are always taken into account. For a proper identification of risks, it is absolutely necessary to have a document, containing the objectives assumed at the level of the organization (Fayol, 2005). This can be a management plan, a strategic plan that includes general objectives, and specific objectives, activities that contribute to achieving the objectives (Hull, 2006). Each organization must define its general objectives in close accordance with the mission of the organization, the achievement of which is carried out in conditions of efficiency, effectiveness, and economy (Sims, Bias, 2019).

After identifying the objectives and related activities, we will move on to the next stage, identifying vulnerabilities (internal / organizational weaknesses, which may cause risks) and threats (coming from outside the organization). The number of hazards rises in direct proportion to the organization's complexity and the number of operations carried out to attain the goals (Jorion, 2011). Risks need to be identified at all levels, where it is perceived that there are consequences for achieving the objectives and problem-solving measures can be taken. An identified risk can impact several objectives of the organization with different degrees of impact.

Depending on the degree of maturity of the organization, risk identification can be in one of two phases (Penza, Bansal, 2000):

1) Risk identification in the initial phase – specific to newly established organizations, without a history in terms of risk management or without a very well developed risk management;
2) Permanent risk identification – specific to organizations that have developed a coherent and consolidated system of internal managerial control and implicit risk management.

Risk identification is not a strictly objective process but depends very much on the perception of those involved. The identified risks must be grouped; the grouping of risks is done according to the perception and needs of the organization. Risk grouping in an organization (risk exposure) leads to its risk profile (Saunders, 2019). It is unique from the perspective of the objectives, the activities carried out, and the general context. Risk identification and assessment is a specific attribute of each organization. The risk profile provides an overview, including the general, documented, and prioritized assessment of the range of specific risks facing the organization (Down, 2012). The impact of risks on the objectives is not what defines them. Impact is a result of how the materialization of a risk affects those objectives,

not a risk. The main factors that can influence the external risk environment and that each organization must take into account are (Holton, 2013):

- Laws and regulations – each organization must identify those laws and regulations, based on which they operate and which define the limits of action of the organization;
- Modification / updating of the objectives of the management program - in some situations, the treatment of some risks by the managers is influenced by the financial decisions;
- Sometimes, the decrease of capital – affects the attraction / maintenance / facilitation of staff training courses.

An important role in the risk management process is the risk assessment. The risk assessment is performed following a type of risk response in an order of priority and represents the subsequent stage of risk identification. The process of risk assessment stages (Saunders, 2019):

- calculating the likelihood of dangers materializing;
- evaluating the impact on objectives/activities in the event of risk materialization;
- risk exposure assessment – probability and impact in combination.

The purpose of risk assessment consists in: establishing a hierarchy of identified risks and, depending on risk tolerance, establishing the most appropriate risk management measures (Greene, 2020). Risk tolerance is the amount of risk that an organization is prepared to tolerate or is willing to expose at some point in situations where risk may be an opportunity or threat (Greuning, Bratanovic, 2004). Once the risks have been discovered and assessed, as well as the tolerance level, the type of risk response for each risk must be determined (strategy adopted). In this way, it is determined whether risks can be managed or not.

The response to the question: Why is risk management necessary? is the decision-making dilemma from which we begin our study strategy. As a result, the goal of this article is to examine information on the most common risk assessment methodologies and how to effectively manage the risk management process.

3. Aims of the Research

The research's goal is to analyze information on the main methods of risk assessment and the management approach that corresponds to the risk management process. Several evaluation methodologies were highlighted in the analysis of the firms that were the topic of the research study, providing a foundation for a more in-depth examination of the risk management concept:

1) MEHARI Method (MEthode Harmonisee d`Analyse de Risques Informatique): covers the phases corresponding to the identification, estimation, respectively, treatment, or acceptance of the risk. The method applies both qualitative and quantitative tools, using a database of risk situations that the analyzed system may face. Methodological support is a computer application that allows calculations, simulations, and optimizations.
2) The method of risk matrices: Predominantly quantitative, it analyzes separately the four basic components of the critical infrastructure: physical, functional

(procedural), informational, and human (serving staff). It operates with the model of the relationship between the threats-vulnerabilities pairs, based on which the risk matrix is built.

3) OCTAVE method (Operationally Critical Threat, Asset and Vulnerability Evaluation): addresses both organizational and technological issues, necessary to ensure the security of critical infrastructure, in a continuous evaluation process. OCTAVE as the probability of occurring a loss caused by the absence or inadequacy of prevention methods, and the implementation of the Security Plan as a protection strategy, through control over assets or processes, in the form of a list of mandatory activities.
4) VAR method: it is a mixed method, both qualitative and quantitative risk assessment. It starts by identifying the most drastic effects that the production of security risks could have on the organization.

The data was collected using a questionnaire, which is a quantitatively organized research method, between November 2020 and February 2021. A total of 523 valid questionnaires were obtained, with each questionnaire taking about 20 minutes to complete. The research study involved company managers from four fields of activity in Romania: IT, energy, automotive, production.

4. Research Methods

The multicriteria decision-making processes that we used in the research of the maximum utility technique pose challenges of supporting economic decision-making in the modeled socio-economic universe (Morgan, 2020).

The procedures for imitating the rational mode of decision-making are, in more or less elaborate forms, the conceptual essence of models. Modeling aims to make the most of the information base scientifically, and procedures for imitating the rational mode of decision-making are, in more or less elaborate forms, the conceptual essence of models. The global utility method's steps are as follows (Morgan, 2020):

Step 1. Create a utility matrix using elements, i = 1, ..., r and j = 1, ..., n.

The equation is used to calculate each element of the matrix for the maximum criterion:

$$x_{ij} = u_{ij} = \frac{x_{ij} - x_{i\min}}{x_{i\max} - x_{i\min}} \quad (1)$$

and for each minimal requirement with expression:

$$x_{ij} = u_{ij} = \frac{x_{i\max} - x_{ij}}{x_{i\max} - x_{i\min}} \quad (2)$$

where:

x_{ij} = the value of indicator *i* associated with indicator *j*;

$x_{i\max}$ = the minimum value of indicator *i*;

$x_{i\min}$ = the maximum value of the indicator *i*.

Step 2. Calculate the overall utility for each project as the sum of the products in the utility matrix element (the project's column vector) and the important coefficient for each indicator.

$$UG_j = \sum_{i=1}^{r} \alpha_i u_{ij}, where \sum_{i=1}^{r} \alpha_i = 1 \quad (3)$$

Step 3. Choose the project that corresponds to the maximum global utility.

$$\max\{UG_j\} \Rightarrow V_j \quad j = 1, ...,n \quad (4)$$

For the division of some choice Vi variations (n variant) and the selection of the best one by considering many criteria of appreciation (Cj, j = 1, ..., n) and the global utility at the same time. The multi-attribute problem is about finding the best mix of traits (variant characteristics).

This entails converting all numerical quantities a_{ij} (in related units of measure) and qualitative features into utilities u_{ij}, i.e., numerical values in the range [0, 1]. The independence of the criterion is a fundamental assumption in the weighted sum method's correct function. The optimal option is indicated by the greatest of the synthesis utilities.

5. Findings

Table 1 presents the informational basis of the study, respectively, the share of importance that managers give to each method of risk assessment.

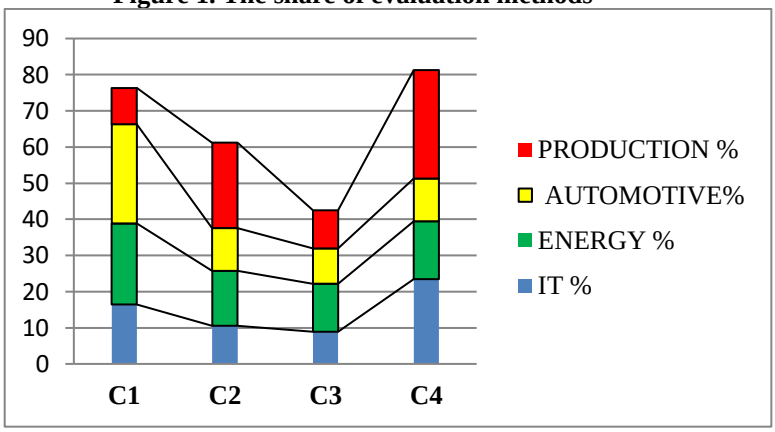
Table 1. Importance of evaluation methods related to the field of activity

MODELS OF RISK ASSESSMENT	**FIELD OF ACTIVITY**			
	IT % (v1)	**ENERGY % (v2)**	**AUTOMOTIVE % (v3)**	**PRODUCTION % (v4)**
MEHARI method C_1	16.45	22.35	27.50	12.50
Risk matrix method C_2	10.55	15.15	11.90	23.61
OCTAVE method C_3	8.90	13.25	9.80	10.54
VAR method C_4	23.45	16.00	11.82	23.55

Source: Based on the information gathered by the authors.

The resulting results indicate that managers first take into account the VAR (C4) valuation method - its ultimate goal being to achieve an optimal balance between the assumed level of risks and the expenses necessary to minimize them, and in the last instance managers take into account the OCTAVE Method (C3) – Figure 1.

Figure 1. The share of evaluation methods



Source: Based on the information gathered by the authors.

Going through the calculation algorithm involved:
Step 1 – building the unit matrix with the elements x_{ij} Figure 2.

Figure 2. The matrix of units

$$\begin{bmatrix} 0.26 & 0,66 & 1,00 & 0,00 \\ 1,00 & 0,65 & 0,90 & 0,00 \\ 0,00 & 1,00 & 0,21 & 0,38 \\ 0,99 & 0,36 & 0,00 & 1,00 \end{bmatrix}$$

Source: Based on the information gathered by the authors.

Step 2 – Calculation of global utilities for each field of activity (Tabel 2):

Table 2. Results of the calculation of global units

GLOBAL UTILITY	RESULT
IT	2.25
ENERGY	2.66
AUTOMOTIVE	2.10
PRODUCTION	1.38

Source: Based on the information gathered by the authors.

Step 3 – Table 2 shows the calculation of global utilities, the highest global utility of companies in the field of ENERGY.

As a result of using the formula for calculating the maximum global utilities technique, it can be determined that ENERGY firms have the best understanding of risk management.

6. Conclusions

In today's organization, you have to take responsibility for information because it is your main working tool. But most do not know how to use it. Few know how to interpret information. In most cases, managers ignore the risk management process, as well as the risks associated with the security of the organization. In general, activities that are not directly quantifiable and for which a level of profit generated cannot be directly presented, tend to be ignored by senior management, which is why risk management activities require awareness-raising, both among the managers of the organization and at the level of employees. There is also a fear that these projects will highlight inconsistencies and shortcomings in the management of the security system. Although a high level of security may seem costly, the lack of adequate security will certainly prove catastrophic in the long run for the organization.

In this sense, we propose some rules associated with risk identification:

- the difficult problems that have already materialized should not be ignored - these can be potential risks in the future, if the organization acts in the same circumstances;
- those problems that will surely materialize, should not be identified as risks. These are not risks, but certainties. Certainties are managed and usually involve resource allocations, changes in objectives, changes in strategy;
- risks have a cause and effect; there is a cause and effect of the materialization of risk. The cause is a favorable context for the occurrence of the risk. The effect is the impact of the materialization of the risk;
- a distinction must be made between inherent risk and residual risk. The inherent risk is the specific risk, related to the achievement of the objective, without risk management measures being taken, while the residual risk is that risk that remains after the risk response has been established and implemented. Residual risk is the expression of the fact that the inherent risks cannot be fully controlled. No matter how much action is taken, uncertainty cannot be removed.

Regardless of the method used, the information on risk management control measures must ensure an acceptable level of risk, so that it is within the accepted tolerance limit. The process of managing information related to risk management requires the involvement of all employees, both those with management positions and those with executive responsibilities, by establishing clear responsibilities at the level of all organizational and decision-making structures. In the risk information management process, both management and executive staff must:

- understands how and how the risks affect the organization (identification of the risk and its evaluation);
- obtains information about risks – the sources and factors that generate it;
- allocate adequate resources for risk management;
- analyze the effects of risks by assigning responsibilities;
- disseminate good practices and inform all departments about the possibilities for risk reduction.

For the efficient management of the risk management process, it is necessary to have:

a) a structure with attributions in risk management;
b) a risk management officer at the level of each department at the first management level (risk manager);
c) a system procedure regarding risk management.

A broad response to the topic of why risk management is required. It is triggered by the realization that there are uncertainties regarding the nature of the threats to attaining the objectives, as well as the nature of the opportunities, in both the organization and the environment in which it operates. Any manager must deal with the issue of managing threats, because failing to meet their objectives would disqualify them, or failing to take advantage of chances for the benefit of the firm would demonstrate their efficiency. If uncertainty is a constant companion, then how we respond to it must also be a constant concern.

In conclusion, a risk analysis on the information used cannot completely eliminate the risk, but can give the management of an organization the ability to:

1) decide whether or not the risk is acceptable;
2) knows the consequences of the decision, both positive and negative;
3) reduce risks through control measures.

References

[1] Down, K. (2012). *Measuring Market Risk*. Chichester: John Wiley of Sons.

[2] Fayol, H. (2005). General and Industrial Management. London: Pitman.

[3] Greene, R. (2020). *Strategic Talent Management: Creating the Right Workforce*. London: Routledge.

[4] Greuning, H., Bratanovic, J. (2004). *Analyzing and Managing Banking Risk, A Framework for Assessing Corporate Governance and Financial Risk*. Bucharest: Irecson.

[5] Holton, G. (2013). *Value-at-risk: theory and practice*. Massachusetts: Academic Press.

[6] Hull, J. (2006). *Risk Management and Financial Institutions*. Chichester: John Wiley & Sons.

[7] Jorion, P. (2011). *Value-at-Risk: the New Benchmark for Controlling Market Risk*. Pennsylvania: McGraw-Hill.

[8] Morgan, J. (2020). Mathematical Methods. London: John Catt Educational.

[9] Penza, P., Bansal, V. (2000). *Measuring Market Risk with Value at Risk.* Chichester: John Wiley & Sons.

[10] Saunders, A. (2019). *Credit risk measurement: New approaches to value at risk and other paradigms*. Chichester: John Wiley & Sons.

[11] Sims, R., Bias, S. (2019). *Human Resources Management Issues, Challenges and Trends: Now and Around the Corner*. Charlotte: IAP.