OPERATIONAL RISK MANAGEMENT AND MONITORING

Ion CROITORU, PhD
„Athenaeum" University of Bucharest, Romania,
E-mail: ion.croitoru.ag@gmail.com

Abstract

A major concern for every organization is to identify the risks they face. Thus, all risks associated objectives, activities or actions taken should be identified and recorded. Although there is a risk management model applicable to all organizations, this activity should be a primary concern of the management, risk manifestation otherwise lead to damage to achieve the objectives.

Operational risk is the risk that the management and all staff encounters in daily and on which to exercise constant monitoring, so it does not affect the expression of the implementation of activities. This risk is related to the ongoing activities within the organization and may cause financial loss or material in case of manifestation.

Operational risk is a constant and significant in an organization and manifests about ongoing activities. Exposure to operational risk organization may have an upward or downward depending on the volume and complexity of transactions carried out, the quality and reliability of systems used internal control system implemented.

Keywords*: risk assessment, risk factors, risk management, operational risk, risk sources.*

JEL Classification: M00; M41; M42

Risk management is not a fad, but provides the basis for implementing the principles of corporate governance and shareholder organization provides a guarantee regarding the use of the resources that they have provided. By implementing risk management process management organization shall ensure that resources are used properly and effectively, yielding at least planned results.

1. Conceptual approach for operational risk

The concept of operational risk is a relatively new concept introduced in the practice of organizations in our country, initially being considered by operators in the banking system, and was later accepted and managed and the management of other economic organizations.

In the literature there is no unanimous view on the definition of operational risk, which is analyzed in terms of several aspects, namely:

- operational risks were identified initially as other forms of financial risks associated with development strategy, positioning in the environment in which the entity is or competence management;

- operational risks were associated second financial transactions or errors in the recording of entries in the system, data processing errors, errors in performing, recording outputs of system errors or errors in financial statements. In this context there is a risk that classification is specific only recording mode operations entry, processing and output of the system, do not take into account the risks of fraud intention, the execution of unauthorized transactions or inappropriate use of financial instruments in the nature of economic transactions;

- operational risks were associated third internal control system implemented by management or its non-functionality;

- finally, operational risks have been associated with direct or indirect loss resulting from improper conduct of activities, inefficient internal control measures implemented and making unauthorized personnel employed by the result of external influences or obligations.

Compared to the above, we can say that operational risk is recognized as the risk of incurring losses or of not reaching planned revenues, following actions to internal factors such as improper conduct of business, staff turnover and inadequate qualification or external factors such are changes in the economic environment, diversification needs, technology, the intention of fraud.

Operational risk is a reality in the entity and its correct approach leads to avoidance of losses and increase efficiency and effectiveness in achieving the objectives.

In practice, operational risk should be viewed both in terms of the relationship cause - event - effect and the effectiveness of controls that take place in the work.

Also, in our opinion, we believe that there must be a relationship between operational risk and the income so that the entity's management can make decisions in full knowledge of the risk level.

Operational risk is included in the category of non-systemic risks to the entity acting; its manifestation depends largely on how resources are

managed. Or the organizational changes concerning the working environment can lead to increased exposure to operational risk.

2. The responsibilities of operational risk management

Practice has shown that in some cases the manifestation of operational risk is so severe that lead to business interruption, the inability to pay or even insolvency organization. In these circumstances it is necessary that the management organization to pay particular attention to operational activities and promote best practices and to ensure effective management of operational risk.

In the process of operational risk management *corporate governance* is responsible for developing and approving strategy and management procedures specific to this risk, structures while *functional leadership* is responsible for communicating the strategy and specific procedures to all staff and to follow the implementation and compliance.

Responsible for operational risks at the level of functional structures are responsible for identifying operational risks faced, accurate and timely reporting to them and to formulate proposals to reduce the risk and monitoring activities were implemented after control measures set . Also, if the event is responsible for monitoring the risk of losses, the implementation of measures to recover losses and tracking their recovery.

Functional structure of risk management is responsible for the development of the internal management of operational risk analysis information from responsible risk and monitoring risk factors for formulating strategies, policies and measures to mitigate operational risks reported in order to prevent future these events and their communication in charge of the implementation and monitoring risk.

Internal audit structure organized in the entity is responsible for operational risk assessment during the audit, identify the causes that led to its emergence and formulate proposals to eliminate the causes and reducing its level.

Operational risk can be managed efficiently given that at the organizational level following requirements are met:

- defining strategy and corporate governance principles underlying operational risk management;
- organize and establish a corporate governance internal audit function within the organization and ensure that operational risk is a concern of this function;
- from executive management can implement policies and procedures arranged levels of corporate governance;

- risks are identified and evaluated objectives;
- risk monitoring and reporting is done objectively by corporate governance and executive management;
- managerial decision making is informed of the existence and the management of operational risk;
- the organization has defined a business continuity plan that can be applied in case of interruption;
- organization ensures transparency and provides clear and true information on their activities, quality management and operational risks faced.

To implement these requirements in operational risk management, the management entity must: (a) a work environment and culture proper operational risk; (b) implementation of appropriate measures to identify and assess the operational risk events while; (c) implementing an adequate internal control system to give priority to the organizational risk; (d) determining the levels to which operational risk is acceptable and maintaining risk within these limits; (e) operational risk anticipation for restructuring activities or change the context in which activities are performed.

Also, internal procedures developed for each of the activities carried out must provide and describe: (a) the methods and techniques used for operational risk assessment; (b) functional structures responsible for the management of operational risk; (c) the actions and tasks performed for operational risk management; (d) a circuit adequate information on the assessment, treatment and monitoring operational risk; (e) mode of action and approach used to identify if an operational risk.

The establishment of operational risk acceptance allows the entity to ensure the achievement of the objectives in terms of efficiency and effectiveness and to adequately manage situations of termination of the activity. Acceptance limits for establishing the Organization must take into account, for each risk factor that is relevant, two values: a warning value and a maximum value that can be supported, for example:

Nr. crt.	**Risk factor operational**	**Attention value**	**The maximum value supported**
1	Losses due to actions committed with the intention of fraud or breaches of regulations, laws or entity/total loss policy	5%	10%
2	Losses resulting from the destruction or damage to tangible assets in the wake of natural disasters or other events/total loss	30%	40%

3	Accounting operations share reversed/total operations	0,05%	0,15%
4	Number of days/employee participation in professional training courses during the year	3 zi	1 zile
5	False documents/records total recorded documents	0,01%	0,01%

If the achievement of the organization's leadership attention value needs to be alarmed and to order a series of measures to prevent or correct the implementation of controls in order to limit the effects of operational risk.

3. Operational risk factors

Managing operational risk must be borne by the entity's management both at the level of each functional structure and of each employee. Staff must be familiar with the operational risks, to report and monitor.

Operational risk management approach can be done from two perspectives: the causal approach process and approach. Hopefully, this approach allows the taking into account of all the activities which they carry out entity and processes involved, namely: operational process, process management and internal control and process support including legal support functions, tax, IT and logistics. The causal approach to operational risk means that the organization is considering changes in the practice of human resources management, performance indicators establish staff and the extent to which they reflect operational risk tolerance, their level of training of staff and whether it ensures the achievement of the objectives, the extent to which employees are complying with regulations, as well as a plan for business continuity.

According to the literature of the operational risk factors are characteristics:

- external fraud-related events and internal fraud;
- personnel-related events, namely the discriminatory practices imposed on personnel selection and career system of employees;
- customer-related events, and unfair practices, breaking the rules in granting the contracts or the execution of works, the preferential treatment given to certain customers;
- tangible assets-related events, namely the existence of organizational and functional problems that endanger the integrity of tangible assets;
- work related events, the lack of programmers to ensure the continuity, changes in activities and system failures;

- events related to the activities, highlighting the inadequate instructions and criteria used to record transactions and transactions made by that entity.

From the analysis of these factors shows that several are factors which have as a result work. Situation where the attention should be focused on the selection of management and implementation of controls in conjunction with the nature of the risks that lead to the minimization of operational risk.

In practice the risk factors you can structure as follows:

Nr. crt.	**Type of event**	**Associated operations**	**Risk categories**
1	Internal fraud	The intention of fraud The fraudulent appropriation of property Circumvention of the rules in force	Transactions not reported Unauthorized operations Registration of operations without the existence of supporting documents The counterfeiting of documents False reports with the intent to defraud Changing information in computer applications Operations carried out by employees in their own name
2	External fraud	Security systems	Counterfeiting of documents Unauthorized access to systems of entity The erroneous assignment of assets
3	Personal	Employment relations Job security Discrimination	Disciplinary of employees Actions contrary to the legislation relating to employment, Assigning responsibilities beyond preparing employee Staff turnover Events of discrimination
4	Customer	Compliance with the rules Unfair practices	Granting of preferential advantages for customers Erroneous conclusion of contracts Facilitating access of clients to obtain contracts The use of inadequate accounting records, nature of operation
5	Active corporal	Disasters and other events	Destruction or damage to assets Unforeseen events affecting assets Misuse of assets
6	Business disruption	Functionaries systems	Damage to equipment Misuse of programs

7	Demonstration activities	Registration operations Making payments	Recording of incorrect data entry Errors in transaction processing Accounting errors Registration of illegal operations Unauthorized access to your accounts Errors in reporting obligations Provision of inaccurate reports

4. Operational risk management

The operational risk management must become a constant concern of the leadership of the entity, in order to achieve an efficient and effective management, in consonance with the principles of corporate governance relating to performance and transparency. Development process involves many activities, such as: analysis of sources of operational risk, the assessment and treatment of operational risk and operational risk monitoring.

a. Sources of operational risk. In general, the sources of operational risk internal events, we find that relate to human resources, systems, processes, organization entity, the nature of activities or external events and organizational changes, which relate to fraud, changes in the political environment, economic or legislative framework which prevents the attainment of the objectives of the organization.

Operational risk sources associated human resource refers to the degree of concordance between the vocational qualification of employees and responsibilities specified in job descriptions, the avoidance of conflicts of interest, establishing staff duties, linking remuneration to performance indicators establish employee, staff turnover and observance of ethical conduct.

Operational risk sources associated with computerization of business processes refer to the security, accuracy and integrity of stored data, access to information, the extent to which the programs used for the fulfillment of requirements of users, the existence of continuity of business plans and the degree of compliance of computer system.

That operational risks related to the Organization's management information systems should take account of the complexity and importance of the operations carried out, the identification of gaps of information systems to current needs, as well as the appearance of unwanted results.

Also, operational risk management entity shall establish and maintain procedures for evaluation, monitoring procedures and procedures for limiting the level of risk and appropriate policies for risk management, which takes into account the types of generators of operational risk events. The practice of generating operational risk events may be fraud, the criteria used for selection and employment of staff, the practices related to the

granting of contracts, ensuring the integrity of the assets, ensuring continuity, to ensure transparency and the equal treatment of all customers, vendors and other individuals who have an interest in the entity.

b. Assessment and treatment of operational risk. Operational risk assessment, which aims to detect vulnerable operations, shall be carried out according to the probability of occurrence of the event generator losses from operational risk and the financial impact on the Organization, through a risk assessment matrix. Risk classification is done by means of a scale of risk (risk small, medium, large).

The probability of the risk matrix vertically should be described according to the specifics of your organization and the types of risk and can be great, very likely to happen; on average, is likely to spend and is more difficult to predict; small, highly unlikely to take place.

The impact on the organization describes horizontal array after the specifics of your organization and the types of risk and can be: high, major effect on operation; moderate, significant, but no major operations; low, the consequences aren't severe and any losses or financial implications are relatively low.

The tools used to assess operational risk shall take into account the following:

a) database of adverse events, including information related to the risk of losses arising from and measures for their rehabilitation;

(b) preventive measures taken for) anticipation of operational risk;

c) verification questionnaire, which includes a set of checklists are used in order to assess the degree of compliance activity relative to the operational risk management is implemented.

Risk control is carried out with the aim to transform uncertainties into an advantage for the organization, limiting the level of threats. It involves tolerating, treatment or transfer.

Operational risks toleration presupposes that they are accepted in the State in which it is not necessary to take any action.

Treatment of operational risk requires that, in the vast majority of cases the organization has management control measures to limit the risks. Thus, while the organization achieves its activities and implements a system of internal control which maintains the risk within acceptable limits. Inefficient risk treatment can lead to significant losses.

Operational risk transfer is determined by the fact that there are risks for which the best solution is to transfer them. In this situation, operational risks are transferred either to reduce exposure to risk, either because another organization is more capable or specialized in managing such risks.

For each element of risk taken into account, depending on the level of risk associated with the severity and risk classification as high risk, medium or small, the leadership has internal control measures in order to limit it and ensure that the objectives, for example:

Element of risk	**High risk**	**Environ mental risk**	**Low risk**	**The proposed measures**
Provision of public information	Providing information that is not public in nature and for which there is no authorizati on	Inadequate communica tion of information of a public character	Surface communicat ion public information	Clear definition of public information, Staff training and ensuring communication with the taxpayer
Erroneous payment of contracts	Erroneous payments for which there are no obligations	Payments on account	Smaller payments in relation to the current requirement	Visa submission of preventive control of the operations carried out before payment and actual payment.
Erroneous records	Recording of documents drawn up in fake	Misuse of accounts	Late registrations	Confirm the input documents by the Compiling of a providers instructions on using accounts

Operational risk posed by shortcomings in the organization's current activity, associated with human error, incorrect application procedures, non-compliance with legislation or other events is hard to quantify in a situation where its nature is not a financial one.

c. Monitoring of operational risk. Monitoring of operational risk requires keeping track of its classification in the threshold levels established by the policy of tolerance of the organization.

The organization must ensure that adequate information flow both vertically (in both directions, i.e. ascending/descending) and horizontally (between the functional structures) that allow the justification of the significance threshold established.

5. Conclusions

Operational risk is considered to be the risk of loss resulting from the deficiencies attributable to the procedures, people, and systems of organization and internal functioning or from external events, but which have an impact on the entity.

In general, the organization has implemented a management system for the management of the risks inherent and residual and less has been focused on identifying and managing operational risks related to the current activities being carried out.

In our opinion, we believe that every organization needs to implement a process of operational risk management in order to ensure:

- evaluation of operations and activities and to identify vulnerabilities to operational risk;
- establishment of indicators with which to be able to determine the level of acceptance of operational risk, and risk assessment can determine the position in relation to acceptable levels;
- permanent monitoring of operational risk.

Operational risk is perceived as the most recent venture, which raises new problems to its leadership. His analysis has taken into account all information sources available, including those relating to internal control.

Taking into account the complexity of the operational risk managers, the organization must ensure the existence of *a tool for evaluating the operational risk management process.* This function can be internal audit, which in accordance with the regulations in force is responsible for the provision of reasonable assurance, independent and objective on how risks are managed, control and governance. In addition, internal auditors can advise management regarding the organization and development of operational risk management, taking into account the broad vision of the entire portfolio of activities that are carried out within the organization.

Bibliography

1. Calota G., *Annual activity, the object of the internal audit in road transport,* The Publishing House SITECK, Craiova, 2011
2. Domnisoru S., Vanatoru S., *Internal control and audit-preliminary conceptual and procedural* The Publishing House Sitech, Craiova, 2008
3. Ghita M., Croitoru I., Togoe D., *Corporate governance and internal audit*, The Publishing House EuroPlus, Galati, 2010
4. Mestchian P., *Advances in Operational Risk: Firm-wide for Financial Institutions*, Second Edition, Incisive Media Ltd., London, UK, 2005
5. Popescu M., Croitoru I., Anghel F., Huduruc N. *Risk management,* International Conference on RISK MANAGEMENT, ASSESSMENT and MITIGATION (RIMA ’10), Universities Polytechnic, Bucuresti, 2010;
6. Socol A., *Accounting and banking firms,* management Economic Publishing House, Bucharest, 2005

7. Sebastian Barbulescu, *Internal audit and risk management in public institutions*, The Publishing House Mega, 2007
8. Vasile E., Croitoru I., *The Integrated System for Risk Management - Key Factor in the Management System of the Organization,* Capitol in book RISK MANAGEMENT, Editura InTech, Croatia, 2011
9. Vasile E., Croitoru I., *Risk management Considerations in Economic organizations,* Conference International Global Economy&Guvernance GEG 2014 10-12 September, Bucharest
10. Integrated Risk Management-Integrated Framework, COSO II, 2004
11. www.ec.europa.eu/internal_market/consultations/docs/2010/audit
12. www.ifac.org
13. www.cafr.ro