OPERATIONAL RISK MANAGEMENT APPROACHES WITHIN AN INVESTMENT FUND. SIF MOLDOVA CASE STUDY

Costel Ceocea
"Vasile Alecsandri" University of Bacau
costel.ceocea@ub.ro, cceocea@sifm.ro

Abstract
Operational risk management consists in the identification and measurement, as complete as possible, of these risks, so that the company to be able to establish appropriate measures to avoid, reduce, transfer or accept, consciously, the risk. The main goal is prevention. Operational risk management is a complex process which involves their identification, assessment, monitoring and management. Starting from the European legislation, SIF Moldova has developed and adapted its own operational risk management system, targeting mainly its identification and evaluation, the analysis of activities vulnerable to operational risk, the establishment of the potential risks for each type of activity, the limitation of the operational risk caused by improper data processing, the implementation of internal regulations on the prevention and discovery of facts that can generate losses. To ensure an adequate quality of operational risk management and of the activities related to their control as well as for maintaining an appropriate level of accuracy on information provided to the supervisory authority (ASF), it is essential that the investment fund to build a stable and viable database, containing information relating to extended periods, and to ensure continued maintenance of this database.

Keywords
management; operational risk; loss, fraud; error; assessment; adequacy

JEL Classification
G32

1. Main stages in the operational management risks

Operational risk management is accomplished through the following four stages:
A. Identification; B. Assessment; C. Monitoring; D. Management

A. Identification – it is defined the operational risk in company's vision, it is identified the component elements detached from other risks and it is described the generating events.
   - identification and ascertainment of real or potential losses;
   - identification of the event that generated the loss;
   - determining the type of risk manifested.

B. Assessment – in this stage there are assessed the risks identified in each structure and the risks are ranked.

C. Monitoring – as a result of identification and assessment of the risk, the structures must take all the measures to ensure the good functioning of the activity and to prevent the risk.

D. Management – in this stage it is decided the measures that must be taken for the control of the operational risk
   - it will be tried to transfer the risk to third parties (through outsourcing or by concluding an insurance)

- it will be tried to diminish the operational risk, in the sense of decreasing the frequency or their magnitude.

Generally, the frauds are more spontaneous than premeditated. They become more frequent where they are not detected from the beginning and where there are not taken the measures necessary for the prevention. Among these measures there are included:

- adequate sharing of responsibilities so that each employee to be liable only by one of the following activities: conclusion of a transaction; making a payment; registration of the transaction in the accountancy, etc. This is necessary because the frauds are committed, usually by one person;
- existence of an effective control system. Those who potentially would like to commit irregularities must be discouraged by the existence of an appropriate control system;
- careful review of the norms and security systems and the identification of the weaknesses that could represent a risk of fraud;
- communication and clear notification of the procedures that must be applied in certain situations;
- the staff must know very precisely the degree of competence and the risk they assume;
- company staff should be always aware of its responsibilities in relation to the identification and reporting of the risks, so that the own risk management to be at the basis of each daily activity for everyone
- identification at the company level of the key persons – as activity, as experience, as knowledge.
- persons who monitor risks must be independent from those who take the risks.

An often used solution in the operational risk management is the risk transfer by contracting an insurance policy for certain risk generator events. The company relies on the ability of the insurer to pay a compensation, in accordance with the contractual terms, thus, financing the coverage of some damages.

Within SIF Moldova, in accordance with the procedures on the operational risk approved by the management of the company, the structures (departments, services, activity groups):

1. **Identifies and assess the operational risk, taking into consideriation the following:**
    a. the factors of internal and external environment in which occurs the company's activities;
    b. the risk tolerance of the company;
    c. the strategic objectives of the company and the potential changes that will be implemented by the company;
    d. elements of suspicion (suspect and incident operations of internal or external fraud) that may result from the carrying out of the transcations which are specific to the activities of each structure of the company, other than those contained in the reports made by the company for the prevention and sanction of money laundering, as well as for the establishment of some measures to prevent and combat the financing of the terrorism in transactions;
    e. the regulatory framework and the internal regulations specific for the company
2. **Analyzes the company activities identified to be vulnerable to the operational risk (implicitly internal fraud), establishing the potential risks by types of activities at each company's structure**, concidering and not limited to:
    a. applying the principle of separation of powers;
    b. number, training and qualifications of the staff;
    c. mode of operation of the internal control;

d. use of information system and degree of availability of the equipment and network;
e. volume and value of the amounts carried;
f. high fluctuation of staff, its relocation, with or without ensuring in advance of its preparation in order to exercise the new responsabilities;
g. frequency of occurrence of events that generate direct or potential losses determined as the ratio between the number of cases in which internal fraud occurred within one year and the total number of cases in which internal fraud might have been occurred;
h. the size of the losses generated by each event which is operational risk generator detected by the control bodies;
i. inconsistencies in documentation (eg: contracts used in relation with the customers, derogation clauses from internal regulations and standard contracts, providing approval of legality, etc.).

3. **Acts to limit the operational risk (implicitly internal fraud) caused by faulty processing of data within each compartment, by having an internal control on all documents,** following:
   a. if these are prepared in accordance with internal regulations and if there are all the authorized signatures;
   b. reality of the data and accuracy of the calculations, legality of the operation, existence of the available funds in account, indicating the correct account for performing the operation, etc.
4. **Implements, in order to prevent and detect acts that can generate / generated material or monetary damages, internal regulations on the verification and guidance, which follow the application of the legal provisions in force and internal regulations** with regards to:
   a. correct preparation and registration of documents for opening current and deposit accounts;
   b. mode of exercising the control of operations;
   c. implements a system of internal control through an appropriate separation of duties by generating dual control, in order to prevent the conflicts of interest and internal fraud.

2. Operational risk management

The loss due to operational risk events represents the negative change in company's revenues, in the company's asset value or in capital, as a consequence of the events due to operational risk. The defining feature of operational risk events is the requirement to take measures of management of the operational risks occured, regardless of the financial effect of those events. If the occurrence of an event of operational risk generates losses, the risk management is done after the identification of the cause / reason which led to the event of operational risk.

Operational risk management includes the following elements:

- a well defined organizational structure, with tasks and responsibilities of operational risk management, covering all the important organizational structures of the company,
- tools of identification and management of the risk,
- mechanisms that facilitate the reduction and prevention of the operational risks and of the losses identified,
- company's management information reports.

The methods and instruments of operational risk management are those processes and systems used by the company for identifying and managing the operational risk, as well

as for the determination of the operational risk level at which the company exposed. These methods and tools of management of operational risk include:

a. collection of data on losses due to the occurrence of operational risk events
b. self-evaluation of operational risk
c. main indicators of operational risk
d. reporting system of losses from operational risks (Operational Risk Application)

The purpose of applying these methods and tools is to increase the awareness of employees with regards to the existance of the operational risks in the activities carried, the identification, documentation and analysis of the operational risks.

2.1. Collection of data on losses due to the occurrence of operational risk events

Operational risk events can be classified into the following four major categories depending on the cause that led to their appearance:

- **Human error**: The errors have their origin in omissions or mistakes due to human factor. Examples: exceed the terms, incorrect input data, lack of knowledge / information needed to perform such work, incorrect customer information, etc.
- **System error**: These errors are the result of using inadequate or incorrect information systems. Examples: hardware or software failures, computing power interruption, errors display of the information requested by the application used (OnlineBanking, Reports, Scoring, Rating, etc.), malfunctioning of ATMs, etc.
- **Process error:** These errors are the results of inadequate or incorrect define of the processes developed. Examples: the regulation norms of the activities carried out are deficient or incorrect.
- **External factors:** These errors are the result of external events affecting the company or are due to unauthorized activities performed by third parties. Example: natural disasters, vandalism, fraud done by customers (settlement tools, trading with financial instruments, etc.)

According to the recommendations of the European Directive *regarding the determination of the minimum capital requirements for the operational risk of the credit institutions and investment firms*, the company must codify every operational risk event identified in one of the seven risk categories:

1. internal fraud,
2. external fraud,
3. employment and safety practices at the workplace,
4. customers, products and commercial practices,
5. damages on tangible assets,
6. activity interruption and inadequate functioning of the systems,
7. execution, delivery and management of the process.

Collection of data on losses represents the collecting, reporting and management of losses due to the occurrence of operational risk events. According to the law, the minimum data collected should include:

a) gross value of loss,
b) date on which occurred the event that caused the loss,
c) recovery mode of the gross value of loss,
d) reasons which have led to the occurrence of the operational risk event.

2.2. Operational risk self-assessment

This is a survey conducted by the directors of the managing committee, in its own structure, with the aim of identifying the operational risk at which is currently exposed the own organizational structure, highlighting the existing internal control level in its own structure and evaluating the ongoing processes in terms of operational risks that

may arise. During the survey, the main operational risks are identified, documented and analyzed based on the following aspects:

- checkpoints within the processes;
- IT/ technology;
- human factors/external factors;
- security.

The survey will be conducted periodically at the initiative of the risk management.

2.3. Key Risk Indicators – KRI

They are used to detect the risks that come into the intervals of attention. It is necessary to set target values for the indicators of risk. There are those indicators whose value is reflected in the changes of the relevant factors in terms of the imminent appearance of some risks. Determination of the appropriate indicators and the change of their value in time, allow the forecast and prevention / reduction of the operational risks.

The main risk indicators indicate that certain processes undertaken within the company are probably more exposed to operational risk than others. The main risk indicators are not representative by their nominal value (an indicator is not too big or too small), but by their tendency that can demonstrate that the operational risk is increasing in certain areas (eg the staff fluctuation in the last period is obviously higher than that which was observed during the previous period, it has increased the number of errors, the surge in sales of a particular product in a branch etc.). The circumstances in which a trend of a main risk indicator has been formed must always be considered.

For an easier understanding of the main indicators of risk they can be divided into the following categories:

- main indicators of general risk – increase of the operational risk at the company level
- main indicators of risk on the product - increasing the operational risk on a certain product
- main indicators of risk on the process - increasing the operational risk on a certain process
- main indicators of risk per unit - increasing the operational risk on a particular area/division/department of the company

2.4. Warning systems

The warning systems (green, yellow or red code) are established to monitor the limits of the main risk indicators. In case a main risk indicator is assigned the yellow or red code, then it is necessary to be undertaken certain actions:

- The green code means a normal state (without operational risk)
- The yellow code means that it has been increased the operational risk and it is required an thorough investigation of the circumstances,
- The red code means an emergency situation that requires immediate action.

In an ideal situation, the main risk indicators must always be of yellow or green color, because, if it is set correctly, this monitoring system for operational risk must allow early detection of the problems and, consequently, the remediation beforehand of the features of the product / process / IT tools, etc. In all cases it is mandatory to check the accuracy of the data and the circumstances in which it was formed the tendency of the main risk indicators.

If, after these plausible checks it is proved that the operational risk has increased (eg a particular process generates too many errors due to the human resources involved, because this process was not automated or a product was wrongly developed and caused high rates of default, etc) then it is required a series of actions, such as those listed below, by way of illustration:

- contact of the concerned department

- clear identification of cause of the operational risk
- identification of all parties involved in the process (inputs – processing - outputs)
- identification of the compartment / department which is directly responsible
- agreeing with the compartment / department which is directly responsible for an action plan (IT development, change of regulation, etc.)
- implementation of the action plan and the assurance that all the parties involved are informed in advance on the details of this action plan.
- continuation of monitoring the main risk indicators in order to measure the impact of implementation the action plan.

3. Conclusions

Operational risk management consists in the identification and measurement, as complete as possible, of these risks, so that the company / investment fund to be able to establish appropriate measures to avoid, reduce, transfer or accept, consciously, the risk. The main goal of the company in the operational risk management is prevention. The requirement is that the cost necessary for the prevention of the operational risk not to exceed the costs or damages that it could generate. To ensure an adequate quality of operational risk management and of the activities related to their control as well as for maintaining an appropriate level of accuracy on information provided to the supervisory authorities, it is essential that the investment fund to build a stable and viable database, containing information relating to extended periods, and to ensure continued maintenance of this database. Implementing methods and instruments of the operational risk management instruments mentioned in this paper, the available options are the use of the standard approach or the alternative standard approach.

References

Ceocea Costel (2010), *The risk in management activity*, Economica Publishing, Bucharest.

Ceocea Costel (2014), *Theory and practice of management decision*, Economica Publishing, Bucharest.

Directive 2006/49/EC of the European Parliament and of the Council of June 14, 2006 on the capital adequacy of the investment companies and credit institutions.

NBR Regulation no. 5 of February 18, 2008 on the approval of using the standard approach or the alternative standard approach for the operational risk.