MANAGING OPERATIONAL RISK IN BANKS

Victoria STANCIU
Faculty of Accounting and Management Information Systems
The Bucharest Academy of Economic Studies
Bucharest, Romania
stanciuvictoria58@hotmail.com

Abstract

Recent years have emphasized focus on risk management, and it became clear that there is an urgent need for a robust framework to effectively manage risk. The financial and economic crisis showed the importance of a strong risk management process and forced banks to take a critical look at how they manage risks. Romanian banking system has known significant changes determined by the implementation of Basel II requirements. These requirements determined an important effort of the banks to improve their risk management process.

Operational risk is considered a significant risk and has an important impact on banks activity and results. Now, there is a clear effort of the banks for applying more advanced methods on operational risk so that their control and management to be improved. The present paper presents the specificity of the operational risk management and the author's solution for the operational risk management in banks.

Keywords: risk management process, operational risk, risk assessment, internal control system.
JEL classification: G32, G38

1. INTRODUCTION

Managing a multitude of internal and external risks is one of the most significant challenges facing any bank. Increasing transaction volumes, and the globalization of business, extended reliance on technology, have introduced higher complexity and uncertainty to banks. In order to maintain a competitive advantage and to improve overall performance, banks are seeking a way to understand and proactively manage the risks that can impact their business. In this respect, it is essential to clearly define the relationship between operational risk processes and the overall control environment.

Banks survive and prosper by accepting risks. Risk must be well managed and for the banking institutions this task has become much more difficult and complex being proved the changing nature of risk in banking industry and its new implications for bankers and bank supervisors. The financial and economic crisis showed the importance of a strong risk man-

agement process and the need of important changes in order to improve the risk management process in each bank and for the banking system as a whole.

The financial crisis showed that the organizations, including credit institutions, have to reanalyze their risk management process, to identify the weak areas and take the needed measures for improving risk management process. In Romanian banks, the risk management process framework remains a priority for the management (having the responsibility to implement an effective risk management process).

Operational risk management represents an area needing important developments. In the last years, the Romanian banks registered higher losses caused by operational events. This is why their efforts focus on better managing the operational risk.

The present paper will explore the approaches and the changes needed in risk management process in general and operational risk in particular.

In order to achieve the stated objectives, a mixed research methodology was used, including deductive positive research, as well as inductive critical interpretative research. These two approaches are able, in the author's opinion, to offer a strong interconnection of theory and research work, merging quantitative and qualitative research methods.

The methodological approach was mostly positive and required the following steps:

- The selection of the research area.
- Research area literature review: The main source of information was represented by Basel Committee on Banking Supervision and CEBS documents, COSO framework and best practice papers. Delimitation of the conceptual framework boundaries which included the specialists' points of view regarding fundamental concepts and the relationships that arises among these concepts. At this level, descriptive, exploratory and evaluative research techniques were used.
- Decisions regarding key questions/areas.
- Defining the starting hypotheses to be verified through empirical research.
- Performing the research: carrying out analysis on the regulatory framework, interviews with banking managers and chief risk officers, documentation on risk management processes implemented in Romanian banks and conducting analysis on these risk management solutions.
- Final conclusions formulation, materialized in the author solution for operational risk management (ORM).

Applicative research was used in order to achieve the objective represented by the testing of the defined framework. The present paper presents the main conclusions, guidelines retained from the research results and solutions for the ORM improvement.

2. RISK MANAGEMENT PROCESS

The effective management of risk is critical for the bank's survival. The risk management goal is to maximize the operational capability of the bank, ensuring an efficient use of resources, valuating the existing opportunities and maximizing the gain. To reach this goal it is necessary to have a good and profound understanding of the existing risks, to implement an efficient internal control system in order to prevent or mitigate the risks. According with the governance principles, risk management and internal control system design and implementation are two linked and very important attributions of senior management. Risk management represents a process directed towards the assessing, mitigating (to an acceptable level) and monitoring of risks. Basel II documents have brought a significant and

explicit focus on risk management and corporate governance. The Basel Committee on Banking Supervision accord is design on three pillars:

- Pillar 1: Minimum regulatory capital
- Pillar 2: Supervisory review process requesting to enforce a strong control environment in order to limit exposure to capital risk
- Pillar 3: Market discipline.

The minimum capital requirements (Pillar 1) concern credit, market and operational risk which are characterized by a quantitative approach of the prudential requirements. Pillar 2 establishes requirements both for banks and supervisory entities. For the banks the requirements require the identification and assessment of material risks, the identification of the most effective controls, the calculus of the amount of capital in relation with the business plan and the defined risk profile and produce capital number and assessment. Pillar 2 also addresses to the supervised entity asking to perform a comprehensive assessment of the banks' capital management and capital adequacy in relation to the risk profile of the business and the risks in its operating environment. Pillar 3 extends Pillar 1 and Pillar 2 of the capital adequacy framework so that depositors, investors and other external parties can assess information on the capital adequacy and risk management of market participants. In this way it is promoted the market transparency and the market discipline is introduced.

An innovative requirement of Basel II documents is the Internal Capital Adequacy Assessment Process (ICAAP). ICAAP is subject to rigorous review by banks' supervisors under Pillar 2.

All Basel Committee documents mentioned above were assimilated in the Romanian regulations starting with 2006 and this update of the banking regulatory framework still continues. National Bank of Romania (NBR) has permanently adjusted its documents and supervision activity to the Basel Committee requirements. As a result of these new documents NBR issued its new regulation 18/2009 increasing the requirements on risk management and compliance.

The financial crisis determined consistent feedback from the financial community. On 7th of December 2009, Basel Committee on Banking Supervision released two new consultation papers with in order to strengthen global capital and liquidity regulations with the goal of promoting a more resilient international banking sector. These two papers together with the Basel II enhancement package issued in July 2009 will determine major changes in the banks' activity determining systems' changes and impacting the banks' profitability [Barfield R. et al, 2009, 5].

In June 2008, the Institute of International Finance (IIF) publishes its report on the Committee on Market Best Practice providing a set of principles of conduct and best practice recommendations for banks in the light of the financial crisis. In March 2009, Ernst & Young conducted a survey having as objective to assess the implementation stage for the IIF recommendations and to identify how the banks are responding to the Committee recommendations. The survey emphasizes very important [Ernst & Young, 2009, 5]:

- Needing changes in governance and risk appetite, the role of the risk function, stress testing and risk transparency. Liquidity risk is also underlined by some banks;
- The banks registering severe impact of the crisis started to work on radical changes. In the markets less affected by the crisis the banks learned from the problems else were and reviewing the controls;

- The top issues amongst UK, US, Swiss, The Netherlands and German banks are in order: corporate governance and risk appetite, liquidity risk, culture and compensation, stress testing, valuation, transparency/quality of information.

The survey emphasize that 92% of the respondents indicated governance and risk appetite as the most important issues to work on. Another 77% of respondents placed culture and compensation as a second priority in their reviewing process, this response being linked by the importance showed to the corporate governance and risk appetite.

Another survey, realized by KPMG in 2009, retained as main conclusions that the significant weaknesses in banks' were [Hashagen J. *et al,* 2009, 3]:

- weaknesses in risk culture and governance;
- gaps in risk expertise at the non executive Board level;
- lack of influence of the risk function;
- lack of responsibility and accountability of those on the front line;
- weakness in the way risk is measured and reported.

The risk management process must take into consideration the fact that risks (of all kinds) action is interrelated and their consequences must be evaluated. It is therefore not recommended to practice risk management on an exposure-to-exposure. Risks must be recognize and managed holistically across the entire bank.

A debate on risk management is not complete without emphasizing COSO documents. COSO documents emphasize that the management must focus on two issues: risks and opportunities:

- Identifying and assessing risks in order to implement adequate controls over the processes and activities so that to obtain the risks' mitigation;
- Identifying and evaluate the opportunities ensures the needed framework to optimize gain.

Starting from this understanding, COSO established its *Enterprise Risk Management – Integrated Framework* comprising eight interrelated components [COSO, 2004, 9]:

- *Internal Environment* – The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.
- *Objective Setting* – Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite. The document states the necessity to be taken into consideration the correlation between the business strategy and objectives and the risk strategy and the targeted risk profile.
- *Event Identification* – The internal and external events, affecting achievement of an organization's objectives, are identified. The identification of events generating risks is an ongoing process. The changing conditions and regulations in the banking industry, the dynamic of products and services and the extended use of the IT solutions induce vulnerabilities that can impact the banking activities.
- *Risk Assessment* – Risks are analyzed, considering likelihood and impact. Risks are assessed on an inherent and a residual basis. In this respect, it is necessary to monitor the risk profile and its alignment to the targeted risk profile.
- *Risk Response* – Management selects risk responses – avoiding, accepting, reducing, or sharing risk – developing a set of actions to align risks with the entity's risk tolerances and risk appetite.

- *Control Activities* – Policies and procedures are established and implemented to ensure the risk responses are effectively carried out. The effectiveness of the implemented controls will be permanently monitor and the correction actions performed in order to maintain an adequate control over the activities.
- *Information and Communication* – Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities.
- *Monitoring* – The entire organization risk management is monitored and the necessary adjustments are done. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.

A quick look on the ERM components emphasize the major attention given to risks: if in the initial version of COSO cube it was presented a single component dedicated to risk topic, in the extended version (ERM) there are assigned three components (Event Identification, Risk Assessment, Risk Response). The extended risk topic in COSO model is natural. Any organization must have processes for the risks' events identification, clear processes and procedures for risk assessment and reporting and effective risk responses developing a set of actions to align risks with the entity's risk tolerances and risk appetite.

The risk management process must ensure a consistent risk identification process. Knowing the significant risks, the management must decide over three types of risks [FAA, 2000, 7]:

Acceptable risk: The part of identified risk that is allowed to persist after controls is implemented. Risk can be determined acceptable when further efforts to reduce it would cause decrease of the probability of success of the operation, or when a point of diminishing returns has been reached.

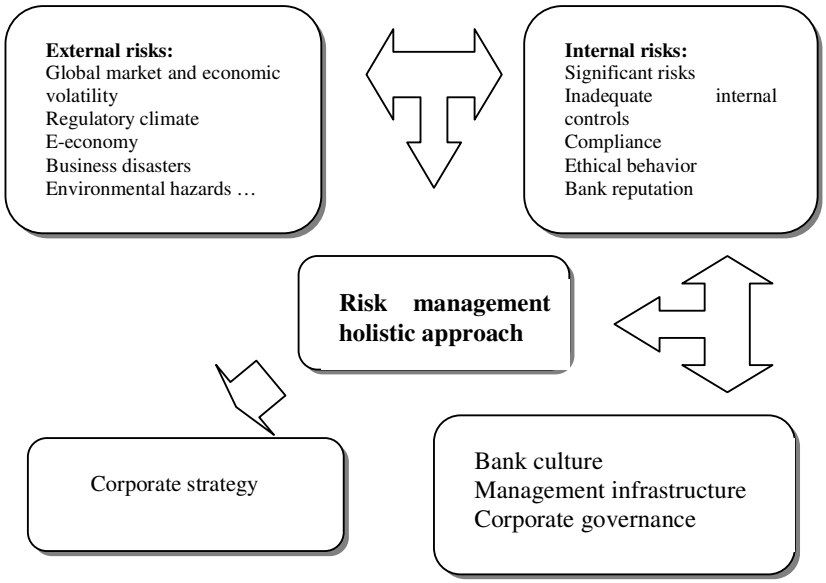
Unacceptable risk: That part of identified risk that cannot be tolerated, and must be either eliminated or controlled.

Residual risk: The part of total risk that remains after management efforts have been employed. Residual risk comprises acceptable risk and unidentified risk.

Risk assessment is an ongoing process that includes identifying risks to achieving organization objectives, analyzing the risks, and deciding how to respond to the risks.

The banks must face to external and internal risks. External risks are generated by from activities outside the organization. These external risks may not be directly controllable by the bank or they may constrain the way in which the bank is permitted to take or address risk. External risks are represented by: technological developments, changing public expectations, legislative directives, natural catastrophes and economic changes. Internal risks arise from activities performed in the bank. The process of identifying risks should consider the following characteristics and attributes: type of risk, source of risk, areas the risk impacts, and level of ability to control the risk.

We consider that a holistic approach is recommended in risk management process assessment. Risk management holistic approach implies correlations with corporate strategy, bank culture, corporate governance, the management infrastructure and is based on internal and external risk identification, assessment and control as figure 1 shows. The holistic approach of risk management implies the analysis of the correlation with the corporate governance and the bank culture. Two of the external risks presented in the figure have an extremely signification for the present context: global market and economic volatility and regulatory climate (characterized by important developments in the last years).



Source: [http://advanced-dynamics.com.au/images/RiskManagementCapabilityModel.gif]

Figure no. 1 Risk management holistic approach

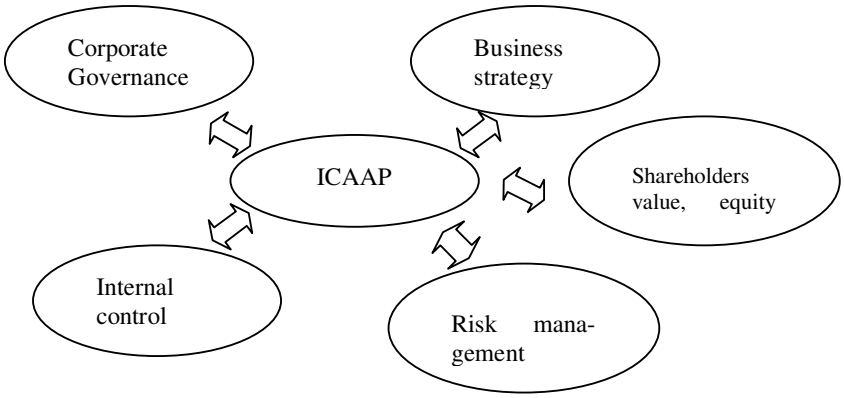
There must be a strong and consistent correlation between the business strategy of the bank and its risk strategy. The business strategy reflects the objectives stated regarding the development of the business lines and the market shares, the level of assets etc. In the current economic context, the business strategy must be based on deep analysis of the macroeconomic and financial industry environment. Alternative scenarios should be prepared. The objectives should reflect the key factors influencing the bank's activity and a careful assessment of the bank's potential in this context. Both external and internal risks must be taken into consideration. The bank must determine its risk bearing capacity and tailor its risk profile being aware of it.

Risk management got an important role in the bank organization and ways of business conduct. There are strong relations between risk management, the business strategy (as we already emphasized), corporate governance and internal control system.

The risk control and reporting is part of the internal control system and the linkage between internal control system and risk management process is very strong.

As it was mentioned in the present paper, an innovative requirement of Basel II documents is the Internal Capital Adequacy Assessment Process (ICAAP). The Figure no. 2 highlights the position of the ICAAP, its interdependences with corporate governance, business strategy, internal control and risk management (being part of it). Capital planning process is related to the business and risk strategies and reflects the risk appetite. In the achievement of the capital planning objectives an important role has risk management process and the quality and effectiveness of the internal control system. The figure also emphasizes the shareholder implication. This implication is given by the fact that ICAAP shows if there is a balance between the existing equity and the needed one as a result to the risks' exposures. If there is no balance, an infusion of capital is required. It is important to notice that the owners are inherently interested in the continued existence of the bank as

they expect a reasonable return on their investment and wish to avoid capital losses. It is important to mention that in the capital adequacy calculus an important component is represented by operational risk.



Source: [Liljeström, 2008, 16]

Figure no. *2* Correlations of risk management internal control, governance and business strategy

3. HOW TO MANAGE OPERATIONAL RISK?

3.1. OPERATIONAL RISK DEFINITION AND CONTENT

Operational risk is not new. We can say, without fear to get wrong, that it is the oldest risk the banks are facing. The Basel Committee defines the operational risk as "the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events" [Basel, 2001, 2]. In the Basel II approach this definition includes legal risk, but excludes strategic and reputational risk.

It is important to state that each bank's operational risk profile is unique and requires a tailored risk management approach appropriate for the scale and materiality of the risks, and the size of the organization. Operational risk is determined by a multitude of factors as for example the complexity of the bank structure, the geographical dispersion of its activities and units, the complexity, range of products and services, number of staff and its professional skills, experience and training and risk management culture as it develops its operational risk management. The complexity of the activity and its geographical extend are extremely important. In the same time, the number of the employees and their professionalism is determinant being proved by the statistics that an important number of operational loss events were determined by human error caused by the lack of competence, experience, overload or insufficient training. Corporate culture is decisive in the fight with risks, operational risk inclusively. Senior management is responsible to ensure the corporate culture development on continuous bases and imbedding the risk awareness in the bank's culture. As long as this awareness related to risks is not ensured, the risk control and management will not attend the desired consistence.

The operational risks can be generated by different causes as for example: business disruption and systems failures, processes failure, compliance gaps, failing controls, people behaviour (internal and external fraud, abuse etc), damage to physical assets, employment practices and workplace safety. These risks may be increased by poor training, inadequate controls, poor staffing resources, or other factors. This is why we emphasized the need of an adequate professional profile and experience for the staff irrespective of their job position. For areas as internal audit, risk management and compliance, Romanian regulations (Regulation 18/2009) are clearly requesting experience and skills.

Each bank is a dynamic organism, knowing permanent growth (in order to increase or conserve its position in the market), developing new products and services more complex, operating in a dynamic regulatory, financial and economic environment as the Romanian one. All these new products and services, new approaches in making business (e-business, alternative distribution channels) imposing more sophisticate IT infrastructure. IT is now a key component of the business activities in any bank and ensures fructifying the identified opportunities but in the same time brings a large set of vulnerabilities exposing the bank to IT risks. In this respect there can be identified some areas where operational risks are emerging:

- Proliferation of new and complex products;
- Extend use of automated technology mapping the potential of manual processing errors into system failure risks. It is also necessary to emphasize the great reliance placed on globally integrated systems;
- Extend of e-business and e-government transactions needing related business applications which expose the companies to potential new risks (e.g., internal and external fraud and system security issues);
- Need for continual maintenance of effective internal controls and back-up systems, adequate and updated BCP;
- Extension of the outsourcing arrangements of all kinds.

The implemented policies, processes and procedures should include principles for how operational risk is to be identified, measured, monitored, and controlled across the bank. In the author opinion, the business lines managers are responsible for day-to-day management of operational risk within each business unit. But all these managers must have a clear understanding of the banks' policies and procedures and they must ensure an effective implementation of those policies in their units' activities. There must be ensured a unique approach in operational risk management so that all operational events to get the most appropriate response and the risk events to be reported and aggregate in terms of number and loss at the bank level. But the awareness of the risks in general and operational risk in particular, must characterize each member of the staff. The implementation of the operational risk framework within each line of business should reflect the scope of that business and its inherent operational complexity and operational risk profile. It also must facilitate the collection of data on operational risk events.

Specialists in operational risk management [PwC, 2010,1] consider that "a key problem often separating operational risk from the rest of the business is that it is often viewed as a distinct risk type rather than being seen as the executional element of all risk types, i.e. from credit and market risk to those risk types falling within the accepted definition of operational risk such as fraud and business disruption" and that is important "to understand that operational risk exists across all risk categories and that operational risk assessment is simp-

ly a vehicle for the continual improvement of controls governing the management of all other risk types".

Our opinion is that operational risk exists across all risk categories and it is very difficult sometimes to delimitate events and losses of operational risk from those like credit or market risk for example, but in the same time there are events that are purely operational risk type. There is no doubt that analyzing operational risk events and causes it will be identified the week areas and improved controls will be put in place in order to better manage other risk. But operational risk must be treated as a significant risk that must be assessed accordingly.

3.2. OPERATIONAL RISK REGULATORY FRAMEWORK

The Basel II Accord was issues in 2001. The Basel documents states operational risk as a distinct class of risk placing it in the category of significant risks. Basel II proposes three approaches for operational risk management exposure each bank being free to adopt any of them (considered to suit them better):

- Basic Indicator Approach: the bank needs to hold capital to a fix percentage of a single indicator;
- Standardized Approach: it is an extension of the previous approach. This approach requests business lines definition and for each of them the regulatory proposes an indicator based on which will be determined the needed capital;
- Advanced Measurement Approach proposes the use on internal models.

It is important to emphasize that Basel documents state that all the approaches can be used in the same bank in different business lines based on qualification standards.

According with NBR document issued in 2007 [Georgescu, 2007, 38] in Romania 22 banks opted for basic indicator approach, 9 banks opted for standard approach; one bank opted for advanced approach. The author believes that it is room for important developments in the operational risk measurement in Romanian banks. It is true that advanced methods need structured databases storing data on a certain horizon of time and more complex methods for risk measurement.

The Basel Committee has an attentive look on the operational risk framework. This is the consequence of the operational risk impact on banks' losses and capital adequacy. CEBS considers that banks must have a clear and complete understanding on the impact that every element has on capital. The impact studies showed the importance of operational risk management (ORM). An important conclusion on CEBS survey [Moscadelli, 2009, 23] is that "banks have significantly improved their knowledge on the nature of operational risk and how it reveals across organizational and business process". In order to sustain the banks' effort, CEBS has recently issued (September 2009) new documents on operational risk topic. The *Compendium of Supplementary Guidelines on implementation issues of operational risk* brings clarifications and supplementary recommendations for the financial institution applying AMA. It is important to state that the above mentioned document can be used also by all the financial institutions applying other models than AMA on operational risk. The document brings details in order to better delimit the operational risk from other risks as for example market risk.

We can conclude that the key elements in the operational risk management process include:

- Appropriate policies and procedures;

• Efforts to identify and measure operational risk;
• Effective monitoring and reporting the operational risk events and their impact;
•A sound system of internal controls ensuring the limitation of the operational risk events;
• Adequate testing and verification of the operational risk framework and continuous improvement of the operational risk framework.

3.3. SOLUTIONS FOR ORM

The present chapter presents the authors' research results materialized in a solution for the ORM improvement. In the author's opinion, this solution requires:

- Creating a system for collecting data related to operational incidents;
- Establishing a set o hey risk indicators;
- Establishing the potential operational risk that can occur;
- Designing and implementing adequate controls for the potential operational risk;
- Periodical test on the implemented controls, reporting controls' failure and taking measures for controls' improvement.

For the data collection, the author recommends the use of an IT dedicated application that ensures the senders' anonymity. This application should be accessed by any employee. The most important problem is to make people input the data events. It is a matter of corporate governance and culture to ensure the awareness of the importance to participate at this data collection process. The employees must be encouraged to take part to this process and make this data event collection part of the business processes run in the bank. Not all the data input by the employees represent operational events. This imposes an analysis of the input information by specialized people and retains in the database just the ones reflecting operational events and losses. The responsibly to analyze the inputs and select the correct ones is usually assigned to risk unit or compliance unit.

Information related on operational risk must be summarize and reported periodically. We emphasize that events with high financial impact will be reported to senior executive managers, at the moment of discovery, in order to be established the most effective response actions.

In our opinion, operational risk management reports should summarize:

• Operational risk loss experience at the organization level, business lines, and event-type basis;
• Operational risk exposure;
• Changes in relevant risk and control assessments;
• Management assessment of early warning elements signalling an increased risk of future losses;
• Exception reporting;
• Operational risk causal factors.

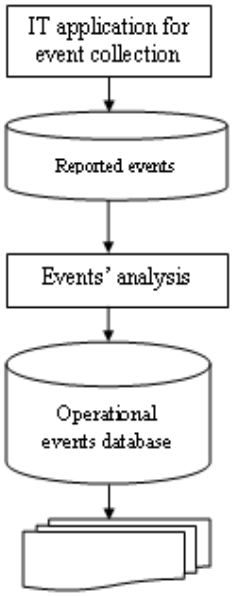


Figure no. 3 Data event collection

In author's opinion reporting loss events must be completed with the presentation of the cause of the loss event and the controls that must be put in place or improved so that a decision to be taken. There are situations that impose deeper analysis and the causes of operational events are more difficult to identify. In those cases the analysis will be performed by risk unit team and business lines representatives and the conclusions will be provided to the management and risk committee when the causes are identified and the solutions to mitigate the risks are defined. It is very important to imply business lines in those analysis because they are responsible for the day-to-day activity and they are the "risk owners". The control effectiveness is their responsibility and all the new developments/improvements in the processes/actions they are performing must have their implication. The solutions can imply changes in the implemented processes so that the processes owners must be involved in these changes.

In the author's opinion it is important that bank design and implement a loss event management process.

This implies risks identification, loss data collection, identification of the threats and the controls implemented, if any, in order to mitigate the risks. The business environment and context is dynamic so that the effectiveness of controls must be periodically tested. It is very important to understand that the controls must be periodically reviewed so that their adequacy and effectiveness to be insured. The test results must be subject of the process owner analysis and the findings, conclusions and solutions must be reported and based of the process owner/senior executive management decisions the changes will be implemented. The senior managers approval is compulsory when the changes are important, affecting the existing processes and implying procedures' updates. Risk monitor implies the usage of key

risk indicators. In the author's opinion, in their selection must be followed a golden rule: avoid the tendency to monitor too many indicators by avoiding irrelevant indicators.

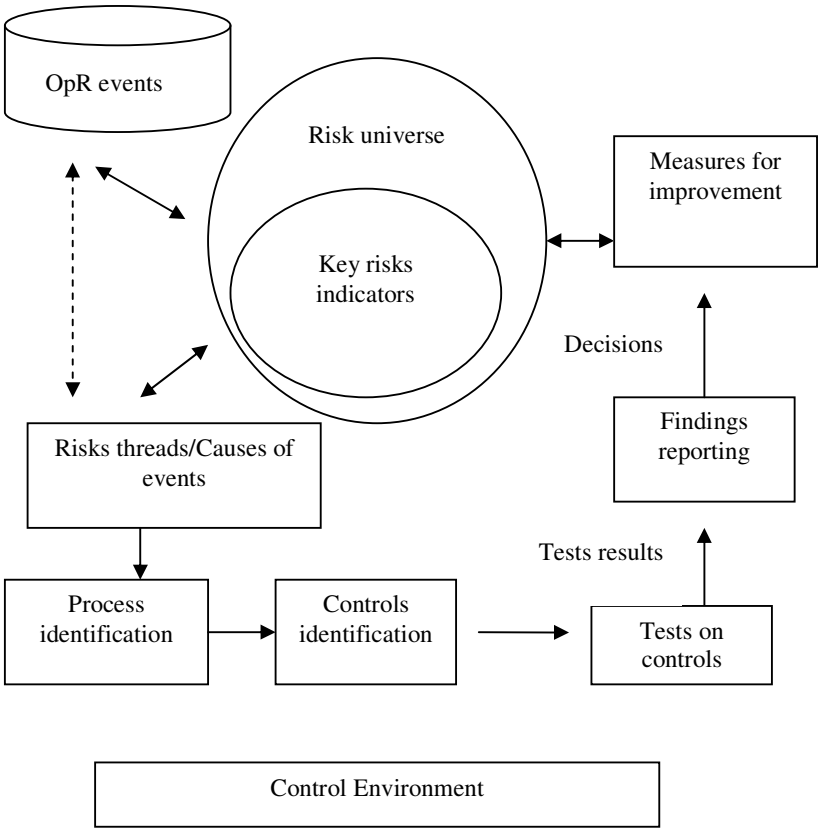


Figure no. 4 Loss event management process

Sound internal controls will reduce the possibility of significant human errors and irregularities in internal processes and systems, and will assist in their timely detection when they do occur. Operational risk inputs play a significant role in both the management and measurement of operational risk. Operational risk inputs aid the organization in identifying the level and trend of operational risk, determining the effectiveness of risk management.

That's why each bank must define and implement its policy that identifies when an operational risk loss becomes a loss event and must be added to the loss event database. The bank must be able to capture and aggregate internal losses that cross multiple business lines or event types. In this context, creating and implementing application that can be accessed

by all the staff in order to input the loss events is critical. The information to be input refers to the followings:

• Loss amount;
• Description of loss event;
• Where the loss is reported;
• Loss event type category;
• Date of the loss;
• Discovery date of the loss;
• Event end date.

In operational risk management there are some "golden rules" that must be followed [FAA, 2000, 4]:

1. Do not accept unnecessary risks:

Unnecessary risk is that which carries no commensurate return in terms of benefits or opportunities. Everything involves risk. The most logical choices for accomplishing an operation are those that meet all requirements with the minimum acceptable risk. As a conclusion: accept just necessary risk, required to successfully complete an operation or a task.

2. Make risk decisions at the appropriate level:

The appropriate decision-maker is the person who can allocate the resources to reduce or eliminate the risk and implement controls. The decision-maker must be authorized to accept levels of risk typical of the planned operation.

3. Accept Risk When Benefits Outweigh the Costs:

All identified benefits should be compared against all identified costs. Even high-risk endeavours may be undertaken when there is clear knowledge that the sum of the benefits exceeds the sum of the costs.

4. Integrate ORM into Planning at all Levels:

Risks are more easily assessed and managed in the planning stages of an operation. The later changes are made in the process of planning and executing an operation, the more expensive and time-consuming they will become.

Figure no. 5 presents, in brief the author vision related to the information flow and decisions related to ORM. The flow starts from each employee reporting an operational risk event filling in the dedicated database (with the mention that all the inputs are analyzed by trained people and just operational events will be kept in the database). The loss events are centralized by ORM Department or Compliance Department who periodically report and present analysis to the Risk Committee. In case of important events, it is recommended to be reported to the Managing Board as soon as possible. The conclusion retained in the Risk Committee and the action plans decided will be presented to the Managing Board. The flow emphasize the place of the risk control self assessment (RCSA) and also the role of internal audit. Internal audit is assessing processes and activities and presents its findings and recommendations to the Board, Risk Committee and Audit Committee in order to be improved the management risk process.

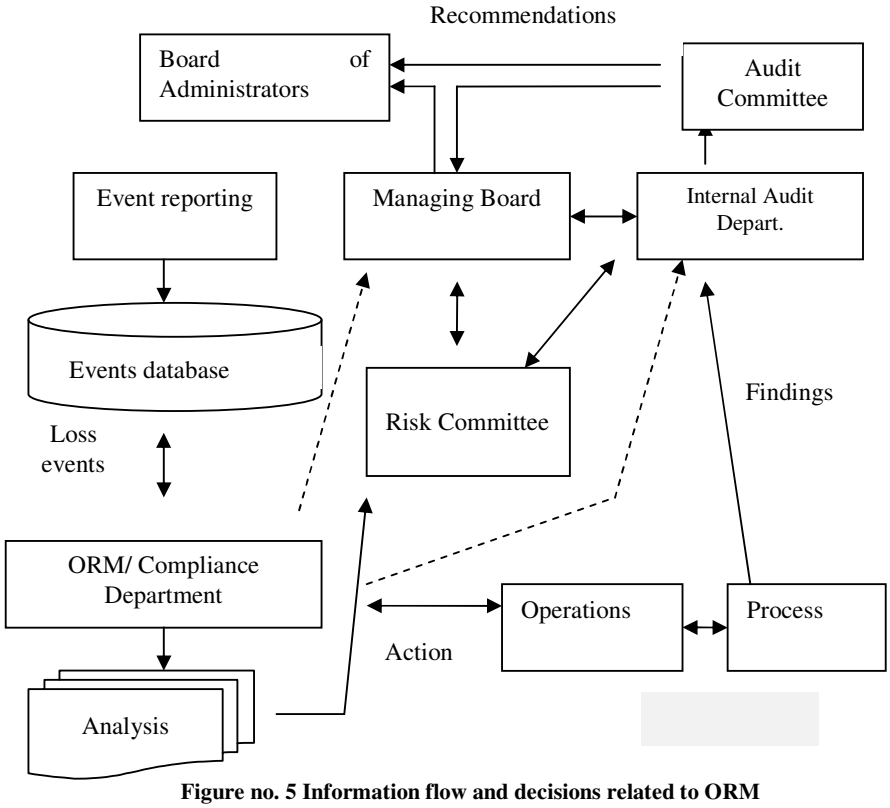


Figure no. 5 Information flow and decisions related to ORM

Risk management topic must be permanently on the agenda of Audit Committee. Internal audit has the responsibility to assess the quality of the risk management process and to provide the assurance on its adequacy. The audit plans and missions are risk oriented. The findings and conclusions of the internal audit missions must to emphasize the auditors' opinion on the risk level and quality of controls. In this respect, risk topic is permanently on the debate of the Audit Committee and senior managers and chief risk officer (CRO) are invited to the meetings.

4. CONCLUSIONS

Risk management is a challenge for all the banks and must be understood and perform as an ongoing process. The bank, being a dynamic organism and operating in a changing environment is exposed to increasing and diversified risks. To reach the established objectives it is compulsory to ensure an efficient use of resources and monitor the risks. There is no predefined solution for risk management in general and operational risk in particular.

Each bank must tailor and permanent improve its risk management process and it is essential to make all employees aware on risk issues.

Operational risk exists across other types of risks. In this respect, it is very important to clearly delimitate loss events generated by operational risk by the ones generated by other significant risks as credit and market risks. The banks are aware that it is a stringent need for their operational risk management improvement. This implies the implementation of the advanced approaches. This process is complex and requires expertise and dedicated processes and IT solutions. Even if the efforts are considerable, the benefits of the advanced approaches use will be reflected in the trends of loss events and capital adequacy amounts.

References

[1] Barfield R et al., *Internal capital adequacy. Assessment process – ICAAP,* KPMG, 2009, at www.kpmg.pl, accessed on March 10, 2010.

[2] Basel Committee on Banking Supervision, *Consultative Document - Operational Risk. Supporting Document to the New Basel Capital Accord*, 2001, at www.bis.org, accessed on April 15, 2010.

[3] Basel Committee on Banking Supervision Supervisory, *Guidance on Operational Risk Advanced Measurement Approaches for Regulatory Capital*. 2003, at www.bis.org, accessed on March 10, 2010.

[4] Basel Committee on Banking Supervision Supervisory*, Compendium of Supplementary Guidelines on implementation issues of operational risk***,** 2009**,** at www.bis.org accessed on March 10, 2010.

[5] COSO, *Enterprise Risk Management - Integrated Framework. Executive summary*. September 2004, at www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf, accessed on April 05, 2010

[6] Federal Aviation Administration (FAA), *System Safety Handbook, Chapter 15: Operational Risk Management*, December 30, 2000, at www.faa.gov/library/manuals/aviation/risk_management/ss_handbook/media/chap15_1200.pdf, accessed on February 05, 2010.

[7] Georgescu F., *Piata creditului din Romania si reglementările Noului Acord de Capital – Basel II*. December 2007, at www. BNR.ro, accessed on May 2008.

[8] Giles Triffitt & al., *Operational risk management Embedding operational risk management: The real use test*. PricewaterhouseCoopers, at http://download.pwc.com/ie/pubs/oprisk.pdf, accessed on March 05, 2010

[9] McNeil A., Frey R., Embrechts P., *Quantitative Risk Management: Concepts, Techniques, and Tools*, Princeton Series in Finance.

[10] Moscadelli M., *The main issues under regulatory scrutiny: a combined reading of the CEBS's and SIGOR's,* 2009, at www.fi.se/upload/43_Utredningar/40_Skrivelser/2009/

[11] oprisk_sep09/oprisk0909_cebs_sigor_moscadelli.pdf, accessed on April 20, 2010.

[12] The Institute of Risk Management, *A risk management standard*. Published by AIRMIC, ALARM, IRM: 2002. at www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf, accessed on March 05, 2010.

[13] PricewaterhouseCoopers, *Operational risk management. Embedding operational risk management: the real use test*, at http://www.pwc.com/gx/en/banking-capital-markets/operational-risk-management.jhtml, accessed on March 14, 2010.