PROCEDURES TO MANAGE OF OPERATIONAL RISK ON THE BANKING INTERNAL LEVEL - ROMANIA'S CASE.

Ph. D. Lecturer SOCOL ADELA
Ph. D. Assoc. Professor IUGA IULIA CRISTINA
Ph. D. Student Assistant GAVRILA PAVEN IONELA
"1 Decembrie 1918" University of Alba Iulia, Romania
Str. N Iorga, nr. 11-13, code: 510009
e-mail: iuga_iulia@yahoo.com

ABSTRACT:

We shall present operational risk as generated by the following primary factors of operational risk: bank personnel, banking processes, systems involved in bank activities, events and factors external to the bank. Each of these primary operational risk factors will be developped in secondary operational risk factors and risk events, with examples and applications, and possible implications for the banks' activities. After identifying and monitoring operational risks, banking societies must be preoccupied with implementing procedures for reducing the operational risk, either settled on internal banking level, by correcting on time the errors registered or by introducing adequate technologies for processing and ensuring information security, either through risk transfer to other fields of activity (for example, insurace against events).

KEY WORDS: operational risk, Basel II Agreement, operational risk managements, operational risk events

1. Introduction:

The perspective of Romania's adhesion to the European Union from the 1th of January 2007 brings the necessity of applying the Basel II Capital Agreement, the name of the International Convergence of Capital Measurement and Capital Standards - a Revised Framework.This study is aimed to be an approach of the operational risk management, describing the main types of risks and showing some preventing and decreasing measures for the Romanian active banking societies. The point 644 of the Basel II Agreement defines operational risk as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk. Legal risk includes, but is not limited to, exposure to fines, penalties, or punitive damages resulting from supervisory actions, as well as private settlements.

Each Romanian bank has adopted a certain strategy regarding the Operational Risk Management. The objective of the strategy regarding the Operational Risk Management is becoming conscious of the operational risk and of the responsibilities in managing this risk at the whole bank's level in order to maintain the risk at adequate parameters to permit the development of the bank's activity in optimum conditions.

The strategy regarding the Operational Risk Management watches over the observation of the following set of **principles**:

1. The management of the operational risk is mainly realized at the level of each organizational entity in a bank;

2. The integration of operational risk's management in the development of the bank's daily activity.

2. Body of Paper:

According to the effectual **[1]** national regulations, the active Romanian banking societies must have politics for the management of the operational risk. These politics must take in consideration at least the following types of events generating the operational risk:

a) The internal fraud (for example bad-faith reporting the positions, theft, concluding of transactions by employees on their own)

b) The external fraud (for example robbery, fake, breaking informatics systems' codes)

c) The conditions for hiring the personnel and the safety of working place (for example compulsory demands of the personnel, not respecting the labor protection regulations, promoting discriminatory practices)

d) Deficient practices regarding the customers, products and activities (for example inadequately using the confidential information about the customers, money laundry, selling unauthorized products, wrong use of products and services regarding the electronic banking system by the clients)

e) Endangering the tangible assets (for example terrorism or vandalism acts, fires, earthquakes)

f) Interrupting the activity and defective functioning of systems (for example defections of hardware and software components, telecommunication troubles, defective projection, implementation and maintenance of the electronic banking system)

g) The treatment applied for customers and commercial counterparts, as well as the defective processing of customers' data (for example wrong recording the income data, defective management of the real guarantees, incomplete legal documentation, unauthorized access to the customers' accounts, disputes)

h) The security of the electronic banking system (for example engagements of the credit institution coming out in false pretences by fabricating the electronic money or getting extra losses or engagements by the customers in case of a defective access in the system).

Table no 1.: The ninth appendix of the Basel II Agreement includes the following classification of the operational risk events [2]:

EVENT- TYPE CATEGORY: **INTERNAL FRAUD** *Definition*: Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/ discrimination events, which involves at least one internal party.	
The category - level 2	*Activity examples – level 3*
Unauthorized Activity	Transactions not reported (intentional). Transaction type unauthorised (w/monetary loss). Mismatching of position (intentional).
Theft and Fraud	Fraud / credit fraud / worthless deposits. Theft / extortion / embezzlement / robbery. Misappropriation of assets. Malicious destruction of assets. Forgery. Check kiting. Smuggling. Account take-over / impersonation / etc. Tax non-compliance / evasion (wilful). Bribes / kickbacks. Insider trading (not on firm's account).
EVENT- TYPE CATEGORY: **EXTERNAL FRAUD** *Definition*: Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party.	
The category - level 2	*Activity examples – level 3*
Theft and Fraud	Theft/Robbery. Forgery. Check kiting.
Systems Security	Hacking damage. Theft of information (w/monetary loss).
EVENT- TYPE CATEGORY: **EMPLOYMENT PRACTICES AND WORKPLACE SAFETY** *Definition*: Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity / discrimination events.	
The category - level 2	*Activity examples – level 3*
Employee Relations	Compensation, benefit, termination issues. Organized labor activity.
Safe Environment	General liability (slip and fall, etc.) Employee health & safety rules events. Workers compensation.
Diversity & Discrimination	All discrimination types.
EVENT- TYPE CATEGORY: **CLIENTS, PRODUCTS & BUSINESS PRACTICES** *Definition*: Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product.	
The category - level 2	*Activity examples – level 3*
Suitability, Disclosure & Fiduciary	Fiduciary breaches / guideline violations Suitability / disclosure issues (KYC, etc.) Retail customer disclosure violations Breach of privacy Aggressive sales Account churning Misuse of confidential information Lender liability
Improper Business or Market Practices	Antitrust Improper trade / market practices Market manipulation Insider trading (on firm's account) Unlicensed activity Money laundering

Product Flaws	Product defects (unauthorized etc.) Model errors.
Selection, Sponsorship & Exposure	Failure to investigate client per guidelines Exceeding client exposure limits.
Advisory Activities	Disputes over performance of advisory activities.
***EVENT- TYPE CATEGORY:* DAMAGE TO PHYSICAL ASSETS** *Definition*: Losses arising from loss or damage to physical assets from natural disaster or other events.	
The category - level 2	*Activity examples – level 3*
Disasters and other events	Natural disaster losses. Human losses from external sources (terrorism vandalism)
***EVENT- TYPE CATEGORY:* BUSINESS DISRUPTION AND SYSTEM FAILURES** *Definition*: Losses arising from disruption of business or system failures.	
The category - level 2	*Activity examples – level 3*
Systems	Hardware. Software. Telecommunications. Utility outage / disruptions.
***EVENT- TYPE CATEGORY:* EXECUTION, DELIVERY & PROCESS MANAGEMENT** *Definition*: Losses from failed transaction processing or process management, from relations with trade counterparties and vendors.	
The category - level 2	*Activity examples – level 3*
Transaction Capture, Execution & Maintenance	Miscommunication. Data entry, maintenance or loading error. Missed deadline or responsibility. Model / system missoperation. Accounting error / entity attribution error. Other task misperformance Delivery failure Collateral management failure. Reference Data Maintenance.
Monitoring and Reporting	Failed mandatory reporting obligation. Inaccurate external report (loss incurred).
Customer Intake and Documentation	Client permissions / disclaimers missing. Legal documents missing / incomplete.
Customer / Client Account Management	Unapproved access given to accounts. Incorrect client records (loss incurred). Negligent loss or damage of client assets.
Trade Counterparties	Non-client counterparty misperformance. Misc. non-client counterparty disputes.
Vendors & Suppliers	Outsourcing. Vendor disputes.

THE PROCESS OF MANAGING THE OPERATIONAL RISK IN THE ROMANIAN BANKS

Compared to the structure of the operational risk events included in the Basel II Agreement, the national regulations had taken over only the first two levels of the operational risk: the type and the category of the operational risk event. The national regulations briefly introduce examples of activities potentially generating banking operational risks, while the Agreement also refers to a third level of the operational risk events: the activities **[3]**.

The Basel II specifies definitions for all the categories of operational risk events, level 1, while the inland legal regulations don't define precisely the operational risk events.

In the Romanian national regulation we can also find two extra categories of risk, compared to those included in the Agreement:

- the treatment applied for customers and commercial counterparts, as well as the defective processing of customers' data
- the security of the electronic banking system

A possible argument for the express mentioning of the security of electronic banking system is the one that these systems are at the beginning in Romania.

The process of managing the operational risk is a cyclic one, meaning the repeated development of four steps, adjusted to the information obtained until then both from the external area and from the inside of the bank. So, the management of operational risk is permanently adjusted to the risk profile of the bank at a certain moment, to the internal risk management abilities, but also to the changes appeared in the economic, financial, political and regulatory field in which the bank develops its activity.

The process of managing the operational risk respects the following steps:

a) Identification,

b) Valuation,

c) Monitoring,

d) Management

a) **Identifying the risks** is a first step which further has to be the basis for developing the viable systems for monitoring and controlling the

operational risk. This process begins with the definition of the operational risk from the bank's point of view, identification of the main elements and description of the generating elements, separation of the operational risk from other risks that appear in the bank's activity.

When identifying the risks there must be had in view:

- **Internal factors**: bank's structure, nature of the bank's developed activities, human resources implied, organizational changes, etc.
- **External factors**: changes appeared in the banking system, technological progress which may have a negative impact on the achievement of the bank's strategic objectives.

The process of identifying the operational risks will be developed in the following ways:

1. Identification of the operations and activities vulnerable to the operational risk.
2. Identification of the operational risk's manifestations meaning the impact on the bank's financial results, following those with potential impact, those efficiently remediate, preventing in this way getting losses, and those that have determined getting losses.

This last process means identifying and catching the losses generated by the operational risk's development. In this way importance is given to the identification of the type of followed losses, the persons responsible for reporting the losses, the criteria and methods of validating the registrations. After validating and insuring the information's consistency, these will be stored in a database regarding the losses from operational risk – "Loss Database"-, and this database will be the foundation for the future valuations of this risk. The database will contain information regarding the registered losses, and also regarding their retrieval, for example the retrieved amounts, the moment of retrieval, sources of retrieval, etc.

b) Valuation

This step of the process of managing the operational risk has as a base the information obtained in the previous step. This process will follow the next directions:

1. Valuating the risks identified for each entity depending on the probability of appearance and on the strictness of its impact on the bank's situation.
2. Ranking the risks
3. Valuating the bank's capacity to face the risks she is confronted with.

For valuating the operational risk, banks will use a series of **instruments** as:

- following the registered losses through a **database regarding the losses of operational risk** (Loss Database);
- identifying and calculating some **key ratios for risk**, and also analyzing them.

Also, each bank has in view to analyze the opportunity of introducing in the future some:

- **self-valuating systems** for the operational risk based on the **experience** and capacity of the implied personnel to assess this risk (risk assessment).

Besides identifying the risks with the highest potential impact on the bank there will be valuated the bank's vulnerability for them.

Valuating the operational risk in a bank implies a straight aggregation of individual risks, despite other risks for which the portfolio risk is lower than the sum of individual risks having in view the portfolio effect.

The valuation of operational risk will also have in view the correlations of this risk with other risks affecting the bank, as this risk may determine the development of other risks, mainly the credit risk, but also the market risk and reputation risk.

c) Monitoring

At risk-owners' level the risk management implies analyzing the operational risks generated by each activity, operation, transaction engaged, product, so that the decisional process to have in view aspects regarding the operational risk.

After identifying and valuating the risks that affect the risk entities activity (board or branch), their risk-owners must ensure the taking of appropriate measures for the activity to develop in good conditions, as well as for preventing the risk's manifestation.

The risk-owners will efficiently send observations and proposals to the adequate bodies for permitting them to generalize the measures for all the entities affected by the same type of event.

Monitoring the operational risk may imply one or more of the following:

- pursuing some **key ratios for risk** which permit the analyze of operational risk's evolution in the bank's activity, from which we can name:
  a) Personnel fluctuation 2%,
  b) Transactions per employee 1000 monthly
- pursuing the situation between the limits regarding the bank's exposure to operational risk.

The reports will be addressed to all the persons for whom the offered information is relevant regarding the management of operational risk. So, when defining the lines and responsibilities for reporting will be taken into account that they should reach all the relevant persons.

The managers of the banks must regularly receive information regarding the development of the risk management process, the bank's exposure

to this risk, and the way in which the procedures for managing the operational risk are applied.

d) Management

After identifying, valuating and monitoring the operational risk each bank is confronted with in her activity, she will decide on the attitude adopted toward them. So, the bank may decide **[4]:**

1. Assuming the operational risks resulted from a certain process, activity;
2. Decreasing the risks – as regards the strictness or frequency – by adequate means of control, by training the personnel or the clients;
3. Transferring the risks to third parties;
4. Eliminating the risks by closing the activity.

Such a decision will take into account aspects regarding the proportion between the costs of control/transfer and the impact of the respective operational risk. There will be also analyzed the efficiency or result of such measures on the risk control.

The operational risk's impact will be valuated both regarding its appearance frequency and regarding the strictness, so that:

- the risks of events with low frequency and strictness will be **assumed**;
- the risks of events with high frequency, but low strictness will be **decreased**;
- the risks of events with low frequency, but high strictness will be **transferred**;
- the risks of events with high frequency and strictness will be **eliminated**.

The risk-owners will take the appropriate measures to maintain the risk between the desired parameters, to restrict the probability of appearance for an event or to reduce its impact.

In order to transfer a part of the operational risks she is confronted with, the bank pursues to sign some insurance policies regarding some types of events generating operational risks.

We will present a brief structure of the main banking activities related to the categories of operational risk events. We mention that actually in Romania each banking society configures its own operational risk profile identifying the activities generating operational risk events. The activities mentioned above offer a possible example in which the banking operational risk events specific for operative banking societies are elaborated.

I. The operational risk event – internal fraud. Activities:

1.1. The bank's engagement in operations with clients, based on the wrong analyze of their activity and potentially loss generating for the bank;

1.2. The deceiving of the clients, by neglecting, errors, deliberate or involuntary elision in clients' information;

1.3. The fabrication of documents by the bank's employees or their complicity in making fake documents (credit contracts, underwriting contracts, cash documents, payment instruments)

1.4. The laying down of fake reports and situations, with bad faith, for cheating the bank;

1.5. The performance of unauthorized banking operations, or operations that are not in the employee's responsibility;

1.6. The registration in the bank's accountancy of operations without documents in proof;

1.7. The information changes made in the bank's informatics applications, without necessary competence and authorization;

1.8. Material and money theft;

1.9. Operations made by employees on their behalf and on their own which affect the bank's patrimony.

II. The operational risk event – external fraud. Activities:

1.1. Counterfeit of documents by third persons, for cheating the bank ;

1.2. Introducing fake banknotes or coins in the bank by clients ;

1.3. Cash deposits made by clients deliberately in a smaller amount than that mentioned in documents;

1.4. Robbery at the bank's wickets or at its cash dispensers;

1.5. Unauthorized access at the bank's informatics system which leads to the bank or clients' prejudice.

III. The operational risk event - the conditions for hiring the personnel and the safety of working place. Activities:

3.1. Disciplinary diversions of the bank's employees;

3.2. Banking activities that can be executed only by several employees, for whom had not been predicted substitutes for unavoidable casualties;

3.3. Absence of key-employees;

3.4. Work assignments that overwhelm the employees' knowledge

IV. The operational risk event - deficient practices regarding the customers, products and activities. Activities:

4.1. Blabbing out information about work tasks, including operations in the clients' name made by employees (to competitor banks too);

4.2. Unequal, preferential, subjective and ungrounded treatments applied to clients;

4.3. Not identifying the money laundry operations;

4.4. Initiating and developing unauthorized banking activities with the clients or operations without contractual documents;

4.5. Not investigating clients' data, according to the requirements for knowing the clients and the internal working regulations;

4.6. Not respecting the internal procedures referring to the maximum limits of exposure on groups or individual clients and the proficiencies on territorial units;

4.7. Incorrect use of the informatics applications accessed by the clients from distance.

V. The operational risk event - endangering the tangible assets. Activities:

5.1. Natural events with impact on the tangible assets (earthquakes, fires, floods);

5.2. Unpredicted events involving third persons or bank employees, generating destructions of the bank's tangible assets (street events, vandalism)

5.3. Inadequate use of the tangible assets and their destruction.

VI. The operational risk event - interrupting the activity and defective functioning of systems. Activities:

6.1. Problems in the functioning of informatics systems, leading to data loss;

6.2. Introducing viruses in the banking informatics system;

6.3. Defections of the physic stocking electronic data equipments;

6.4. Errors in the electronic transmission of data (e-mail);

6.5. Falling down of the electricity supply, generating interruptions in the development of cash dispensers' operations or in the bank's front-office operations;

6.6. Defections in the communication systems, both at intra banking and interbanking level.

VII. The operational risk event - the treatment applied for customers and commercial counterparts, as well as the defective processing of customers' data. Activities:

7.1. Incomplete or wrong contractual documentation signed with the bank's customers;

7.2. Involuntary actions of the bank's employees, generating errors in documents or informatics applications;

7.3. Insufficient study of the quality of values and cash manipulated by the operative bank units;

7.4. Inadequate transportation and taking over of cash from other banking units or from the branches of the National Romanian Bank;

7.5. Inadequate preserving, recording and processing the clients' documents and banking operations;

7.6. Deficient knowledge of the legal and internal banking regulations regarding the clients;

7.7. Wrong and unauthorized registration of documents in the customers' accounts.

VIII. The operational risk event - the security of the electronic banking system. Activities:

8.1. Not allowed activities performed in the system (by employees or customers), generating extra liabilities for the banking society or for the customers, including fabrication of electronic money.

3. Conclusion:

In conclusion, the actual stage of development for the inland legal frame regarding the banking operational risk management shows a generalized assuming of the Basel II Agreement's stipulations. Likewise, the omission of clearly specifying the second and third level of banking operational risk events (the event category and the activity) brings up the necessity that the banking societies should establish their own operational risk profile. Despite the positive aspects of this situation, we can identify some disadvantages too; the banks have extra responsibilities in determining the activities generating banking operational risk. If there existed a national general valid frame, possibly enforced by legal regulations, the banks would have the possibility to configure their own management strategies for the operational risk, based on an existing frame. We don't deny each bank's specificity in the operational risk management, but we underline the innovation of its approach in the banking field, not only national, but also international. We also underline the complexity of operational risk events' types, which makes the banks' situation more sophisticated.

REFERENCES:

[1] Article 78 of the National Romanian Bank's Regulation no.17/2003.

[2] International Convergence of Capital Measurement and Capital Standards – a Revised Framework (sau Acordul Basel II), (2004), Basel Committee on Banking Supervision

[3] Bichi C., (2003), Basel II and operational risk, Financial Market Review, no. 11; Bichi C., (2004), Basel II, final version, Financial Market Review, no. 7-8

[4] Socol A. (2005), Accounting and Management of Banking Societies, Economica Publishing House, Bucharest