CONTEMPORARY APPROACHES TO MANAGING OPERATIONAL RISK IN BANKS

Milica Ranđelović[1]; Milica Stamenković[2]
[1]Higher Business School, Leskovac, SERBIA, millicastankovic94@gmail.com
[2]Higher Business School, Leskovac, SERBIA, stamenkovic.milica.mika@gmail.com

Abstract: *Risk is a term that follows man and all his activities, as well as business entities, on a daily basis, and relates to the situation in the future in which there are several possible solutions with the appropriate probability of taking place. Reguardless of the organizational level they belong to, all bank's employees face everyday risk. Due to globalization and various technical, technological and other innovations, there are increasingly complex risks that a bank is exposed to, and as such require close attention. One of them is operational risk that represents a threat to the bank's capital due to unpredictable external events, inadequate internal processes and procedures, mistakes and fraudsmade by the employees etc. The operational risk is among the most important risks in banking, and as such should be recognized, monitored and controlled in order to reduce its impact and probability of taking place. Some of the many risky events, their consequences, as well as the ways banks defend against them will be described in the paper through examples.*

Key words: *risk, banking, operational risk.*

1. INTRODUCTION

Continuous development of the banking sector, which carries various innovations with it, brings new and more complex problems in banks, i.e. many risks that jeopardize its business liquidity which ultimately reflects on the profit of the bank. These problems are conditioned by internal factors, such as the incompetence and mistakes of employees, and external factors, such as various events on the market, changes in the law, etc.
Risk is a situation where there is a possibility of a negative deviation from the desired outcome that we expect.[1] Hopefully, its impact may be lower or higher but it still cannot be completely eliminated. Therefore it should be controlled or reduced to an acceptable level. In order to successfully deal with these risks in terms of preserving liquidity, achieving its long-term objectives, etc., a bank has to take appropriate action to protect itself from risk. Therefore, the point is not to avoid risk but to identify, assess, measure and control it. All of this minimizes the impact of risk on the bank's operations. These phases constitute the risk management process and the bank is obliged to prescribe adequate procedures for the implementation of the overall risk management process. One of the risks which is very important for the bank and is present in the commercial as well as in the non-performing sector, is the operational risk that will be discussed in the continuation of the work.

2. OPERATIONAL RISK EXPRESSION

Operational risk is as old as just doing business in any business. It is represented in banking in almost all business activities and as such represents a widely debated topic. The impact of operational risk may be smaller or bigger and the realization of its existence may be very important when it comes to the existence of a bank. There are many definitions of operational risk, and one of them is: "Operational risk is the risk of adverse effects on the financial result and capital of the bank due to employee's failure, inadequate procedures and processes in the bank, inadequate management of information and other systems in the bank due to the appearance of unpredictable external events."[2]
The current economic crisis and a large number of individual cases indicate that cumulative operational risks in the area of financial operations cause a domino effect, which can bring financial institutions into the zone of extreme losses, or even bankruptcy. Operational risks are heterogeneous and very complex and can generate disproportionately high losses, since they are interacting with other risks and multiplying their effects. The Basel Committee recently published an informal research where it discussed the growing risk exposure that is neither market nor credit risk, but rather the operational risks that have become the main cause of some of the most important financial and business problems over the past years. [3]

2.1. Operational risk classification

Operational risks belong to a group of non-financial risks, resulting in operational losses caused by three groups of factors: [4]

- Internal risky events - scams, internal failures and operational errors, systematic and legal failures;
- External risky events, which are difficult to control and predict - natural disasters and catastrophes, wars, terrorist attacks and
- Business risk factors, such as declining volume of business activities, changes in aggregate demand, fall or price increase.

The risk of inadequate infrastructure is due to insufficient staff experience, poorly formed liability system, outdated capacity, and so on. The human risk factor is manifested due to an inadequate culture of employee behavior or insufficient number of employees in relation to the volume of work. A specific type of this risk is the risk of management resulting from criminal activities and the failure of management personnel. The risk of the business process is manifested due to inadequate and outdated procedures, various technical and technological problems and limited one-day activities. Technological risks are information technology risks in terms of inadequate software performance, inadequate data protection by third parties, deliberately caused software failures, and the like. External events represent losses resulting from the natural forces or forces that a person has caused, or as a result of a work done by a third person.

Table 1. Matrix of events which are the source of operational risk (types of sources) [5]

Source	Event category
Human factor	Unauthorized activities Employee thefts and frauds Internal system of safety Employee relations Differentiation and discrimination Inadequate business or market strategy
Processes	Processes
Systems	Inadequacy, inefficiency, bad functioning or IT system breakdown
External factor	Thefts and frauds (performed by a 3rd person) External system of safety Other intentional activities Natural disasters Disasters caused by human factor Political and regulatory risk (Public services/information) lack of providers Business partners Sellers and suppliers

The Basel Committee carried out the classification of operational risk in the following way: [6]

- Interminal frauds that involve unlawful acts, misappropriation of property and violation of regulations or undertaking business operations that are contrary to the business policy of a company, involving at least one participant within the observed organization.
- Excerpts that involve events that result in the execution of certain frauds, misappropriation of assets and violations of regulations by third parties, and are categorized as theft, fraud, or violation of security rules.
- Employment and occupational safety, implies acts that are contrary to employment rules, and health and safety regulations that reflect the relationships between employees. This also applies to environmental issues, but also to issues of diversity and discrimination on various grounds.
- Non-professional treatment of clients, or damage arising from the nature or product design, including the disclosure of confidential secrets, improper business and market practices, product errors, etc.
- Damage includes events that lead to property losses due to natural disasters and other hazards.
- Other events that cause business distraction or lead to system errors.

3. OPERATIONAL RISK MANAGEMENT

Operational risk management falls into a relatively young discipline, and for this reason knowledge and experience in this field is very important for the banking industry in our country, which seeks to adapt to European principles and

define strategies for managing important types of risks.
In order to properly manage the operational risk in banking operations, it is first necessary to ensure its identification, monitoring of its development, control and response in order to mitigate this risk. The Basel Committee has a specific role in overseeing the operations of banks through the establishment of certain rules that banks should abide by in their business, in order to properly manage operational risk. Consequently, a certain framework of operational risk management is developed, which is primarily adapted to the business culture of a bank and it shows the practice of the industry in which it operates. The rules with which the bank should coordinate their operations lead to the creation of certain operational risk management frameworks, which are:

- The operational risk event;
- Scenario analysis;
- Risk indicators;
- Self-assessment of controls and risk in processes.

3.1. Framework for managing operational risk

By establishing these frameworks, certain rules, procedures and policies are formed, and positive changes in the risk management process are initiated, since access to data for reporting on exposure to operational risk is enabled. It also enables monitoring and control of both external and internal factors that can lead to undesirable outcomes in the business, and in the process of risk realization, a risk management plan is developed. The framework for managing operational risk provides us with data that will be used to form a model for calculating capital requirements.
The structure of the operational risk management framework has four levels: [7]

- **Strategy** - is the basic approach of the bank to operational risk management.
- **Process** - represents daily activities and decisions related to operational risk management.
- **Infrastructure** - means data, systems and other instruments necessary in the process of managing operational risk.
- **Offering** - important for successful operational risk management is the professional and responsible behavior of employees in the prevention and mitigation of operational risk, as well as external factors that can significantly affect the operational risk intensity.

3.1.1. Operational risk management strategy

Creating a risk management strategy is the basic tool for managing operational risks in banks. The requirement to create a strategy is to understand the nature and objectives of managing operational risks. When defining the strategy, first it is important to determinegoals and business objectives (forming an organizational structure that seeks to achieve goals, the adequacy of procedures and processes, the impact on raising awareness of employees about potential risks, etc.), financial goals (drafting a crisis plan in a crisis that predicts possible losses) and regulatory objectives (requirements of the regulatory body in order to prevent risk protection).
The next step is identifying the participants, i.e. defining their roles and responsibilities. At the top of the hierarchy scale is the Board of Directors whose role is to approve and revise the Bank's Operational Risk Management Framework at the level of the entire bank. The role of senior management is to develop procedures and processes, as well as the policy for managing operational risk while line managers monitor the exposure to operational risk, analyze the causes, the possible consequences or are responsible for the operational implementation of the strategy for managing this risk.
The next stage in defining a strategy which relates to the definition of an operational risk management model. Two models of operational risk management are identified:

- Downstream –senior management communicates decisions to lower levels of management;
- Upside down – senior informs lower line management of results of everyday decisions made by line managers.

3.1.2. Process of managing operational risk

When it comes to management of a bank, in order to reduce losses based on operational risk, it is necessary to manage and control those organizational units of a bank in which this risk is particularly dominant.
Operational risk management has the following phases: [8]

- Identification of risks - in all existing (and those it plans to introduce) products, activities, processes and systems;
- Operational risk - means estimating the size of potential cash losses due to the realization of a risk event and regular monitoring of the realization of potential operational risk with the appropriate reporting form;
- Appropriate control framework - includes policies, processes and procedures for control and/or mitigation of operational risk;

- Analysis of the implementation of control mechanisms and their efficiency - banks are obliged to periodically review the set risk limits and control strategies in accordance with the appropriate risk profile of their bank.
- Risk analysis that remains - in order for the bank to continue to operate, regardless of the realization of the risky event.

3.1.2.1. Identification of operational risk

According to the law, the bank is obliged to identify and assess the events and causes of these events that result in losses in relation to operational risk, taking into account all significant external and internal factors. In the identification process, risk assessments are collected by each business unit on the basis of a risk catalog that enables clear identification of all types of risks. Here the risks that can be avoided are identified. In this case, the bank uses internal and external databases.
When compiling an internal database, it is important that the participants in the process of managing operational risk understand the risky event. Internal databases must be the subject of constant updating and improvement as they provide the basis for quantification, mitigation and control of operational risk.
An external database is an extension of internal database. The category of external databases includes: reports of competing banks that are being publicized, analyzes by government agencies or specialized institutions that collect this type of data, newspaper articles, internet sources, and so on.

3.1.2.2. Measurement of operational risk exposure

Continuous monitoring of data on the causes of operational risk and types of events is very important for the decision making of the bank's management in order to assess the overall exposure of the bank to operational risk on the basis of all relevant data. All the information collected by the management is necessary in order to perform the analysis and assessment of operational risk, as well as to measure the bank's exposure to operational risk. Measurement of operational risk exposure is a stage in determining the degree of bank sensitivity to operational risk, which facilitates the risk management process in banks.
The instruments used by the bank to assess the exposure to operational risk are:

- Self-evaluation - as a process of quantitative analysis within the bank conducted by employees of the bank. The purpose of using this instrument is to identify and close control gaps, which can increase operational risk, well above the acceptable level. It contains the elements of the measurement system which are most often descriptive (eg, small/medium/high exposure) or numerical ranks (such as: structured questionnaires, workshops and SWOT analysis);
- Risk events and processes;
- Scenario analysis - represents a complex and dynamic approach to assessing future exposure to risk;
- Risk indicators - measures to identifying potential losses before they really happen. Risk indicators are located within the bank and have different kinds of forms. They connect quantitative and qualitative methods for measuring exposure to operational risk. The structure of the operational risk indicators consists of the connection with the content of the business process and the calculated measure of one or more critical success factors.

3.1.2.3. Control frame

The need for the Bank to monitor the risk and their disclosure to the financial result and capital of the bank imposes the need to create a model called "three lines of defense". This model is used to provide a multi-layer internal control system. All relevant stakeholders (with their roles and responsibilities) associated with risk management are within this model. The "three-line defense" model provides a simple and effective way to improve communication on risk and control issues precisely by clarifying key roles and tasks (individual groups in the organization). This model provides a new look at the business, supporting the continuing success of risk management initiatives, and it suits every organization regardless of its size and complexity of business.
The key roles and responsibilities of the main stakeholders related to the Bank's operational risk management are:

- **The first line of defense (Business Management)** - Under the supervision of members of the Executive Board, business management is responsible for day-to-day management of operational risk. This means that business lines are the owners of operational risks within their business activities. They should create an adequate awareness of operational risk and a culture that ensures effective operational risk management within thier business domain. Business lines are responsible for the proper implementation and implementation of the policy and the implementation of all guidelines for the effective management of operational risk obtained from the risk management function.
- **Second line of defense (Risk Management function)** - consists of several functions that provide independent support and supervision of processes for managing operational risk. The second line of defense provides support

for the first line in managing operational risk. It develops methodologies, guidelines and reports for the management board and senior management of the bank about the degree of exposure to operational risk.

- **Third line of defense (internal audit)** - Internal audit independently assesses the control environment. Internal audit will implicitly or explicitly - through its risk-focused work report - express an opinion on the quality of risk management by putting them in a relationship with responsibilities. The internal audit will address its recommendations to responsible persons in business lines but will also report the relevant function for independent support and oversight of structural errors and deficiencies in processes and systems.

In case of significant losses in the realization of the risk, in order to ensure continuity in the business, the Executive Board of the Bank is obliged to adopt two plans that enable the smooth functioning of the systems and processes as well as prevention of losses in emergency situations:

- Business Continuity Plan - the plan contains a description of procedures in case of termination of business, a list of resources necessary for recovery, the appointment of teams responsible for setting up business after unforeseen events, established duties and responsibilities, and a backup location in case of inability to establish business processes on the primary location.
- Disaster Recovery Plan - The plan contains procedures for recovering the IT system in the event of disaster events, the procedures for creating and storing backup copies of all data needed to restart processes that support that system.

In order to adequately manage operational risk, the bank's management must have a business map showing all the business activities within each line of business, that is, if any banking activity cannot be classified in these listed lines of business and represents a complementary job to a major business belonging to one of the listed lines of business must be located in the line of business to which the main business belongs.

When determining the location of some of the bank's business lines on the specified standardized business folder, it is necessary to follow the following principles: [9]

- All activities must be located in one of the eight business lines that are mutually exclusive.
- If a banking activity that cannot be accurately located in one of the activities around a business directory map because it refers to an auxiliary function, it should be located in the business unit it supports.
- When entering into the gross income map, in the case of an activity that cannot be allocated to one of the given business lines, the rule to locate the business line that brings the largest burden on the bank must be applied.
- Entry into the business activity map for the purpose of determining the required capital due to operational risk must be consistent with the definitions of business lines used when calculating the level of capital prescribed by the competent regulatory body.
- The process used when entering the folder must be clearly documented, including that the documentation must contain clear motifs for possible deviations and their recording.

3.1.2.4. Treatment of operational risk

After identifying risky events, one should consider their treatment. This implies a choice between four alternatives:

- Recognition of risks;
- Risk avoidance;
- Risking;
- Distribution and transfer of risks.

A widely accepted instrument for mitigating exposure and transferring operational risk according to Basel II is insurance whose application can mitigate the consequences of a financial nature in the event that the insured event occurs. The use of insurance is regulated by the national regulatory body. However, it should be kept in mind that insurance policies are not complete protection against operational risk because the insolvency of the insurance policy maker means that the bank will hardly or by no means collect its claims on the basis of insurance.

3.1.3. Infrastructure

Infrastructure is a prerequisite for successful management of operational risk, and it relates to a set of components that facilitate the functioning of this process. These include:

- Adequate organizational structure in the bank, as well as the quality structure of staff involved in the risk management process;
- Defined strategy, procedures and policies for managing operational risk;
- Adequate selection of methods for measuring exposure to operational risk and continuous development of internal databases;
- Establishing an adequate communication system among participants in the risk management process;
- Continuous development of software systems, etc.

3.1.4 The environment

The bank's environment represents internal and external components that affect the bank's exposure to operational risk. Internal components are employees and management of a bank, which is why a bank must pay attention to their improvement, as it must monitor the flow of information and communication between them within the bank. External components refer to third-party bank contacts, such as clients, competition, laws, etc. In order to ensure the smooth flow of the internal process, these factors must be constantly monitored.

4. EXAMPLES OF OPERATIONAL RISK REALIZATION

4.1. Bank robbery on the example of the bank "Poštanska štedionica" A.D.

In March 2016, thirty customers of the "Poštanska štedionica" bank, A.D. were robbed so that unidentified thieves took their money from their accountsusing "cloned" credit cards. Thieves used ATMs of another bank where they installed a device for stealing data from bank cards. Clients were trying to withdraw money at their bank's ATMs, but unsuccessfully. The money has already been taken. Also, the thieves "hid" the cards at the ATM "Poštanska štedionica", and withdraw money using ATMs of other banks. It is assumed that the thieves used a "skimmer device" and thus scanned the payment cards of clients and obtained the codes for their use. "Skimmer" is a device that reads data from a magnetic or "black band" and later writes it on blank, white, plastic cards which afterwards can be used to withdraw money. In this case, the bank has suffered a loss because it had to compensate its customers.
In order to prevent this type of fraud and abuse which is becoming increasingly common, card companies and banks are trying to increase the security of cards that their clients use. This protection system is based on so-called smart or chip cards, from which it is virtually impossible to copy data. They have additional levels of protection and support and banking "alarm systems" for complete card security. One of the ways is a system called "risk alarm". This system exists in almost all banks in Serbia. The principle is the following - when a client withdraws money from an ATM, in the next few seconds he receives a message on his mobile phone that his card has been used. The message also tells the exact time and place where the card was used. If it was not the client who used the card, it means that his card is "skipped", that is, a duplicate has been created. At that moment, the client can call his bank and ask it to blocks the card so that the risk no longer exists. This form of protection applies to clients who have applied to use a free SMS notification service for each transaction via a payment card. However, this is not the only way of fraud. [10]

4.2. ATM software failure on the example of Intesa A.D.

The failure of Intesa Bank in Serbia due to the use of the new ATM (Automatic Teller Machine) software to control the use and authorization of payment cards cost the bank 985,000 euros. The client who used the error in the software system made 647 transactions, 474 of which were successful. [11] The failure occurred in such a way that the software, instead of withdrawing the amount raised from an ATM, added the raised amount to the client's account. For example, if a client wants to withdraw 20,000 dinars, he will receive those 20,000 dinars in cash, while, on the other hand, instead of reducing the client's account for the same value, it is increased by an additional 20,000 dinars. A failure in the implementation of this software was recorded only with one client, where Banca Intesa noticed the problem after a month, indicating that the bank did not have a well-organized internal audit system. For this reason, it is unlikely that officials have not noticed the irregularities that occurred on accounts when it comes to large sums of money. This created a suspicion that certain persons were involved in concealing this error, that is, that the risk of insider activities occurred. Such omissions have significant influence on the confidence of clients and if affects the growth of the number of new clients. Realization of operational and other risks is of great importance for the bank to build trust for the normal functioning of its business.

4.3. "Phishing" fraud on the example of the National Bank of Serbia

Recently, in April 2017, a scam occurred in the National Bank of Serbia. Fraud was created using a phony e-mail account and forged documents. The fraud was due to the fact that the NBS received new payment instructions, that is, it received by email a new modified electronic address to pay for the hologram film. One letter was changed in the e-mail so that the NBS paid 175,000 euros to the account of "OpSec Security unlimited" instead of an e-mail ending with opsecsecurity.com. Otherwise, the hologram foil is used to create specific holographic protection on banknotes, personal cards, passports and other documents, and is ordered by the Bureau for making banknotes and coins operating within the Central bank.

This type of scam is also known as BEC (Business email compromise) scam, direct email fraud or whaling tactics (fishing for big fish). The goal is to get information that is available from highly positioned managers or people who have access to important information or important jobs, such as payment. The attackers have been investigating the company and employees for months to find out as much information as possible on the basis of which they create an email message that is completely legitimate to the recipient. The email message contains typical business terms and builds confidence by providing relevant and specific information that are confidential. This information is collected, mainly, from public sources, such as business pages or social networks. Whether the scam will be exposed depends on whether the potential victim will believe the authenticity of the message.
In order to prevent this type of fraud, it is necessary for:

- Employees to be educated and warned of this type of fraud;
- Employees to check email addresses, as well as unusual information and requirements that are not in accordance with the procedure;
- Employees not to open links and attachments of suspicious emails and do not send their personal information or customer data;
- Transactions to be monitored to make sure that only transactions made are collected and the like.

4.4. A hacker attack on the Central Bank in Bangladesh

In February 2016, the Central Bank of Bangladesh was the victim of a hacker attack organized by the Lazarus criminal group. The attack was carried out on SWIFT Alliance Access software, which banks use worldwide in their business. The hacker attack began on February 4, 2016, by hacking SWIFT with malware that manipulates logs and deletes the transaction history that has been done. By establishing control over the target network, hackers could be represented as officials of the Central Bank of Bangladesh and made 35 payment instructions in the amount of $ 951 million by the Federal Reserve in Newrock. The first five transactions were executed, but the rest were blocked due to the attackers' mistake.The attackers made a spelling mistake in the payment transaction, which automatically prevented the completion of transactions. As a result, the German Bank marked the transaction as a suspect. However, after the transaction was approved by the Federal Reserve in New York, the money was shipped to Sri Lanka. An unusually large transaction amount was noticed by a banking officer who contracted the German Bank to confirm the suspicion of the transfer. After determining that the recipient is a non-existent entity, the bank froze the rest of the assets and returned it to the originated bank. Of the total amount of $ 951 million, hackers transferred only $ 81 million to accounts in the Philippines: $ 31 million was transferred to the Operator Casino, $ 29 million was sent to the Solaire Casino and 21 million pounds were sent to casino "Eastern Havaii Leisure". [12] The investigation of this case suggests that the attack would not have occurred had the Central Bank of Bangladesh used the prescribed IT equipment, that is, if computers were not networked through the used routers attached to SWIFT, without the existence of firewill which would provide protection against hacking. All this points to the great failure of a significant institution in the country and it serves as a warning to financial institutions to pay attention to the protection of their systems.

CONCLUSION

The operational risk is a possible loss on the financial result and the capital of a bank that arises as a result of various inadequate internal processes, systems or employee errors, as well as due to the occurrence of various external events such as natural disasters, damage caused by human actions, passing of laws and regulations etc. Because of these numerous and varied impacts, we conclude that managing operational risk is an extremely complex process, which requires great attention and focus. In order for the process of management of operational risk to be adequately implemented, it is necessary to provide certain procedures and systems that will be respected in business, as well as appropriate IT systems for monitoring and controlling the occurrence of operational risk.
Frequent attacks on the banking system, both in Serbia and worldwide lead to the realization that there exist many risks that could jeopardize the financial stability of any institution, and in the worst case, the economic stability of a country. The aforementioned examples of operational risk realization indicate serious problems that banks face in today's time.This requires the bank's management to carry out all the necessary activities in order to prevent the occurrence of adverse events. Namely, there should be a well-established system of monitoring the work of bank employees in order to prevent fraud and abuse of office or money laundering. Constant monitoring of the application of innovative IT technology is necessary because of the modern way of doing electronic work as any failure in implementation of certain applications can lead to large losses and even to the disappearance of a bank from the financial market.
It is in the greatest interest of banks to properly manage not only operational but also other risks in order to protect their portfolio from possible financial losses on the one hand, and on the other hand it is important to establish a high quality banking system in the country as it has great influence on the development of a society and economy of a country.

LITERATURE

[1] ANDRIJANIĆ, I.;KLASIĆ, K.:*Tehnika osiguranja i reosiguranja*, Zagreb, 2002.
[2] Odluka o upravljanju rizicima banke, tačka 22.
[3] STOJANOVIĆ, D.; KRSTIĆ, M.; JANJIĆ BADULI, Lj.:*Upravljanje rizikom i osiguranje*, Visoka poslovna škola strukovnih studija, Leskovac, 2017.
[4] TOMAŠEVIĆ, N.; TEŠIĆ, A.:*Upravljanje finansijskim rizicima*, Visoka škola strukovnih studija, Beograd, 2013.
[5] http://www.ubs-asb.com/Portals/0/Aktivnosti/PravnaLica/Preporuka/Metodologija.pdf
[6] STOJANOVIĆ, D.; KRSTIĆ, M.; JANJIĆ BADULI, Lj.:*Upravljanje rizikom i osiguranje*, Visoka poslovna škola strukovnih studija, Leskovac, 2017.
[7] BARJAKTAROVIĆ, L.:*Upravljanje rizikom*, Univerzitet Singidunum, Beograd, 2013.
[8] BARJAKTAROVIĆ, L.:*Upravljanje rizikom*, Univerzitet Singidunum, Beograd, 2013.
[9] International convergence of capital measurement and capital standards, Basel Commitee of the Bank for International Settlements, July 1988.
[10] https://www.srbijadanas.com/it/vesti/evo-kako-da-se-zastitite-od-krade-na-bankomatu-jako-su-ceste-2017-07-30)
[11] http://www.bankar.me/2015/08/07/srbija-fudbalski-menadzer-sa-bankomata-ukrao-skoro-milion-eura/
[12] https://www.nettitude.com/wp-content/uploads/2016/12/Nettitude-SWIFT-Threat-Advisory-Report-client.pdf.