OPERATIONAL RISK MANAGEMENT IN BANKING AND BUSINESS FORENSICS

Dragan Cvetković, PhD[1]
Ministry of the Interior of the Republic of Serbia

Marija Mićović, PhD
Marta Tomić, PhD
University of Criminal Investigation and Police Studies, Belgrade, Serbia

Abstract: In everyday business, banks are exposed to a large number of risks. A special type of banking risk is an operational risk, which due to its form is present in every business activity of the bank. Operational risk represents the risk of loss in the course of business operations, which arise due to inadequate procedures and failed internal processes, human factors, systemic or external events. This is the risk with which scams are most often connected and which tend to develop and take on new forms. Scams not only jeopardize the performance of one bank in terms of its financial status, but significantly affect its reputation. In this paper we discuss the management of operational risk in banking with emphasis on the importance of forensic methods in detecting fraud. The aim of the paper is to point out through the basic theoretical settings and examples from modern banking practice the potential of forensic business in terms of reducing the risk of fraud.

Keywords: banks, operational risk, fraud, business forensics. Introduction

INTRODUCTION

Banking risk represents any uncertain situation in banks' operations, or the likelihood of loss (reduction of profits) arising from the effects of uncertain events in the operations of banks. Of all possible types of risks that threaten financial institutions, operational risk is the most dangerous and it is most difficult to predict. Unlike other risks (market, credit) that are typically a characteristic of individual business lines, operational risks are present in all business processes of banking.

Operational risk management is a key component in financial management and risk that affects net income, capital management and customer satisfaction. It also allows anticipating adverse circumstances or events that could hinder the

1cvetkovicdragan@mts.rs

attainment of the objectives of the institution and direct control procedures and limited resources to key areas of activity and related risks. If the risk is controlled under strict control, even though it is managed properly, resources and capital are released and an opportunity to generate income is created. There is no doubt that management operational risk is becoming increasingly important in financial institutions. Therefore, banks are increasingly specialized in its application. In the banking sector, this is a new area of governance, full of challenges.

Business forensics is the field of forensics which implies the application of knowledge and methods in the fight against business fraud of all kinds and against corruption, includes the investigation, the detection and proofing of not only fraud that is directly visible in accounting, but also those in which there was a violation of the legal norms of some companies such as fraud in business contracts, fraud and deception of customers, consumers and suppliers, evasion of taxes, fraud in the quality of products and services, various types of embezzlement, bribery and money laundering. Business forensics is a general term used to describe any economic investigation, which outcome can later lead to legal or other consequences. It also includes forensic accounting, but is often used to highlight the part of forensics that is not included in forensic accounting in the narrow sense.

DEFINITION, CATEGORIZATION AND IMPORTANCE OF OPERATIONAL RISK

The risk can be defined as the probability that an unfavorable event will occur, which will negatively affect the business (fulfillment of objectives) (Fabris, 2006). The existence of a risk is conditional on a minimum of two possible outcomes. On the one hand, there is a possibility of making a loss, while on the other hand, the gain may be lower than expected. Considering the fact that there is always a risk in the operations of banks, risk management is an integral part of the bank's business policy. This is a discipline of a recent date and can be defined as the function of a bank for risk insurance (The Law on Banks, The Official Gazette of the Republic of Serbia, Nos. 107/2005, 91/2010 and 14/2015).

The bank is obliged to identify, measure and evaluate the risks to which it is exposed in its operations and to manage those risks in accordance with the Banking Law, other regulations and acts. The bank is obliged to establish a comprehensive and reliable system of risk management, which is included in all business activities and which ensures that the risk profile of the bank always complies with the already established risk aversion.

The key risks faced by banks are: credit risk, country risk and transfer risk, market risk, interest rate risk, liquidity risk, currency risk, legal risk and reputation risk, and operational risk (Vunjak, Kovačević, 2006).

Operational risk represents the risk of losses arising from inadequate procedures and failed internal processes, human factors, systemic or external events. This definition of operational risk is embedded in the New Capital Adequacy Framework - Basel II and is the result of a longer debate between regulators and industry from multiple jurisdictions on the scope of the concept of operational risks (Bank for International Settlements, 2009). Although the Basel Committee for Banking Supervision published its definition of operational risk, it left the national regulators and central banks the ability to set their own operational risk definition. Thus, the National Bank of Serbia shaped its understanding of operational risk in the following way: "Operational risk is the possibility of adverse effects on the financial result and capital of the bank due to omissions in the work of employees, inadequate internal procedures and processes, inadequate management of information and other systems in the bank, as well as due to unpredictable external events. "Such a definition includes the legal risk that constitutes the possibility of loss due to penalties and sanctions arising from litigation arising from failure to comply with enforcement and legal obligations, as well as due to sanctions imposed by the regulatory body, excluding the reputation risk that presents the possibility of losses due to the negative impact on the market positioning of the bank, and excludes the strategic risk that represents the possibility of loss due to the lack of a long-term development component in the management and management team banks (Dragosavac, 2012).

One of the definitions of operational risk states that operational risk is a risk that arises from errors or unforeseen events that occurred during the performance of business activities of companies. Sources of this risk can be very wide: fraud, legal risks, environment, terrorist attacks, etc.

Since the definition of operational risk is very broad, it is necessary to categorize events and link them to all relevant information. According to the definition of operational risk, there are four main causes of operational risk events (Milenković, 2011).:

1. People (employees) - within this category are assigned losses caused by employees (fraudulent actions, unauthorized actions, unauthorized approvals, losses due to poor employee behavior and losses in transactional proceedings). This category also includes losses resulting from non-compliance with the Labor Law, internal procedures and acts (litigation with employees).

2. Processes - this category includes losses caused by unintentional errors and omissions in the work of employees, negligence or inadequate business practices.

3. System - within this category, losses are incurred due to errors or defects in software, hardware, system of technology (due to system development and servicing), system overruns for system development and other technologies (misuse of technical infrastructure of the bank). This category includes all the losses that reflect the bank's dependence on technology.

4. External events - this category includes losses arising from events caused by external factors that the bank cannot influence (natural disasters, changes in

political and economic conditions, legislation, public activities or the work of business partners, clients).

In accordance with the regulations of the National Bank of Serbia, and according to Basel II principles, events or sources of operational risk are divided into seven basic categories:

- Internal frauds are losses due to intentional activities or omissions involving at least one person working for a bank or a bank. It is important that there is an "intention" to gain personal gain. Subcategories are: unauthorized activities, theft and fraud, and internal security system.

- External frauds are losses due to deliberate actions committed by third parties, where there is a prevailing intentional and malicious concept, and therefore involve fraud and misappropriation procedures, or avoidance of laws and regulations, regulations and policies of the bank. Subcategories are: theft and fraud, the external security system and other deliberate activities.

- Failure in relation to employees and in the occupational safety system are losses due to the non-enforcement of labor laws and other regulations related to work, employment, health and social and workplace safety. Subcategories are: relationships with employees, workplace safety, diversity and discrimination.

- Problems with customer relationships, product placement and business practice are the losses resulting from deliberate or unintentional omissions in meeting professional obligations towards clients or due to the nature or construction of the product. Subcategories are: convenience, transparency and confidentiality, inadequate business or market practices, product and service defects, selection, sponsorship and client exposure, advisory activities and accidents, and general safety.

- Damages on physical assets are damage to fixed assets due to natural disasters and other events. Subcategories are: natural disasters, human factor catastrophes, political and legal risks.

- Business overdue and system failures are losses due to the inaccessibility and inefficiency of IT systems and providers of utility and information services, and losses due to poor functioning of hardware and software, structural inadequacy, telecommunications deficiencies, etc. Subcategories are: inadequacy, inefficiency, poor performance or system crashes, and unavailability of providers.

- Execution of transactions, delivery and process management are losses due to unintentional errors associated with processes and/or management support. Relations with business partners, customers and suppliers are also included. Subcategories are: process management, transaction engagement and execution, monitoring and reporting, customer acceptance and documentation adequacy, customer account management, business partners, and sellers and suppliers.

Due to its form, operational risk is present in every business activity of the bank and as such occurs in every business unit of the bank, which implies certain assumptions that must be fulfilled to ensure efficient management of

operational risk. First, it is necessary to provide a precise definition of the function of managing operational risk in terms of clearly defined roles and responsibilities of all participants in the process. Secondly, an adequate organizational structure in the bank should be provided in terms of operational risk management. Thirdly, a precise and comprehensive framework for managing operational risk should be established.

Bearing in mind its nature, operational risk management must be seen as a process consisting of two key components (Chorafas, 2004).:

- A proactive approach - which allows proper insight on all business lines, a sufficient level of economic capital and the required level of education and communication of employees;

- Phase structure of decision-making - which enables adequate coverage of the process, since it links the realization of the goals defined by the bank strategy with the day-to-day decisions in operations and operational risk management, at all levels of the management structure.

Risk management is not an end in itself, but a key tool that helps the management to realize corporate goals. The objectives of operational risk management are:

- prevention from a potential event that manifests operational risk,

- mitigate the effects that have arisen within the operational risk and reduce its impact,

- adequate control of the damage incurred in case of manifestation of an operational event (Dragosavac, 2012).

Thus, this process seeks to avoid insolvency of the bank as well as to maximize the rate of return on capital with correction for risk.

FRAUD RISK MANAGEMENT

Fraud involves a wide array of manifest forms of irregularities and illegal acts that are characterized by deliberate misrepresentation or misrepresentation, which are carried out with the aim of achieving unlawful benefits for an individual or organization, where the fraudster may be outside or within the organization. The term fraud is used to describe actions such as deception, forgery, extortion, corruption, theft, misappropriation, unlawful appropriation, giving inaccurate information, hiding material facts, false representation, confusion, etc., resulting in property benefits for the perpetrator, organization or the other at the expense of the organization, individuals, communities, etc.

Fraud is just one of the many risks the bank faces. The frequency and diversity of fraud as well as the fraudulent losses have increased significantly in the last decades, especially due to the greater interaction of all market participants, globalization and the application of modern technology in business. In all processes involving a human factor, a certain degree of risk of fraudulent actions is exposed

organizations. Of the following factors, the degree of exposure to the risk of criminal activity depends on:

- the inherent risk of a fraudulent behavior inherent to the business itself;
- measures in which effective internal controls are available to prevent or detect fraud;
- the honesty and integrity of the persons involved in the process (Singleton, Singleton, Bologna, Lindquist, 2010).

The goal of fraud management is to reduce the likelihood of potential fraudulent activity and their negative impact. The activities undertaken by the organization to reduce or mitigate risks are control activities. The purpose of risk mitigation is to enable the continuation of risk-taking activities, while taking measures (controls) to maintain risk at an acceptable level. Control activities are based on written rules and principles, procedures and other measures that are set up to achieve the goals of the organization by reducing risk.

The conditions for fraud should be reduced to the minimum. The fraud is like "virus" - which slowly, seamlessly penetrates into the body and infects it. Symptoms may include high temperature, headache, drowsiness, etc. Some are recovering after taking antipyretics or antibiotics while for some organisms the consequences are fatal. The virus is being adapted, new forms appear, and new problems persist. It should be pointed out that the virus is activated and comes to the fore when it comes to the smallest opportunity (weakened or decreased immune system). Similarly, fraudsters use every weakness, failure in the organization's protection system. Thus, the cure for this problem is effective internal control, adequate management support and fraud prevention procedures. Antipyretics and antibiotics can be effectively used as a preventive or for treatment. Similarly, the anti-fraud procedure and business forensics, which would be hired as needed, should also have a preventive and corrective aspect. No organizational part is excluded from the risk of fraud, it is worn by all employees at all levels of management from top to bottom and vice versa.

FRAUD RISK ASSESSMENT

The fraud risk assessment is a process aimed at proactively identifying and locating organization's vulnerability to internal and external fraud. For each organization, the process of assessing the risk of fraud is often more art than science. What is gained by the assessment and how to adapt the assessment to the organization? The risks of fraud are constantly changing. This is why it is important to understand that the fraud risk assessment is a continuous, dynamic process (Association of Certified Fraud Examiners – ACFE, 2018).

In general terms, the goal of fraud risk assessment is to help the organization identify what makes it most vulnerable. Through an assessment of the risk of fraud, the organization is able to identify the place, business activity where it will

likely become scam, allowing for the application of proactive measures, in order to reduce the chance that this can happen.

Each organization should conduct a fraud risk assessment. Evaluating the risk of fraud can be a great tool for the organization to start communication and raise employee awareness. Employees are reminded that the organization is concerned with preventing fraud and that there are certain sectors, services within the organization, authorized to declare if they suspect that a fraud has taken place. Open communication and awareness of fraud can deter potential cheaters by increasing their perception that there are professional services that can identify their activities and report them.

Fraud triangle containing three basic elements:

- pressure/motive/need,
- opportunity/opportunity,
- justifying attitude/rationalization.

The fraud risk assessment is the starting point in fight against all types of criminal acts and misconduct in business. Scam researchers, auditors, need to understand criminal schemes, be cautious about indicators that point to criminal action and ways to prevent criminal activity. A key factor in committing fraud is an opportunity. Existence is a situation that management can directly cite while pressure and attitude are human factors that often go beyond the direct impact of the organization. Occasions often trigger features or policies that make misconduct possible or reduce the likelihood that fraud will be detected or punished. Fraud opportunities can be classified either as personally created or organically created. Personally created opportunities happen when there are weak controls, and employees know very well the jobs they perform and believe they can conceal their scam. An employee is often in a position to be trusted when work independently and are closely with suppliers and other key people. Organized opportunities arise from the lack of administrative, business control, processing control and document control. These conditions are characterized by a rapid change of key employees, inadequate employee rehearsal policies, dominant top management, the state of constant crises, internal relations, low morale, and the absence of policies and procedures.

It is extremely important to notice the main cause of fraud in the organization. This makes it easier to assess the risk of fraud, and provide adequate corrective and future protection procedures. In many cases, professional investigators are required for testing or other factors. Maybe it's necessary to talk to lawyers. When deciding who will take part in the investigation, it is necessary to carefully define the role of internal audit in terms of assistance to the investigation and the preparation of the report. When fraud is discovered, a complete investigation must follow. Investigation into fraud is done in order to recover the lost amount of money, to release or punish the perpetrators, to prevent its repetition, and innocent peo-

ple to free suspicions. Fraud investigations must provide proof of loss, dishonesty and allow preparation for a criminal complaint.

BANKING CHANNELS AND MONEY LAUNDERING - EXPLANATORY FORMS WITH EXAMPLES

Banks are particularly vulnerable to fraud, and this is regardless of their size. Since fraud is most often associated with operational risk, banks must account for this risk. Banks rarely emphasize the risks of fraud, although they are exposed to more than other organizations and institutions. In practice, fraud cases are rarely communicated in public because most financial institutions want to avoid negative publicity. This reduces the prospect of prosecution and makes it difficult to deter future fraudsters. However, the big losses of banks that appeared in many financial scandals of the bank were the cause of the collapse of not a small number of banks.

The global financial system has been significantly shaken by numerous banking scandals over the last two decades, largely due to the fact that the risks faced by banks (primarily internationally active banks) have become more challenging and more complex. Large-scale operational losses during the aforementioned period have led to a bankruptcy, a merger, or a significant drop in the price of capital of many world-renowned and recognized financial institutions (Bering Bank declared bankruptcy, in 2008 due to a huge loss resulting from fraud, Societe Generale Bank reported a loss in in the amount of € 4.9 billion (about $ 7.2 billion) as a direct result of unauthorized transactions made by only one employee - a low-level broker, the Riječka banka outburst that erupted in 2002 went missing about € 75 million and through unauthorized transactions). At the end of 2017, there were bankruptcies and liquidations for 24 banks in Serbia. Part of the property was offered by the Deposit Insurance Agency, Privredna Banka Beograd, Agrobanka, Investbanka, Jugobanka, Razvojna Banka Vojvodine, Kosovska Banka, as well as many others (Čudan, Nikoloska, 2018).

Typical examples of fraud involving banks are related to the money, fraudulent crediting, covering debts owed to unauthorized transactions, that is, collecting bills, taking money and writing off; collection of written-off accounts and non-declassification; and deliberately creating a confusion in posting to hide the trail of funds for transfers transferred to the importer's account, failure to comply with procedures and internal procedures, etc. (Stanišić, 2014).

Banks and other financial institutions are the most vulnerable because they do business with money, and are also exposed to the high risk of fraud in various ways. These scams can be made by insiders, i.e. bank employees and managers, or by external scams, whether it's physical or legal persons (often in conjunction with insiders), and lately more and more frauds are spread over the information systems. There are more elaborate classic "schemes". Another danger is the general

misuse of the financial system and financial intermediaries, where banks are most exposed, for "money laundering", which comes from various illegal activities.

Nevertheless, since banking operations are regulated by a positive law in which banks are founded and operated, it represents suitable grounds for various misconduct related to money laundering. Money laundering is still at the center of the attention of the financial and banking sector, because it is precisely in this sector that the occurrence of money laundering is likely to occur five times higher than in other sectors of the economy. The banking sector is used extensively to hide money that is illegally due to the evasion of taxes, corruption, economic crime and other criminal activities, with the aim of including these funds through legal money flows through money laundering. On this path, the funds thus obtained must go through a bank account. The tendency is, therefore, that nothing is left to the case and that the traces are successfully masked, especially in the international business, using the banking sector, so financial experts, lawyers and accountants who devise complex transactions are hired, which effectively hides traces and illegal origin of money (Radojčić, 2013:368).

Typical cases of money laundering are:

1. Placement - deposits at the client's account; purchase of various forms of payment instruments; investing in jobs where the most cash is used as a cover for depositing dirty money into banks; changing banknotes of smaller denominations into banknotes of larger denominations.

2. Layering (concealment) - transfer of money abroad or cash deposited in international banking systems.

3. Integration - early repayment of loans, payment of counterfeit bills; a complex network of international transactions that makes tracking the original source of funds impossible.

In banking operations in Serbia in the past period, numerous abuses in the field of credit policy were observed: the placement of dinar loans to some companies with inadequate guarantees, non-verification of the creditworthiness of the beneficial loan, non-mortgaging of their mortgages, or non-taking of loan security measures. On the other hand, as a guarantee for repayment of loans, some banks accepted bills that were impractical due to insolvency or opening of bankruptcy proceedings. Loans are redeemed based on false documentation. Beneficiaries made false use of received funds with falsified accounts and other relevant documentation, especially for the purposes for which the loan was granted.

The following text will show cases of fraud, misuse, forgery and other incriminated actions in banks, which represent classical examples of operational risk due to fraudulent actions and omissions in the work of employees, inadequate internal procedures and processes, as well as disregard for them, etc. resulted in great damage / loss for banks and other institutions, and the property benefit for the perpetrators of fraudulent actions:

According to indictments for abuse of office in Metals bank and the Development Bank of Vojvodina, which has been in bankruptcy for more than a decade, twelve persons responded. This is a malware indictment with thirty-nine loans, worth about 1.6 billion dinars, which are granted to companies associated with the bank. There are now six former managers of the bank who are accused, as well as one director of a private company.

The Prosecutor's Office for Organized Crime filed an indictment for seven persons, including the Chairman of the Credit Committee of Privredna Banka Beograd, the members of the Credit Committee, the Deputy Credit Committee member of the aforementioned bank and the financial director of the domestic company. According to the allegations of the criminal charges, the suspects are charged with obtaining unlawful property benefits from the domestic company as responsible persons of Privredna Banka Beograd by unlawful reprisal of ten loans. Given that the loans were not returned to Privredna Banka Beograd, it was damaged by about fifteen million euros and about 60 million dinars. During the realization of the credit placement, the bank did not possess adequate security means, uneconomic bills were used as cover (Čudan, Nikoloska, 2018).

In May 2008, the cashier of the Raiffeisen Bank in Kragujevac, who was aware of the lack of internal procedures, unlawfully withdrew from the bank's account of 1.1 million euros. The money, which the cashier unlawfully lifted from the account, had to return it to the bank (Barjaktarović, 2013).

Police officers in Belgrade arrested a bank employee because of the suspicion that, as a liquidator of the bank, he made counterfeit payment orders for vehicle registration, which he filled in with data on vehicles and owners and authenticated by the seal of the bank and his initials. It is suspected that in the period from the beginning of 2014 until the end of 2016, he had forged a payment for 511 registration of motor vehicles and obtained a material benefit in the amount of about 3,750,000 dinars, to the extent that the budget of the Republic of Serbia, the Ministry of Internal Affairs, the National the Bank of Serbia and the budget of the Municipality of Sopot (https://www.alo.rs/vesti/hronika/bankarka-uhapsena-zbog-falsifikovanja/100668/vest).

Members of the Ministry of the Interior filed a criminal complaint against one person because of the suspicion that he committed the crime of fraud. He was suspects that by falsely presenting facts about his financial situation and creditworthiness, demanded and received four loans with several commercial banks in February and March 2017, in the total amount of 5,672,500 dinars. After obtaining loans and raising money from bank accounts, he, as suspected, left the territory of Serbia, and commercial banks damaged the amount of 6,480,925 dinars in the name of the debt.

Two people were arrested on suspicion of attempting to obtain unlawful property gain with false documentation. It is suspected that, by handing over forged documents to the National Bank of Serbia, they tried to obtain unlawful material gain in the amount of several hundred thousand euros. At the burden, a crime of

fraud is attempted. This was prevented thanks to the multisectoral cooperation and efficient operation of the prosecuting prosecutor, the police, and the National Bank of Serbia, who immediately reported this event.

ANALYTICAL PROCEDURES AND TECHNIQUES FOR FORENSIC RESEARCH

The decision on engaging forensic accountants can be made by the bank's management, company, owner of capital, creditors, investors, etc., if they need objective, independent and expert judgment regarding the existence of fraud in the organization. The choice of goals for forensic analysis depends on its purpose, which is determined by the contracting authority itself. For some purpose the assessment of a potential partner is sufficient for assessing forensics about possible, major irregularities, and a high level of fraud risk. When there is a suspicion of fraudulent actions, the goal is to determine whether it has already happened or happens and determine who its executor is. Therefore, the initiation of criminal responsibility is a necessary, valid proof of irregularities or fraud. In support of disputes, the client is the one who sets the goal. Forensic analysis has the following basic goals:

1. detection of areas of possible irregularities or fraud, narrowing of the search area for certain irregularities, or locating the area of irregularity or fraud,

2. detection of specific irregularities or fraud or methods of execution, assessment of the level of risk of established irregularities or fraud, or assessment of the danger of irregularity or fraud committed (intentionally, unintentionally, high or low level of irregularity, big or small risk of fraud)

3. the production of evidence, i.e. the provision of material and other evidence that the irregularity or fraud has been committed and the manner of the breach (Muminović, 2011).

The tasks of forensic accountants are to analyze, interpret, summarize and present interconnected business-financial positions, so that they understandable and properly corroborated. Forensic accountants participate in the following activities:

- investigating and analyzing evidence of fraud committed;

- developing computerized applications that will serve in analyzes and presentations on financial evidence;

- presentations of the results of the research in the form of reports and completion of documentation;

- assisting in legal proceedings, including testimony in court as expert witnesses, and preparing visual means to serve as evidence at trial (Dimitrijević, Danilović, 2017).

For the detection of fraud, specific knowledge and experience are needed, that is, specialists need to know the technology and method of doing business in certain areas, as well as the regulations governing the same, and then the forms of fraudulent actions and the method of proving them. The development of forensic accounting has enhanced the specialized knowledge and skills necessary for a more effective fight against fraud. It implies the application of all accounting, auditing and other financial skills and knowledge in clarifying relationships, facts and economic transactions that may or may already be the subject of judicial proceedings, and the like. There are several possible models of forensic accounting: involvement of a forensic accountant in the audit team during a regular annual audit of the financial statements; the introduction of a compulsory forensic audit for all entities of public interest; the introduction of a sudden forensic audit according to the principle of random choice for all entities of public interest; implementation of a reactive or proactive forensic audit at the request of the shareholders, and performing a forensic audit on the basis of a report or a suspicion of fraud (Tušek, Klikovac, 2013).

Forensic accountants combine their accounting knowledge with auditory, investigative techniques, and other skills, all for the purpose of detecting fraud. During the investigation of possible fraud, forensic accountants use various analytical techniques to analyze the relationship between the elements of financial statements. These analyses are used for a later detailed analysis of business transactions if the initial analysis of the elements of the financial statements points to the possibility of fraud. Analytical procedures in forensic accounting, as a rule, are applied phase-based, graded from the most general to extremely direct. Each of these segments of the analysis has its specific objectives, such as: preliminary (preparatory) analytical procedures, as the most general, are used to identify areas of high risk of fraud, acquiring insights into nature and the time of manipulation, as well as assessing the degree of necessity of applying appropriate forensic procedures to prove them; independent analytical procedures are used to obtain evidence, by comparing and harmonizing specific data, as well as establishing the credibility (correctness) of documentation, posting and accounting, and final analytical procedures, as the most direct, which serve to make conclusions about the impact of problematic transactions.

The most common techniques used by forensic accountants are based on various techniques of financial analysis, such as:

- horizontal analysis - compares items from the current period with the same items from the previous period;
- vertical analysis - compares the percentage shares of individual items in the financial statements;
- comparison of detailed items in the financial statements - with the same or similar items from the previous periods;
- analysis of relationships - in the financial statements in the areas of profitability, liquidity, solvency, activity and value creation.

- Forensic accounting, besides the traditional accounting technique, intensively applies some specific techniques:

- Benford's law - shows the likelihood that a figure is found in the right place in the number. The essence of Benford's law is that certain figures appear more often than others in datasets;

- Beneish's model - used to estimate the potential level of fraud in the financial statements based on eight variables (indexes);

- Computer-Assisted Audit Techniques (CAATS) - is a practical application of information technology in forensic audit work;

- Data mining techniques - a set of techniques designed to automatically search for large amounts of data for the purpose of finding information that will help detect fraud;

- Ratio analysis - has a great analytical role in forensic research. Each of the ratios is a fairly reliable trace in detecting potential fraudulent actions.

Forensic accounting has some disadvantages. Engagement of forensic accountants is expensive, there is the possibility of leaking confidential information, upsetting the reputation of the company and losing the confidence of employees (Lazović, 2014). Every engagement of forensic accountants requires a certain cost for the company it engages, because the analysis uses procedures that require the use of computer software and work of accountants. Loss of information that they possess, as well as unprofessional handling of a database, can be a blow to the real-time reports.

CONCLUSION

The operational risk in the bank's operations stems from fraud, inadequate practices, procedural errors due to human factors, and infrastructures and systems. For these reasons, it is necessary for every bank to perform a quality risk assessment of fraud and establish a comprehensive and reliable risk management system.

Banks are particularly vulnerable to fraud, and this is regardless of their size. Since fraud is most often associated with operational risk, banks must take care of this. In practice, it is not rare that fraud cases are not publicly disclosed, as most financial institutions want to avoid negative publicity. This reduces the prospect of prosecution and makes it difficult to deter fraudsters.

For the purpose of more efficient fight against fraud, a new scientific discipline and activity was born - forensic accounting as part of business forensics. Firstly, the need for forensic accountants' services was felt in banks, insurance companies, and lately, primarily in the police and investigative institutions for the prevention of economic crime.

Cheating activities in banking operations are becoming more complex and more difficult to discover. Since fraud is the risk of very significant losses, it is important to understand the motives of such activity, the ability to detect fraud, the means to reduce the risk of fraud and the role of business forensics in detecting and preventing fraud. Therefore, the underlying goal of forensic accounting is the continuous development of detection methods and fraud protection mechanisms.

The key message of this paper is to point out the need to involve forensics in the management of operational risks, in the field of prevention and fraud detection, all with the aim of more efficient protection of the banking sector from fraudulent actions. It is therefore necessary to make additional efforts to promote the importance of forensic accounting and encourage its development, in order to minimize the number of frauds. The process is not cheap, but it is certainly beneficial for society as a whole.

REFERENCES

1. Association of Certified Fraud Examiners - ACFE (2018) Fraud Examiners Manual, International Edition, Inc. United States of America.
2. Albrecht, W. Steven., Albrecht, Chad., (2004), Fraud Examination & Prevention, Thomson-South-Western, Ohio.
3. Barjaktarović, L., (2013), Risk Management, University Singidunum, Belgrade.
4. Budimir, N. (2013), Forensic Accounting, Business Analysis Anals, No.8,
5. Vunjak, N., Kovacevic, L. (2006), Banking - Banking Management, Faculty of Economics Subotica.
6. Dimitrijevic, D. and Danilović, M., (2017), Discovering fraud in companies in the Republic of Serbia using the Beneish model, Anals of the Faculty of Economics in Subotica, 37/2017, vol. 53.
7. Dragosavac, M., (2012), Operational Risks, School of Business, Novi Sad, nr 4.
8. The Law on Banks ("Official Gazette of the Republic of Serbia", No. 107/2005, 91/2010 and 14/2015).
9. Lazović, G. (2014). The advantages and disadvantages of forensic accounting. Business Consultant, 6-36, FINconsult, Sarajevo, 6-36.
10. Milenković, I. (2011), International Banking, Faculty of Economics Subotica.
11. Muminović, S. (2011), Forensic Accounting - Need or Empowerment, Auditor, Institute of Economics and Finance, No.54.
12. Radojčić, S., Avoidance of Tax Payments, Economic Crime and Corruption, University of Kragujevac, Kragujevac, 2013.
13. Stanišić, M., (2014), Internal control and audit, University Singidunum, Belgrade.

14. Singleton, T., Singleton, A., Bologna, J., Lindquist, R. (2010), Crime Review and Forensic Accounting, Association of Accountants and Auditors of Serbia, Belgrade.
15. Skalak, Golden, Clyton & Pill (2011) A Guide to Forensic Accounting Investigation, New York, John Wiley and Sons Inc.
16. Tušek, B. and Klikovac. A., (2013), Analysis of possible forensic revision models in the Republic of Croatia, Economic Review, 64 (2).
17. Fabris, N. (2006), Central Banking in theory and practice. Podgorica: Central Bank of Montenegro.
18. Chorafas, N.D., (2004), Operational Risk, Control with Basel II - Basic principles and capital requirements, Butterworth Heinemann, Oxford.
19. Čudan, A., Nikoloska. S., (2018), Economic Crime, Criminalistic Police Academy, Belgrade.

Internet sources

1. https://www.alo.rs/vesti/hronika/bankarka-uhapsena-zbog-falsifikovanja/100668/vest Accessed: 04/20/2019.
2. https://www.valjevskaposla.info/krivicne-prijave-za-vise-lica-zbog-prevare-i-falsifikovanja-isprava/ Accessed: 04/21/2019.
3. http://www.rts.rs/page/stories/sr/story/135/hronika/3428131/pokusali-da-prevare-narodnu-banku-srbije.html Accessed: 27.04.2019.