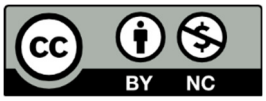
ECONOMICUS

Prosinac	2024	Broj 24	IX. godina izdavanja
December	2024	Number 24	IX.Year of publishing
ISSN 1849-9686		UDK/UDC 330.1(05), 30(05)	

Ksenija Hruška [1]

Pregledni znanstveni rad
Subjcet Review

UDK (UDC): 336.71:658.155



UPRAVLJANJE OPERATIVNIM RIZIKOM U BANKARSKOM POSLOVANJU S FOKUSOM NA RIZIKE POVEZANE S INTERNIM I EKSTERNIM PRIJEVARAMA

Sažetak:
Rad analizira upravljanje operativnim rizikom u bankarskom poslovanju, s posebnim naglaskom na rizike povezane s internim i eksternim prijevarama. Temelji za učinkovito upravljanje operativnim rizikom dati su kroz domaći zakonodavni okvir te standarde Basel II i Basel III. Pred bankama se svakodnevno pojavljuju novi izazovi zbog digitalizacije poslovanja te su u porastu sve složenije prijetnje, poput raznih vrsta internetskih prijevara. Kroz sekundarno istraživanje literature, studija slučaja i regulativa, kroz rad su istražene najbolje prakse u borbi protiv prijevara u bankarskom sektoru, te je naglašena važnost naprednih tehnologija i snažnijih unutarnjih kontrola. Potvrđena je hipoteza da učinkovito upravljanje operativnim rizikom može smanjiti gubitke od prijevara.

***Ključne riječi**: Basel II, Basel III, bankarski sektor, digitalizacija, operativni rizik, prijevare, sigurnosne mjere.*

OPERATIONAL RISK MANAGEMENT IN BANKING WITH A FOCUS ON RISKS RELATED TO INTERNAL AND EXTERNAL FRAUD

Abstract:
The paper analyses operational risk management in banking, with a particular focus on risks associated with internal and external fraud. The foundations for effective operational risk management are established through the national legislative framework and the Basel II and Basel III standards. Banks face new challenges daily due to business digitalization, leading to increasingly complex threats such as various types of cyber fraud. Through secondary literature research, case studies, and regulatory analysis, the paper explores best practices in combating fraud within the banking sector and emphasizes the importance of advanced technologies and strengthened internal controls. The hypothesis that effective operational risk management can reduce fraud-related losses is confirmed.

***Keywords:** banking sector, Basel II, Basel III, digitalization, fraud, operational risk, security measures.*

ECONOMICUS

Prosinac	2024	Broj 24	IX. godina izdavanja
December	2024	Number 24	IX.Year of publishing
ISSN 1849-9686		UDK/UDC 330.1(05), 30(05)	

INTRODUCTION

The subject of this paper is the analysis of operational risk management in banking, with a particular focus on risks associated with fraud, as this type of operational risk can lead to significant financial consequences. The paper examines the regulatory framework, primarily the Basel II and Basel III guidelines, which establish the foundations for an effective system of control and mitigation of operational risk.

The aim of this paper is to explore the theoretical aspects of operational risk, analyse the regulatory frameworks related to managing this risk, and provide insight into the specific challenges associated with fraud in the banking sector. The paper will consider best practices and measures adopted by banks to reduce these risks.

To achieve the aim of this paper, the following hypothesis is proposed:

H1: Effective operational risk management can reduce fraud-related losses, but it requires the application of advanced technologies and robust internal controls due to increasingly complex threats.

The paper employs a secondary research method, including an analysis of available professional literature, regulations, and case studies. By using existing scientific research, regulatory guidelines, and data from the financial industry, the paper offers insight into current trends and methods in operational risk management, with a particular emphasis on fraud prevention measures in the banking sector.

1. THEORETICAL ASPECTS OF OPERATIONAL RISK IN BANKING

Operational risk in banking is defined as the risk of loss resulting from inadequate or failed internal processes, human errors, technological malfunctions, or external events (Basel Committee on Banking Supervision, 2010). This definition of operational risk is incorporated into the second set of international banking regulations known as Basel II (Basel II: International Convergence of Capital Measurement and Capital Standards), developed by the Basel Committee on Banking Supervision. Basel II emerged as a response to the regulations established in Basel I, aiming to enhance the stability and resilience of the global banking system, with a focus on stronger regulation, greater transparency, and improved risk management. Specifically, regarding risks, it regulates standards for managing credit, market, and operational risks (Basel Committee on Banking Supervision, 2004). Managing operational risk is crucial for the stability of financial institutions, especially in the context of increasing digital operations and rising threats such as fraud and cyber attacks (Gačević and Dragosavac, 2023). Ineffective management of operational risk can significantly jeopardize the operations, reputation, and financial results of banks (Bank for International Settlements, 2009). According to the Credit Institutions Act that came into force on January 1, 2009 (Credit Institutions Act, 2021), operational risk is defined as "the risk of loss resulting from inadequate or failed internal processes, people and systems or external events, including legal risk." This Act (Credit Institutions Act, 2021) stipulates that a credit institution is required to encompass credit risk, concentration risk, securitization risks, residual risk, market risks, operational risk, liquidity risk, interest rate risk in non-trading book positions, excessive financial leverage risk, and other risks to which it is exposed or may be exposed in its operations within its risk management system.

1.1. Categories of operational risk

Banks, as credit institutions, are obliged to categorize their data on losses arising from operational risk based on the type of event, type of loss, and type of risk. It is important to consider that a single event can lead to one or more types of losses or financial damages resulting from that event (Croatian National Bank, 2013). In this regard, Basel II provides a categorization of operational risk as shown in the following table (Table 1).

Table 1. Categories of operational risk according to Basel II

Categories of Operational Risk
Internal Fraud
External Fraud
Employment Practices and Workplace Safety
Clients, Products, and Business Practices
Damage to Physical Assets
Business Disruption and System Failures
Execution, Delivery, and Process Management

Source: Basel Committee on Banking Supervision (2004).

Internal fraud refers to losses arising from unauthorized actions, fraudulent activities, embezzlement, theft, misappropriation of assets, or other violations of regulations and/or internal acts of a credit institution, involving at least one internal party. External fraud encompasses losses resulting from actions taken with the intent to commit fraud, theft, misappropriation of assets, or other regulatory violations by a third party. Employment practices and workplace safety involve losses stemming from violations of laws or contracts governing employment relationships, health care, or workplace safety. The category "Clients, Products, and Business Practices" pertains to losses incurred in dealings with clients that arise from unintentional and/or negligent actions or that result from the nature or characteristics of the product or service provided. Damage to physical assets includes losses resulting from the destruction or damage of physical assets due to events such as natural disasters, terrorism, or vandalism. Business disruptions and system failures refer to losses incurred due to interruptions in operations, errors, or unavailability of systems. The category "Execution, Delivery, and Process Management" relates to failures in executing tasks or inadequate process management and losses arising from relationships with business partners and service providers (Decision on the Adequacy of Capital Guarantees for Credit Institutions, 2/2010).

1.2. Specificity of Operational Risk in Banking

Operational risk in the banking sector is distinct compared to other industries due to the potentially high financial damage that can occur. Specifically, banking activities involve a high dependence on technology and human factors, as evidenced during the financial crisis of 2008 when banks suffered significant financial losses. The most notable example is the case of Lehman Brothers, which reported losses of approximately $619 billion in total assets in September 2008. These losses included over $40 billion in net losses in the year preceding its bankruptcy, which is considered the largest in U.S. history and marked the beginning of the global financial crisis. Inadequate management of operational risk significantly contributed to the collapse of this institution. Specifically, there were issues related to insufficient internal controls, a complex financial structure, and a high reliance on technological systems, which hindered timely recognition and response to financial problems (Wiggins et al., 2019).

It is also essential to mention the terrorist attack in New York on September 11, 2001, which not only resulted in irreplaceable human casualties but also involved property losses, business disruptions, and long-term economic consequences. For instance, it is estimated that Bank of New York lost assets worth $140 million, while the total financial losses caused by this event are considered the most expensive insured property losses in history, with estimates ranging between $40 billion and $70 billion. In this case, when viewed from an operational risk perspective, there were not only asset losses but also disruptions in the operations of financial institutions, interruptions in operations, increased security costs, and changes in regulations that affected the entire industry (Chernobai et al., 2007).

2. OPERATIONAL RISK MANAGEMENT IN BANKS

According to Basel II (Basel Committee on Banking Supervision, 2010), operational risk does not arise directly as expected profit but is present in the daily activities of banks. Inadequate

management of this risk can lead to misrepresentation of banks' risk profiles and significant losses.

Managing operational risk involves identifying, assessing, monitoring, and controlling risks; specific approaches depend on the size of the bank, its technological capabilities, and the complexity of its activities. Key elements of a successful framework include a clear strategy, oversight by management, a culture of operational risk awareness, and internal controls (Basel Committee on Banking Supervision, 2010). Effective management of operational risks enables banks to reduce losses and improve operations.

There are four main factors in managing operational risks: process; application at all organizational levels; the need for qualitative and quantitative data; and sponsorship from top hierarchy (Mestchian, 2003). Managing these risks encompasses efficient resource utilization, process improvement, clear internal controls, and information sharing (Mestchian, 2003). Basel II emphasizes operational risk as a response to increased complexity in the banking sector and links capital requirements with how actual risks are managed (Bies, 2006). According to Marshall (Marshall, 2001), the process of managing operational risk includes defining objectives; identifying critical risks; assessing; analyzing; implementing management activities; and monitoring and reporting.

The assumptions for managing operational risk are defined in Basel II, which encompasses the bank as a whole and all levels of management. This framework is described in two documents: "Sound Practices for Managing Operational Risk" (Basel Committee on Banking Supervision, 2003) and Basel II (Basel Committee on Banking Supervision, 2010).

Furthermore, there are two approaches to managing operational risk: quantitative and qualitative. The quantitative approach includes three basic models for calculating capital requirements that differ by their level of sensitivity to risk (the basic approach; standardized approach; and advanced measurement approach).

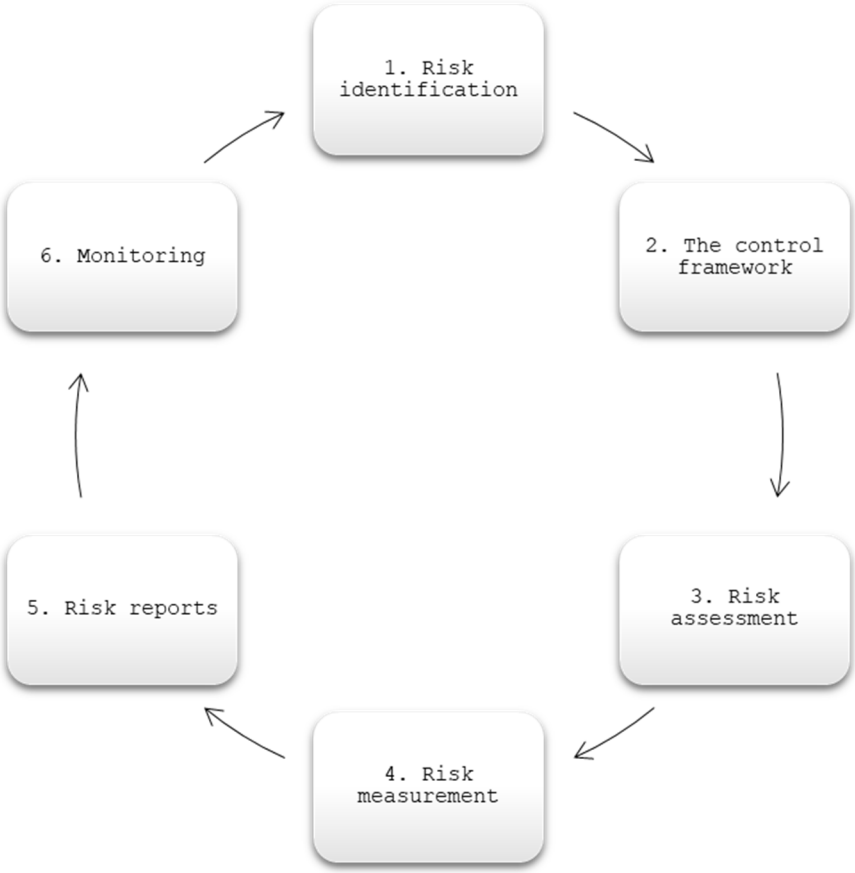
The qualitative approach encompasses ten principles that banks should adopt including enhancing board awareness regarding operational risk; effective internal audit; defining responsibilities for all employees; and regular monitoring of operational risk profiles. Additionally, banks should have strategies for controlling operational risk; contingency plans for unforeseen circumstances; business continuity plans; and disclose information enabling assessment of their operational risk management approach (Basel Committee on Banking Supervision, 2010).

According to these principles, the framework for managing operational risk consists of four core components: strategy; process; infrastructure; and environment. Establishing an operational risk management framework begins with defining the bank's strategy which includes objectives; governance model; and policies. According to Basel II guidelines, strategy should define objectives; risk appetite; an organized approach to risk management; and corresponding responsibilities.

The process for managing operational risk represents another key component of this framework consisting of six parts illustrated in the following figure (Figure 1).

Prosinac	2024	Broj 24	IX. godina izdavanja
December	2024	Number 24	IX.Year of publishing
ISSN 1849-9686		UDK/UDC 330.1(05), 30(05)	

Figure 1. The process of managing operational risk



Source: author based on Basel Committee on Banking Supervision (2010)

Risk identification involves determining all potential risks that a bank may face. It is crucial to understand the types of risks that exist and their impact on the bank's operations. Risk identification tools often include risk mapping, which helps gather information about exposure, type, and intensity of risks.

The control framework defines the best approach for managing identified risks, including assessing existing controls and the costs of implementing new ones, while focusing on risks that can be managed without additional expenses. Controls may include periodic reviews, monitoring, mitigation, and assurance.

Risk assessment refers to a qualitative process that results in a risk profile for the bank, along with a description of responsibilities and an activity plan that must be approved by senior management. This includes analyzing exposure to risk, the effectiveness of controls, and weaknesses in the risk management framework (Alexander, 2003).

In the *risk measurement* phase, various types of measures can be utilized, such as key risk indicators, historical loss data, causal models, and capital models. The goal is to provide more information about control outcomes and changes in the risk profile over time (Cruz, 2002).

The next phase encompasses *reports* on business lines, internal loss data, and key risk indicators, which must be tailored for management to ensure transparency and informed decision-making (Alexander, 2003).

In the *monitoring phase*, the focus is on trend analysis and accountability, where management needs to consider all risk measures and assessment results to maintain control over operational risks (Basel Committee on Banking Supervision, 2010).

3. OPERATIONAL RISK RELATED TO FRAUD

One of the significant categories of operational risk in banking is fraud: both internal and external fraud. Understanding this category is crucial for effective risk management and ensuring the stability of financial institutions. The difference between these two categories is evident in their causes, perpetrators, and consequences; however, they share the commonality of unauthorized acquisition of assets or financial resources. According to the Decision on the Adequacy of Capital Guarantees (HNB, 2009), internal fraud refers to losses arising from unauthorized actions, fraudulent activities, embezzlement, theft, misappropriation of assets, or other violations of regulations and/or internal acts of a credit institution involving at least one internal party. In contrast, external fraud encompasses losses resulting from actions taken with fraudulent intent by third parties.

Internal fraud typically involves employees of an institution who have access to sensitive information or systems that allow them to manipulate data or resources. According to research conducted by KPMG (KPMG, 2014), 74% of organizations reported some form of fraud, with internal fraud being a common cause. Additionally, a PwC report indicates that internal risks are one of the main challenges faced by banks, revealing that 37% of organizations consider internal fraud to be the most significant form of fraud (PwC, 2020).

When it comes to external fraud, perpetrators can be various individuals outside the institution—clients, suppliers, criminals, etc. Besides traditional bank robberies, advancements in technology have led to these frauds often involving sophisticated techniques (e.g., phishing, skimming, or malware) for unauthorized access to banking systems or information. According to a report by the Anti-Phishing Working Group (2021), the number of phishing attacks has significantly increased in recent years, with banks being among the most frequent targets. A McAfee study shows that cyberattacks, including phishing schemes, have caused losses amounting to $1 trillion, with the banking sector being the most affected (McAfee, 2020).

An example of operational risk losses from external fraud in Croatia is the robbery of Zagrebačka banka that occurred on April 23, 1996. Two armed robbers intercepted a bank vehicle in Zagreb. The robbers managed to disarm the drivers and security personnel under threat of weaponry and escaped with 5.5 million kuna in various currencies that were never recovered along with the perpetrators (24 sata, 1996). From an operational risk perspective, this event can be analyzed at several levels:

- Internal Processes and Controls:

It can be concluded that there were weaknesses in the bank's internal controls and procedures as well as inadequate protective measures such as poorly developed security protocols or insufficient employee training.

- External Events:

The robbery is considered an external event disrupting the bank's operations.

- Reputational Risk:

Reputational risk is closely linked to operational risk since damage to a bank's reputation further complicates recovery after an incident.

Both internal and external fraud can have serious impacts on financial institutions as losses incurred due to fraud affect profitability and undermine client trust and the bank's reputation. According to a report from 2022, total losses caused by fraud in banking are expressed in billions of dollars; this trend is expected to continue with increasing digitalization (ACFE, 2022). Recommendations from the World Economic Forum suggest that banks should develop strategies through implementing sophisticated technologies for data analysis; training employees on recognizing fraud; as well as establishing clear procedures for reporting and investigating suspicious activities (World Economic Forum, 2022).

CONCLUSION

This paper analyzed key aspects of managing operational risk in banking operations with a particular emphasis on the category of operational risk related to fraud. By reviewing regulatory frameworks and practical examples, it highlighted the importance of effective internal controls and advanced technology applications in combating increasingly complex threats facing banks' operations. The growing digitalization encompassing the financial sector has brought more sophisticated opportunities for fraud; thus managing operational risk has become more complex and demanding. Due to escalating challenges faced by banks in maintaining high standards against internal and external frauds, they are compelled to continuously adapt and invest in new technologies and employee education.

Based on the analysis conducted, it can be concluded that the hypothesis stating that effective management of operational risk can reduce losses

from fraud—requiring advanced technologies and strong internal controls due to increasingly complex threats—has been confirmed. As the banking sector faces ever more intricate dangers associated with internal and external frauds as well as other types of operational risks, it is essential that measures taken by banks in preventing these risks must be dynamic and adaptable in order to adequately respond to new challenges within the financial environment.

IZVORI

1. Alexander, C. (2003). Statistical Models of Operational Risk. In: Alexander, C. *Operational Risk Regulation, Analysis and Management*. London: FT Prentice Hall, pp. 348.
2. Association of Certified Fraud Examiners (ACFE). (2022). 2022 Report to the Nations. Available at: https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2022/2022-report-to-the-nations.pdf [Accessed 17 September 2024].
3. Basel Committee on Banking Supervision (BCBS). (2011). *Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches*. Available at: https://www.bis.org/publ/bcbs195.pdf [Accessed 19 September 2024].
4. Basel Committee on Banking Supervision. (2003). *Good Practices for Operational Risk Management and Supervision*. Available at: http://www.hnb.hr/supervizija/papiri-bazelske-komisije/h-dobre-prakse-za-upravljanjem-operativnim-rizikom.pdf [Accessed 17 September 2024].
5. Chernobai, A.S., Fabozzi, F.J., and Rachev, S.T. (2007). *Operational Risk: A Guide to Basel II Capital Requirements, Models, and Analysis*. John Wiley & Sons, Inc.
6. Cruz, M. (2002). *Modeling, Measuring and Hedging Operational Risk*. New York: John Wiley & Sons.
7. Gačević, M., and Dragosavac, M. (2023). Operational Risk in Digital Business, *SKEI – International Interdisciplinary Journal*, 4(2), pp. 58-67. Available at: https://hrcak.srce.hr/311410 [Accessed 18 September 2024].
8. Croatian National Bank. (2010). *Decision on the Adequacy of the Guarantee Capital of Credit Institutions*. Available at: http://www.hnb.hr/propisi/odluke-nadzor-kontrola/odluke-zoki-veljaca-2010/h-odluka-o-adekvatnosti-jamstvenoga-kapitala-ki.pdf [Accessed 18 September 2024].
9. Croatian National Bank (HNB). *Decision on the Adequacy of the Guarantee Capital of Credit Institutions*. Narodne novine no. 1/2009, 75/2009, 2/2010, 118/2011, 2013.
10. KPMG. (2014). *The Global Anti-Money Laundering Survey*. Available at: https://kpmg.com/mt/en/home/insights/2014/01/global-anti-money-laundering-survey.html [Accessed 19 September 2024].
11. McAfee. (2020). *The Hidden Costs of Cybercrime*. Available at: https://www.mcafee.com/blogs/other-blogs/executive-perspectives/the-hidden-costs-of-cybercrime-on-government/ [Accessed 19 September 2024].
12. Mestchian, P. (2003). *Operational Risk Management: The Solution is in the Problem*. In: *Advances in Operational Risk*. London: Risk Books in association with SAS UK, pp. 3-16.
13. PwC. (2020). *Global Economic Crime and Fraud Survey*. Available at: https://www.pwc.com/ua/en/survey/2020/economic-crime-survey.html [Accessed 17 September 2024].
14. Bies, S. S. (2006). An update on regulatory issues. Remarks at the Banking Institute, Charlotte, March 31. Available at: https://www.bis.org/review/r060405e.pdf [Accessed 17 September 2024].
15. Wiggins, R.Z., Piontek, T., and Metrick, A. (2019). "The Lehman Brothers Bankruptcy A: Overview." *Journal of Financial Crises*, 1(1), pp. 39-62. Available at: https://elischolar.library.yale.edu/journal-of-financial-crises/vol1/iss1/2 [Accessed 17 September 2024].
16. World Economic Forum. (2022). *The Global Risks Report*. Available at: https://www.weforum.org/publications/global-risks-report-2022/ [Accessed 19 September 2024].