BG Pulse Journal USA
ISSN:1947-2536 http://www.bgpulseusa.com/index.php/bg

MANAGEMENT OF OPERATIONAL RISKS IN COMMERCIAL BANKS

Nishanov Shoazam Baxramovich
Tashkent University of Applied Sciences
Candidate of Economic Sciences, Department of Banking and Finance
doi:https://doi.org/10.5281/zenodo.22938046

Abstract: This article examines the theoretical and practical aspects of operational risk management in commercial banks. Operational risk is associated with inadequate or failed internal processes, human errors, information systems, external events, and other factors that may negatively affect banking activities. The article analyzes the main sources of operational risks, methods for their identification, assessment, monitoring, and mitigation. Particular attention is paid to the role of internal control, risk management systems, information technologies, cybersecurity, business continuity, and employee competence in reducing operational risks. The study also emphasizes the importance of developing an integrated operational risk management system based on international principles and the specific characteristics of commercial banks. The results show that effective operational risk management contributes to financial stability, continuity of banking services, protection of customer interests, and strengthening public confidence in the banking system.
Keywords: operational risk, commercial banks, risk management, internal control, cybersecurity, banking system, information technology, business continuity, risk assessment, internal processes.

INTRODUCTION

The development of the modern banking sector is accompanied by the expansion of financial services, digital technologies, electronic payment systems, remote banking, and automated decision-making mechanisms. These processes create new opportunities for commercial banks but simultaneously increase their exposure to various operational risks. Failures in internal processes, employee mistakes, technological disruptions, cyberattacks, fraud, and external events can interrupt banking operations and result in significant financial and reputational losses.

Operational risk is fundamentally different from traditional financial risks such as credit, market, and liquidity risks. While financial risks are generally associated with changes in financial conditions, operational risk may arise from almost any stage of a bank's activities. Therefore, its effective management requires a comprehensive approach that covers organizational processes, human resources, information technologies, internal control, cybersecurity, and business continuity.

The relevance of operational risk management has increased particularly with the rapid digitalization of banking services. The growing use of mobile applications, online banking, cloud technologies, automated payment systems, and electronic identification has increased the importance of technological resilience and information security. Consequently, commercial banks need to develop risk management mechanisms that can identify potential operational failures before they lead to serious consequences.

The purpose of this article is to analyze the main characteristics of operational risks in commercial banks and examine effective approaches to their identification, assessment, monitoring, and mitigation.

LITERATURE REVIEW AND METHODOLOGY

Operational risk management has become an important area of banking risk management research. One of the widely recognized approaches defines operational risk as the risk of loss resulting from

inadequate or failed internal processes, people and systems, or from external events. This definition emphasizes that operational risk can originate both within the organization and outside it.

The Basel Committee on Banking Supervision has played an important role in establishing international approaches to operational risk management. The Basel framework emphasizes the importance of effective governance, risk identification, measurement, monitoring, and control. In this context, commercial banks are expected to establish appropriate internal mechanisms for managing operational risks and maintaining adequate resilience.

Operational risk may arise from several major sources. The first source is internal processes. Poorly designed procedures, inadequate segregation of duties, insufficient documentation, and weaknesses in internal controls may create significant operational vulnerabilities. The second source is human factors. Employee mistakes, insufficient qualifications, intentional misconduct, fraud, and violations of internal procedures can result in financial and reputational losses.

The third source is information technology. System failures, software errors, data loss, network interruptions, and inadequate technological infrastructure may prevent banks from providing services to customers. The fourth source is external **events**, including natural disasters, infrastructure failures, criminal activities, and other circumstances beyond the direct control of a bank.

The methodology of this study is based on theoretical analysis, comparative analysis, system analysis, and generalization of scientific and regulatory approaches to operational risk management. These methods make it possible to identify the main sources of operational risk and determine the key mechanisms for reducing their potential impact.

DISCUSSION AND RESULTS

Operational risks in commercial banks are diverse and interconnected. Their classification according to the main source makes it easier to identify vulnerabilities and develop appropriate mitigation measures.

Human-related risks are among the most common operational risks. Bank employees are involved in almost all banking processes, from customer service and transaction processing to risk assessment and information management. Errors in data entry, incorrect transaction processing, failure to follow procedures, and unauthorized actions may lead to financial losses.

Process-related risks occur when internal procedures are poorly designed, inadequately documented, or improperly implemented. For example, weaknesses in authorization procedures or insufficient separation of responsibilities may increase the possibility of fraud and operational errors.

Technology-related risks have become increasingly significant as banks expand digital services. Technical failures, software vulnerabilities, cyberattacks, data breaches, and disruptions in electronic payment systems may affect the continuity of banking operations.

External risks include natural disasters, power outages, telecommunications failures, and other events that may disrupt the normal functioning of a bank. Although banks cannot always prevent such events, they can reduce their consequences through effective business continuity and disaster recovery plans.

An effective operational risk management system begins with the timely identification of potential risks. Commercial banks should regularly analyze their business processes and determine areas where operational failures are most likely to occur.

One important instrument is the Risk and Control Self-Assessment (RCSA). This approach allows organizational units to identify operational risks associated with their activities and assess the effectiveness of existing controls.

Another important instrument is the use of Key Risk Indicators (KRIs). These indicators allow banks to monitor changes in operational risk exposure. Examples include the number of system failures, customer complaints, processing errors, cybersecurity incidents, and unauthorized transactions.

Banks can also use historical loss data to identify recurring operational problems. Analysis of previous incidents helps determine the causes of losses and develop preventive measures.

Internal control represents one of the fundamental elements of operational risk management. An effective internal control system should ensure that banking operations are performed according to established procedures and regulatory requirements.

The separation of duties is particularly important. Employees responsible for initiating transactions should not necessarily be responsible for approving or recording the same transactions. Such segregation reduces the possibility of errors and fraudulent activities.

Regular internal audits also contribute to the identification of weaknesses in operational processes. Audit findings can provide management with information necessary to strengthen controls and improve risk management practices.

The digital transformation of banking has significantly changed the operational risk environment. Commercial banks increasingly depend on information systems for payment processing, customer identification, account management, lending, and communication.

Consequently, cybersecurity has become an essential component of operational risk management. Banks need to protect their systems against unauthorized access, malware, phishing, data theft, and other cyber threats.

Effective cybersecurity requires a combination of technological and organizational measures. These may include access controls, authentication mechanisms, data encryption, system monitoring, regular security assessments, employee training, and incident response procedures.

Banks should also establish procedures for rapid recovery after technological failures. Backup systems, data recovery mechanisms, alternative communication channels, and disaster recovery plans are important components of operational resilience.

Business continuity management is particularly important for commercial banks because interruptions in banking services can affect a large number of customers and financial transactions.

A business continuity plan should identify critical banking functions, possible disruptions, responsible personnel, alternative operational procedures, and recovery priorities. Regular testing of these plans is necessary to determine whether they are sufficiently effective.

Business continuity should not be regarded as a separate technical function. It should be integrated into the overall risk management framework of the bank.

The effectiveness of operational risk management depends significantly on employees. Even advanced technological systems cannot completely eliminate risks arising from human behavior.

Therefore, banks should regularly train employees in operational procedures, information security, fraud prevention, and risk awareness. Employees should clearly understand their responsibilities and the potential consequences of violating internal policies.

An effective risk culture encourages employees to identify and report potential problems rather than conceal them. Management should create an environment in which operational incidents are analyzed objectively and used as a basis for improving internal processes.

The analysis demonstrates that operational risk cannot be managed effectively through a single instrument. Commercial banks need an integrated system combining risk identification, assessment, monitoring, control, reporting, and continuous improvement.

This approach enables banks to move from a reactive model, in which risks are addressed only after losses occur, toward a proactive model focused on preventing operational failures.

The integration of operational risk management with information technologies can further improve the efficiency of this process. Automated monitoring systems can identify unusual transactions, system failures, and other risk indicators in real time.

CONCLUSION AND RECOMMENDATIONS

Operational risk management is an essential component of the overall risk management system of commercial banks. Operational risks may arise from internal processes, employees, information technologies, external events, and other factors. Their effective management requires a systematic and continuous approach.

The analysis shows that commercial banks should strengthen internal controls, improve employee training, develop effective cybersecurity systems, regularly assess operational risks, and maintain reliable business continuity plans. Particular attention should be given to the digital transformation of banking services because technological dependence creates both new opportunities and new operational vulnerabilities.

The following recommendations can be proposed:

1. Commercial banks should establish comprehensive operational risk management frameworks integrated with their overall risk management systems.
2. Risk and Control Self-Assessment procedures should be regularly conducted to identify weaknesses in banking processes.
3. Key Risk Indicators should be developed and monitored systematically.
4. Internal control mechanisms and segregation of duties should be strengthened to reduce errors and fraudulent activities.
5. Banks should continuously improve cybersecurity systems and conduct regular information security assessments.
6. Employee training in operational risk, cybersecurity, fraud prevention, and internal procedures should be conducted regularly.
7. Business continuity and disaster recovery plans should be regularly tested and updated.
8. Digital technologies and automated monitoring systems should be used to detect operational risks at an early stage.
9. Operational incidents and losses should be systematically analyzed to identify their root causes and prevent their recurrence.
10. Risk management should become an integral part of the organizational culture of commercial banks.

In general, an effective operational risk management system can contribute to the stability and continuity of banking activities, reduce potential losses, protect customers, and strengthen confidence in commercial banks. The integration of organizational, technological, financial, and human-resource measures provides a comprehensive basis for improving the resilience of the modern banking sector.

REFERENCES

1. Basel Committee on Banking Supervision. Principles for the Sound Management of Operational Risk. Bank for International Settlements.
2. Basel Committee on Banking Supervision. Basel III: Finalising Post-Crisis Reforms. Bank for International Settlements.

3. Basel Committee on Banking Supervision. Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches. Bank for International Settlements.
4. Hull, J. C. Risk Management and Financial Institutions. Wiley.
5. Moosa, I. A. Operational Risk Management. Palgrave Macmillan.
6. Crouhy, M., Galai, D., Mark, R. The Essentials of Risk Management. McGraw-Hill.
7. Jorion, P. Financial Risk Manager Handbook. Wiley.
8. International Organization for Standardization. ISO 31000: Risk Management – Guidelines. Geneva: ISO.
9. International Organization for Standardization. ISO 22301: Security and Resilience – Business Continuity Management Systems. Geneva: ISO.