DOI: https://doi.org/10.59503/29538009-2024.2.14-183

FEATURES OF OPERATIONAL RISK MANAGEMENT IN THE REPUBLIC OF ARMENIA

Jemma Poghosyan

Armenian State University of Economics,
Ph.D. student
poghosyanjema@mail.ru

Abstract: Any type of business activity is not free from the formation of risks. Banking is also no exception. For banking business, it is important not to avoid risks in general, but to anticipate the consequences of risks and minimize their consequences. This article presents the main mechanisms for containing operational risks of banks, taking into account possible scenarios and changes. The goal is to find out how risks are managed and the possible limits of risk indicators. Forecasts of key operational risk indicators are based on banking experience and historical data, which makes it possible to monitor potential risk thresholds. According to the author, with precise management, the latter can help differentiate and limit potential risks.

Keywords: bank, operational risk, legal risk, risk indicators, cyber security, risk appetite

JEL code: G21

Research aims: The operational risk management process is continuous, and the results are embodied in decisions taken to accept, reduce or eliminate risks that affect the achievement of goals.

Research novelty: Cyber security plays a great role as a risk factor, the main purpose of which is to ensure the continuous, uninterrupted and secure use of information systems and critical information infrastructure.

Introduction

In the current reality, economically developed countries carry out a wide range of banking operations, one of the main tasks of which is to manage potential risks. Risk management is an important concept related to security and financial integrity, and operational risk assessment is an important part of its strategic development.

For banking, it is important not to avoid risks in general, but to predict the consequences of risks and minimize their results. In order to make a profit and take a decent position in the market, the bank must seek and apply effective methods and tools to manage these risks. Therefore, as long as banks and banking functions exist, risk management, regulatory and control mechanisms of the bank will always be important. Operational risk management is especially relevant, which is currently one of the most important factors in ensuring the stability of the banking system. Every activity, whatever it is, involves a part of the risk, is subject to uncertainty associated with changes in the market. Risk is a part of any human activity. The word "risk" comes from the Greek word "ridiscon", in the Italian

dictionary "risico" it means danger. In Webster's dictionary, risk is defined as danger, damage, and the likelihood of incurring losses (Babayan, V., 2003).

Research results

Operational risk is the probability of losses arising as a result of inadequate or unsuccessful internal processes, systems and human factors or external factors that may have a direct or indirect negative impact on the bank's capital and/or profit. Operational risk also includes legal risk. Legal risk is the likelihood that contractual provisions, lawsuits, court decisions, rulings or other legal procedures will interrupt or have a negative impact on the bank's operations.

The purpose of the organization of the operational risk management system is:

- ✓ Preventing the occurrence of operational risk,
- ✓ Reduction of possible losses of the bank caused by the occurrence of events caused by internal and external factors),
- ✓ ensuring the continuity and normal process of the bank's activities,
- ✓ reserve formation and optimization of processes to cover possible future losses,
- ✓ Operational risk control,
- ✓ To achieve the above objectives, the operational risk management system is aimed at solving the following main tasks,
- ✓ Identification, assessment and analysis of operational risks

- ✓ Regular monitoring of accidents and incidents related to operational risks,
- ✓ Implementation of a system of warning indicators of operational risks, monitoring in relation to them,
- ✓ Raising awareness of operational risks in the bank,
- ✓ Reducing operational risks, including through the introduction of standardized functions and the maximum possible automation of banking processes,
- ✓ Improving the efficiency of banking processes

The bank has three defenses of operational risk management control: (Operational and integrated risk Management Exam Part 2, 2016)

1) Control level 1: All divisions of the bank in which operational risk exists or may arise, which assume risks directly, are responsible for them and inform those responsible for risk management,

2) Control level 2: Persons responsible for risk management, who generally coordinate operational risks,

3) Control level 3: An internal audit that evaluates the effectiveness of the components of the risk management system:

In the current reality, there is a dynamic increase in risks also as a result of external factors, in which the role of cyber security is also great, the main purpose of which is to ensure the continuous, uninterrupted and secure use of information systems and critical information infrastructures through the introduction of effective cyber security tools.

Cyber security: A set of organizational, technical, and software tools that ensure access, integrity, and confidentiality of information

that is processed, stored, and transmitted in a computer, computer equipment, digital memory disks, information system, critical information infrastructure, electronic communications network, from accidental loss, unauthorized access, use, disclosure, hacking, changes, losses, destruction, attacks, copying, writing, damage /losses resulting from proliferation and other unlawful interference/ (The Law of the Republic of Armenia on Cyber security, Draft, 2023).

Depending on the assessments of individual risk factors and trends (directions) that may arise, mostly the overall risk assessment is formed in accordance with the Table 1. Each bank sets its own risk assessment criteria.

Table 1. Risk assessment criteria

The direction of risk	**General risk assessment**			
	Low	**Average**	**Above average**	**High**
Decreasing	Low	Low	Average	High
Stable	Low	Average	Above average	High
Increasing	Average	Above average	High	High

When determining the direction of risk, risk factors that require and do not require a technical solution are considered separately. In the case of risk factors requiring a technical solution, the direction of risk is determined in the manner described below:

✓ Increase: The direction of risk is considered increased if there are still technical gaps associated with the occurrence of this accident, sufficient control mechanisms have not been implemented to manage the risk and there is a high probability that the accident will happen again,

✓ Stable: The direction of risk is considered stable if there are still technical gaps associated with the occurrence of this accident, but sufficient control mechanisms have been implemented to manage the risk, thanks to which the probability of a recurrence of the risk is practically eliminated,

✓ Decrease: The direction of risk is considered downward if there are no technical gaps associated with the occurrence of this accident, sufficient control mechanisms have been implemented to manage the risk and the probability that the accident will happen again is low.

In the case of risk factors that do not require a technical solution, the direction of risk is determined as follows:

- ✓ Increase: The direction of risk is considered to be increasing if, due to the occurrence of this accident, sufficient control mechanisms have not been implemented to manage the risk and there is a high probability that the accident will happen again,
- ✓ Stable: The direction of risk is considered stable if the mechanisms for excluding this accident are not fixed by internal legal acts regulating the process, but control is carried out in accordance with business habits,
- ✓ Decrease: The direction of risk is considered decreasing if the mechanisms for excluding this incident are fixed by internal legal acts regulating the process and are actually implemented.

The Bank applies the following mechanisms to reduce the level of operational risk:

- ✓ Standardization of banking operations and other operations (including the development of internal legal acts, the development of standard contracts, procedures, procedures, technologies for operations and transactions),
- ✓ Implementation of a system of additional and subsequent control, systems of ongoing verification of transactions and operations,
- ✓ Definition of the processes of development and approval (coordination) of internal legal acts,
- ✓ Ensuring the necessary level of staff qualifications, continuous improvement,
- ✓ Automation of banking processes and technologies, especially in areas related to standard functions and a large amount of work.,
- ✓ Allocation of responsibilities based on workload,,
- ✓ Double checking of the performed operations (the principle of "two eyes"), setting appropriate approval limits in the processes,
- ✓ Insurance of risks for individual losses (conclusion of a comprehensive insurance contract for bank risks with an insurance company licensed by the Central Bank of the Republic of Armenia).

An important factor for the implementation of an effective operational risk management system is also the priority types of risks based on the international experience and approach of the Central Bank of Armenia.

Table 2. Types of operational risks

No.	Types of operational risk
1	Risks related to customers, products and business behavior
2	Risks associated with the implementation of processes, management of functions
3	The risk of information systems failure
4	Cybercrime and information security
5	AML risk
6	Internal fraud
7	External fraud
8	Legal risk
9	Outsourcing
10	Geopolitical ris
11	Loss, damage to material assets
12	Stricter regulation, sanctions
13	Risks arising as a result of employment relations, remuneration policy

In parallel with the implementation of loss control from operational risks, a system of warning indicators was introduced, the change in values of which allows you to predict the amount of losses associated with operational risks. Of course, each bank can

set different thresholds depending on the strategy and software features. According to international experience, as well as its historical series established for this bank, the bank sets acceptable thresholds for risk options for each factor, which contribute to a more complete understanding of the level of operational risk.

Risk is an inherent phenomenon that accompanies all actions and functions available in the bank, and arises or does not arise depending on the conditions created for this. The risk can cause negative consequences that worsen the quality of management decisions, reduce the amount of profit and affect the functionality of the organization, which may even lead to blocking the execution of activities.

Inherent risk is a risk that naturally exists in any activity and is defined as "a risk that exists until internal control measures are taken to reduce it" or "all risks that threaten the organization and may be internal or external risks, measurable or immeasurable".

Residual risk is the risk remaining after the implementation of internal control measures. The application of these measures should lead to limiting the inherent risk at a level acceptable to the organization. The residual risk must be controlled in order to maintain it at acceptable levels. Risk appetite is the level of exposure that an organization is willing to accept. Risks cannot be avoided, and it is necessary to assess them by keeping them "under control", keeping risks at levels that the organization considers acceptable, acceptable, and not always striving to completely eliminate them, since this can lead to other unexpected and uncontrollable risks. In case of risk reduction or transfer, the bank manages to limit the risk to a level corresponding to the bank's appetite.

The bank decides to simply take on the risk if its level already matches the bank's appetite. And, in the end, risk is a choice, not a final option.

Conclusion

Risk definitions can be listed with ten other definitions, as a result of the analysis of these definitions, the following conclusions can be drawn.

Probability versus consequences: While some definitions of risk focus only on the probability of an event occurring, other definitions are more comprehensive, covering both the probability of risk occurrence and the consequences of the event.

When defining a concept, it is necessary to distinguish between risk and threat.

- ✓ A threat is an event whose probability of occurrence is low, but the negative consequences are high, since the probability of occurrence in these cases is difficult to assess.
- ✓ Risk is an event with a high probability of occurrence, for which there is enough information to assess the probability and consequences.

Operational risk can be defined as a problem (situation, event, etc.) that has not yet arisen, but may arise in the future, threatening the achievement of results. The impact of risk is a consequence of the result when the risk is realized. If the risk is a threat, the consequences of the result are negative, and if the risk is an opportunity, the consequences are positive.

The role varies depending on when the analysis is performed.

- ✓ If a risk assessment is carried out before the risk is realized, the goal is to avoid the occurrence of this event;

- ✓ If a risk assessment is carried out after the risk has been realized, the goal is to ensure the development of the activity and the continuity of the activity.

References:

1. Operational Risk Management Policy of Armenian Banks, (cba.am)
2. ***Babayan. V.*** (2003). Basics of banking, Yerevan, p. 40, (in Armenian)
3. Regulation 4 "Minimum conditions for the implementation of internal banking control" of the Central Bank Armenia, pp. 51-52. Microsoft Word - vor 102-n.doc (cba.am), 2013
4. The Central Bank's of Armenia Operational Risk Management Guidelines, pp. 5-13. Operationa risk management manual.pdf (cba.am)
5. The Law of the Republic of Armenia on Cyber security, pp. 1-2.
6. Operational and integrated risk Management Exam Part 2, 2016.
7. https://www.udemy.com/course/introduction-to-operational-risk-management-orm/
8. https://www.coursera.org/learn/operational-risk-management
9. Official Website of Central Bank of RA https://www.cba.am
10. The three lines of defense (kpmg.com)

ԳՈՐԾԱՌՆԱԿԱՆ ՌԻՍԿԵՐԻ ԿԱՌԱՎԱՐՄԱՆ ԱՌԱՆՁՆԱՀԱՏԿՈՒԹՅՈՒՆՆԵՐԸ ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅՈՒՆՈՒՄ

Ջեմմա Պողոսյան
Հայաստանի պետական տնտեսագիտական համալսարան,
ասպիրանտ

Բանալի բառեր - բանկ, գործառնական ռիսկ, իրավական ռիսկ, ռիսկի ցուցանիշներ, կիբերանվտանգություն, ռիսկի ախորժակ

Ձեռնարկատիրական գործունեության ցանկացած տեսակ զերծ չէ ռիսկերի ձևավորումից: Բանկային գործունեությունը նույնպես բացառություն չէ: Բանկային գործունեության համար կարևոր է ոչ թե խուսափել ռիսկերից, այլ կանխատեսել ռիսկերի հետևանքները և նվազագույնի հասցնել դրանք: Հոդվածը ներկայացնում է բանկերի գործառնական ռիսկի հիմնական զսպողական մեխանիզմները՝ հաշվի առնելով հնարավոր սցենարներն ու փոփոխությունները: Նպատակն է պարզել, թե ինչպես է իրականացվում գործառնական ռիսկերի կառավարումը և ռիսկի ցուցանիշների հնարավոր սահմանների կառավարումը:

Այն ուղղված է բանկի ակտիվների պահպանմանը, բանկի գործունեության անընդհատության ապահովմանը, բանկի գործունեությանը ներհատուկ ռիսկերի ժամանակին բացահայտմանը, գնահատմանն ու շարունակական կառավար-

մանը, հաշվապահական հաշվառ-ման և ֆինանսական հաշվետվությունների՝ գործող ստանդարտներին համապատասխանության ապահովմանը, իրականացվող գործառնությունների արդյունավետության բարձրացմանը, բանկի գործունեության համապատասխանության ապահովմանը գործող օրենսդրությանը և բանկի ներքին իրավական ակտերին:

Գործառնական ռիսկի հիմնական ցուցանիշների կանխատեսումները կատարվում են հիմնվելով բանկային փորձի և պատմական շարքերի վրա, որոնք հնարավոր են դարձնում վերահսկել հնարավոր ռիսկային շեմերը:

Հեղինակի կարծիքով ճշգրիտ կառավարման դեպքում վերջիններս կարող են օգնել տարբերակել և սահմանափակել հնարավոր ռիսկերը:

Submitted: 09.10.2024; Revised: 27.10.2024; Accepted: 08.11.2024