Jakhongir Rabbimov
Independent researcher at
Tashkent State University of Economics

RISK AND CONTROL SELF ASSESSMENT (RCSA) IN UZBEK BANKS: CHALLENGES AND OPPORTUNITIES

ABSTRACT

This article explores the adoption of RCSA practices within the Uzbek banking sector, shedding light on the distinct challenges and emerging opportunities in this dynamic market. Also, the paper describes key challenges such as insufficient technological infrastructure, limited expertise in risk management methodologies, and the complexities of adapting to evolving regulatory frameworks. Conversely, opportunities lie in adopting advanced technological solutions, harmonizing practices with international standards, and incorporating innovative approaches. The study underscores the importance of RCSA in fostering a culture of accountability, this approach helps make banking operations more efficient. The research offers practical recommendations for integrating RCSA into banking operations. These suggestions aim to strengthen risk management practices to guide financial institutions in advancing risk resilience and supporting the sustainable development of Uzbekistan's banking sector.

ANNOTATSIYA

Mazkur maqolada O'zbekiston bank sektorida RCSA (xatarlarni nazorat qilish va o'z-o'zini baholash) amaliyotini joriy etish masalasi o'rganilgan bo'lib, ushbu sohadagi muayyan muammolar va yuzaga kelayotgan imkoniyatlar yoritilgan. Shuningdek, maqolada mavjud muammolar - yetarli texnologik infratuzilmaning yo'qligi, xatarlarni boshqarish metodologiyalarida yetarli tajribaning mavjud emasligi va o'zgarib borayotgan normativ-huquqiy talablar bilan moslashishning murakkabligi - haqida so'z boradi. Aksincha, zamonaviy texnologik yechimlarni joriy etish, xalqaro standartlar bilan uyg'unlashuv va innovatsion yondashuvlarni integratsiya qilish sohadagi muhim imkoniyatlar sirasiga kiradi. Tadqiqotda RCSA tizimining hisobdorlik madaniyatini shakllantirishdagi roli ta'kidlanadi, bu esa bank faoliyatini samaraliroq qiladi. Shuningdek, maqolada RCSA amaliyotini bank ish faoliyatiga integratsiyalashga oid amaliy tavsiyalar berilgan. Ushbu tavsiyalar moliyaviy institutlarga xatarlar barqarorligini mustahkamlash va O'zbekiston bank sektorining barqaror rivojlanishiga hissa qo'shishda yo'l-yo'riq beradi.

АННОТАЦИЯ

В данной статье рассматривается внедрение практики RCSA (оценка рисков и контроль на уровне подразделений) в банковском секторе Узбекистана, а также освещаются ключевые проблемы и новые возможности на этом динамично развивающемся рынке. В частности, в работе обозначены такие вызовы, как недостаточная технологическая инфраструктура, ограниченный опыт в области методов управления рисками и сложность адаптации к изменяющимся нормативным требованиям. В то же время открываются перспективы внедрения передовых технологических решений, гармонизации с международными стандартами и интеграции инновационных подходов. Исследование подчеркивает важность

RCSA как инструмента формирования культуры ответственности, что способствует повышению эффективности банковских операций. В статье предложены практические рекомендации по интеграции RCSA в деятельность банков, направленные на укрепление системы управления рисками и поддержку устойчивого развития банковского сектора Узбекистана.

KEYWORDS

Risk and Control Self-Assessment (RCSA), Risk Management Practices, Operational risk management systems, Regulatory Compliance, Financial Sustainability

KALIT SO‘ZLAR

Risklarni nazorat qilish va o‘z-o‘zini baholash (RCSA), xatarlarni boshqarish amaliyotlari, operatsion xatarlarni boshqarish tizimlari, normativ-huquqiy talablarga muvofiqlik, moliyaviy barqarorlik.

КЛЮЧЕВЫЕ СЛОВА

Оценка рисков и контроль на уровне подразделений (RCSA), практика управления рисками, системы управления операционными рисками, соответствие нормативным требованиям, финансовая устойчивость.

I. INTRODUCTION

□ Background on the Uzbek Banking Sector

Uzbekistan's banking sector is a cornerstone of the country's financial system, playing a pivotal role in fostering economic growth and supporting key industries. As of 2024, the sector comprises 36 banks, including 9 state-owned, and 27 private, and foreign-owned banks. The state has historically dominated banking activities, particularly through large state-owned banks that primarily focus on financing public sector projects and industries. However, recent reforms initiated under the National Development Strategy 2030 have sought to privatize these institutions, reduce state involvement, and enhance competition. These changes aim to modernize the sector, promote private sector participation, and align financial practices with international standards.

Despite these advancements, the sector faces challenges such as high levels of non-performing loans (NPLs), limited financial inclusion, and outdated risk management practices. These challenges make it essential for banks to develop practical internal frameworks that can effectively manage operational, credit, and market risks.

Although business processes are exposed to numerous risks, it is essential that they remain accurate and consistent. The Risk and Control Self-Assessment (RCSA) is a valuable tool for evaluating these processes and identifying potential weaknesses. Based on the results of the RCSA, banks can effectively formulate action plans to enhance and strengthen their operational procedures.

□ What is a risk and control self-assessment (RCSA)?

In simple terms, a Risk and Control Self-Assessment (RCSA) is a process that helps organizations look closely at their operations, spot potential risks, and check whether their existing controls are working effectively. It is considered one of the most practical tools in risk management because it encourages teams to take ownership of risks before problems escalate.

The idea behind RCSA gained momentum in the early 90s of 20th century, particularly after the Committee of Sponsoring Organizations of the Treadway Commission published important standards on internal controls. Over time, these practices evolved into a recognized method for ensuring compliance with laws such as the Foreign Corrupt Practices Act (FCPA) and for strengthening internal governance across industries.

Financial institutions commonly use RCSA to fulfill regulatory obligations, such as conducting an annual self-assessment of operational risks across the organization. Beyond the financial sector, it is also a useful method for assessing risks associated with third-party vendors.

A significant shift in modern risk management has been the move from a centralized, top-down model to a more integrated, employee-driven approach. As Deddy Jacobus (2015) explains[1], this "new paradigm" places Risk and Control Self-Assessment (RCSA) at the heart of effective enterprise risk management. Instead of relying solely on management to identify and mitigate risks, organizations are encouraged to involve employees across all departments. This participative method not only helps uncover operational risks more accurately but also builds a stronger sense of ownership among staff. By using workshops and structured discussions, RCSA fosters better communication, improves understanding of internal controls, and supports continuous improvements in organizational processes.

□ Importance of Risk Control and Self-Assessment in Banking

Today, RCSA plays a crucial role in how banks manage risks. This approach helps financial institutions spot risks early and take action before they escalate. An effective RCSA framework not only verifies the presence of internal controls but also evaluates whether those controls genuinely mitigate the intended risks and align with the bank's strategic objectives.

Several important aspects illustrate why RCSA has become such an essential part of modern banking risk management:

RCSA allows organizations to identify potential risks before they materialize into significant issues. By empowering employees to assess risks and controls in their areas of responsibility, institutions can address vulnerabilities promptly and implement preventative measures.

RCSA fosters a culture of accountability by involving staff at all levels in the risk management process. When employees take ownership of risk identification and mitigation, it strengthens organizational commitment to maintaining operational integrity.

[1] Jacobus, D. (2015). New paradigm of managing risks: Risk and control self-assessment. *Agriculture and Agricultural Science Procedia, 3*, 32–34. https://doi.org/10.1016/j.aaspro.2015.01.008

In an increasingly regulated financial environment, RCSA helps institutions meet compliance requirements by providing a systematic framework for documenting risks, controls, and mitigation efforts. This ensures readiness for regulatory audits and reduces the risk of penalties for non-compliance.

By providing a clear understanding of risks and the effectiveness of controls, RCSA supports data-driven decision-making. Management can prioritize resource allocation, develop contingency plans, and align risk strategies with the institution's overall goals.

RCSA identifies inefficiencies in processes and controls, enabling organizations to streamline operations and reduce costs. This continuous improvement approach ensures that risk management practices remain agile and effective in a dynamic business environment.

Examples of Major Operational Risk Losses

Throughout recent decades, several high-profile cases have demonstrated how serious operational risks can be for financial institutions:

a) Republic New York Corporation faced a loss of around $611 million as a result of external fraud, one of the largest cases of its kind at the time.
b) Wells Fargo incurred losses totaling $150 million due to failures in transaction processing systems, highlighting the risks associated with technology-driven banking services.
c) Providian Financial Corporation suffered losses estimated at $405 million, stemming from improper billing practices and internal process weaknesses.
d) BNP Paribas was fined approximately $9 billion in 2014 for violating economic sanctions, underlining the importance of compliance and regulatory risk management.

These examples show that operational risks can result not only in substantial financial losses but also in long-lasting reputational damage. They serve as important lessons for all banks aiming to strengthen their internal control environments.

The financial sector is exposed to a constantly evolving risk landscape, including technological disruptions, cybersecurity threats, and market volatility. RCSA equips institutions with the tools to identify and adapt to emerging risks, ensuring resilience and sustainability.

I. LITERATURE REVIEW

Risk and Control Self-Assessment (RCSA) has developed over time as a practical tool for managing operational risks in banks. It became more important as financial institutions started looking for ways to better understand and control risks internally, beyond just relying on external audits. This shift reflects a broader move toward giving more responsibility to banks themselves when it comes to managing risks. This approach was further supported by the Basel II and III regulations, which

encouraged banks to use their own systems to assess and manage operational risks (Basel Committee on Banking Supervision, 2006)[2].

Research has shown that RCSA can help reduce losses and make risk management more transparent. Cruz (2002), for example, highlights that while numbers and data are important, some risks are not captured in past records[3]. RCSA is especially useful in detecting latent risks that traditional metrics or historical data often overlook. Mikes (2009) adds that banks make risk assessments part of their daily decisions tend to build a stronger sense of responsibility and awareness among employees[4].

The use of web-based RCSA applications has also gained prominence, particularly in the context of operational risk management. Yulianto (2019) demonstrates that integrating RCSA into a web-based system facilitates real-time data capture and analysis, which supports continuous risk monitoring and decision-making. By implementing such technologies, banks can reduce manual errors and promote a more agile risk management process.[5]

Moreover, in recent years, banks have increasingly adopted technology to enhance their Risk and Control Self-Assessment (RCSA) processes. KPMG (2023) explains how integrating Artificial Intelligence (AI) and Natural Language Processing (NLP) can streamline control libraries and automate the identification of redundant controls, thereby improving efficiency.[6]

III. METHODOLOGY

This article is based on a review of available studies, international regulations, and practical examples from Operational Risk Management. No special surveys, interviews, or numerical research were conducted.

The main goal of this research is to understand how Risk and Control Self-Assessment (RCSA) systems, commonly used by large banks in developed countries, can be introduced and adapted to Uzbek banks. To achieve this, the paper examines global standards, such as those from the Basel Committee, and advice from the International Monetary Fund, and compares them with the current situation in Uzbekistan.

We began by reviewing articles, reports, and banking guidelines to understand the common practices for implementing RCSA. It also involved examining how Uzbek banks are currently organized, the difficulties they face, and areas where improvements could be made. The focus was particularly on operational risks and internal control systems.

---

[2] Basel Committee on Banking Supervision. (2006). International Convergence of Capital Measurement and Capital Standards: A Revised Framework - Comprehensive Version. Bank for International Settlements. https://www.bis.org/publ/bcbs128.htm

[3] Cruz, M. G. (2002). Modeling, measuring, and hedging operational risk. Wiley.

[4] Mikes, A. (2009). *Risk management and calculative cultures.* Management Accounting Research, 20(1), 18–40. https://doi.org/10.1016/j.mar.2008.10.005

[5] Yulianto, E. (2019). Implementation of Risk Control Self Assessments Using Rapid Application Development Model in Bank Operational Risk Management Process. Journal of Theoretical and Applied Information Technology, 97(11), 2965–2968. Retrieved from https://www.jatit.org/volumes/Vol97No11/7Vol97No11.pdf

[6] KPMG. (2023). *Risk and Control Self-Assessment: What's Next?* Retrieved from https://assets.kpmg.com/content/dam/kpmg/es/pdf/2024/01/risk-control-self-assessment.pdf

While the paper does not draw on primary data or case studies, it offers a structured foundation that banks can build upon when designing or refining their risk control strategies. It also identifies areas where future research could build upon deeper studies based on real cases.

IV. DISCUSSION

Risk and Control Self-Assessment (RCSA) is a critical tool in the operational risk management framework of banks, offering a structured approach to identify, assess, and mitigate risks within banking processes. The introduction of RCSA in Uzbek banks (hereinafter the banks) presents both challenges and opportunities as these institutions strive to align with international best practices while navigating local operational and regulatory landscapes. The following analysis synthesizes findings from the document and applies them to the specific context of Uzbekistan.

Many banks struggle to identify operational risks accurately and to apply RCSA methods effectively. Many employees lack adequate training on how to identify and classify risks, as highlighted in the document's emphasis on training needs to ensure effective risk management.

Effective RCSA requires robust systems for capturing and analyzing loss data. The banks frequently encounter technological limitations, including outdated hardware and software, which impede automated data collection and processing. Manual processes, which remain prevalent, increase the likelihood of errors and inefficiencies.

The banks operate within a dynamic regulatory environment. Frequent updates in banking laws and compliance requirements necessitate agility in RCSA practices. The document highlights compliance risks as a serious component of operational risk, underscoring the need for banks to adapt their RCSA frameworks to regulatory changes.

The banks can benefit from adopting standardized RCSA templates and methodologies as outlined in the document. These practices include incorporating Basel-compliant frameworks and risk matrices to align local processes with global standards.

The role of training in fostering a culture of risk awareness is very necessary. By conducting regular workshops and interactive RCSA sessions, the banks can empower employees to effectively identify and manage operational risks.

Transitioning to automated RCSA systems offers the banks an opportunity to enhance efficiency and accuracy. Implementing technologies such as data analytics and machine learning can streamline risk identification, assessment, and reporting processes.

Establishing networks for sharing external loss data, as suggested in the document, could significantly benefit the local banks. Platforms like the Operational Risk Exchange (ORX) provide valuable insights into emerging risks and successful mitigation strategies employed by peer institutions.

Collaboration between banks and the regulator in Uzbekistan can create a conducive environment for implementing RCSA. Clear guidelines and incentives for adopting robust risk management practices will encourage compliance and innovation in operational risk management.

□ **Vulnerability Assessment**

Final Risk Rating:	
Risk Assessment Rating	The final rating of the risk arrived at by multiplying the Risk impact score and Vulnerability score
Risk Index	Risk rating expressed in percentage terms depending upon the risk score
Health Index	Risk index deducted from above

Risk Rating

The risk rating process is carried out based on a score derived from assessing both Impact and Vulnerability, taking into account the existing risk and internal control framework within the bank. It is crucial to understand that although the speed at which a risk materializes can influence the bank's perceived vulnerability and aid in formulating an appropriate mitigation strategy, it does not directly affect the risk rating itself.

The main factors considered when determining the risk rating are as follows:

Impact / Severity Rating: The proposed impact scale evaluates both financial and non-financial consequences of operational risk events to ensure a comprehensive risk mitigation approach. The RCSA register automatically assigns ratings for both financial and non-financial impacts. The risk rating is determined by selecting the highest score from the financial and non-financial ratings attributed to each risk.

Frequency / Vulnerability Rating: Vulnerability reflects the likelihood of a risk occurring, given the effectiveness of the existing control environment. RCSA participants assign vulnerability scores to risks based on a subjective evaluation of the current control measures and the probability of the risk occurring.

Risk Rating (Incorporating Impact and Vulnerability): The proposed risk rating matrix uses standardized scores derived from the combined assessment of impact and vulnerability for both Business and Support units. The risk levels are categorized into four distinct scales: critical, high, medium, and low.

Risk Index

Risk index of individual risk:

The individual risk statements in an RCSA register are allotted a risk index which is useful in monitoring the changes in the risk and its control environment. The risk index is derived by dividing the risk score with the product of a maximum score of impact (say10 scales are set) and a maximum score of frequency/ vulnerability (say 4 scales are set) i.e., 40 and multiplying by 100

#	Item	Formula
1	Risk score	$Risk\ score = Risk\ Impact\ Score * Risk\ Vulnerabilty\ score$
2	Risk Index	$Risk\ Index = \frac{Risk\ Score}{40} \times 100$

Risk index of RCSA entity:

The overall rating of the RCSA entity will be done based on the risk assessment of each risk. The final rating must be available for validation with internal audit scores/results.

The methodology that can be adopted for the rating of the RCSA entity is given below

$Risk\ index\ of\ the\ RCSA\ entity = (\sum Impact * vulnerability\ for\ individual\ risk)/\{.of\ risks\ events * Maximum\ score\ fo$

E.g.: if an RCSA entity has 5 risks and each has been rated on impact and vulnerability as given below

Risk Events	Impact	Vulnerability	Severity = Impact * vulnerability
Risk 1	2	4	8
Risk 2	3	2	6
Risk 3	6	1	6
Risk 4	5	2	10
Risk 5	1	3	3
Total Score			**33**

In this case:

$\sum$ ***Impact × vulnerability for individual risk = 33***

No. of risks events = 5

Maximum score for impact = 10

Maximum score for vulnerability = 4

Risk index of the RCSA entity=33/5×10×4=33/200=16.50%

Evaluation of Health Index

The bank assesses Health Index for capturing the Operational Risk profile of the Bank. Like the calculation of Risk Index,

a) Health index of individual risk: 1 - Risk index of individual risk

b) Health index of RCSA entity = 1 - Risk Index of RCSA entity

As per the previous example, Health index of RCSA entity = 1 - 16.5% = 83.5%

V. PROPOSED ROADMAP FOR IMPLEMENTING RCSA IN UZBEK BANKS

Implementing a Risk and Control Self-Assessment (RCSA) framework in a developing financial environment such as Uzbekistan requires a phased and realistic approach. Based on best practices from international institutions and tailored to local conditions, the following roadmap outlines the key steps that banks can follow to gradually establish effective RCSA processes.

Step 1: Define Objectives and Scope

Begin by clearly identifying the objectives of the RCSA. This includes aligning with the bank's overall risk management strategy and determining which departments or processes will be assessed. Initially, it may be practical to focus on high-risk areas or business units that are most exposed to operational risk.

Step 2: Identify and Categorize Key Risks

Departments, in collaboration with the risk management unit, should identify risks specific to their functions. These can include process failures, IT breakdowns, fraud, or human errors. Risks should be classified using a consistent taxonomy to allow comparison and reporting across the bank.

Step 3: Evaluate Existing Controls

For each identified risk, current internal controls should be listed and evaluated. Are the controls working as intended? Are they documented and tested? This step helps to highlight gaps or weaknesses in risk mitigation.

Step 4: Assign Risk Ratings (Impact and Likelihood)

Using a standardized matrix, each risk is rated based on its potential impact (financial and reputational) and its likelihood of occurring. This produces a risk severity score, which helps prioritize areas that need immediate attention.

Step 5: Develop Action Plans for Improvement

For risks rated as high or critical, action plans should be developed. These may involve strengthening controls, revising processes, or providing staff training. Each plan should have a timeline and a responsible person or team.

Action plan – per each priority risk						
#	Action title	Due date	Responsible person	Action details	Impact details	Priority

RCSA findings and conclusions shall be summarized in the management report which includes overview of scope and activities, main risks and controls, priorities and proposals for management actions. Summary report shall be submitted to the senior management with appended RCSA mapping report, profile report, questionnaire, heat map, and action plan, and presented by responsible working team. With management decision business line manager shall start execution of action plan, and risk management shall perform control function over implementation of management decisions.

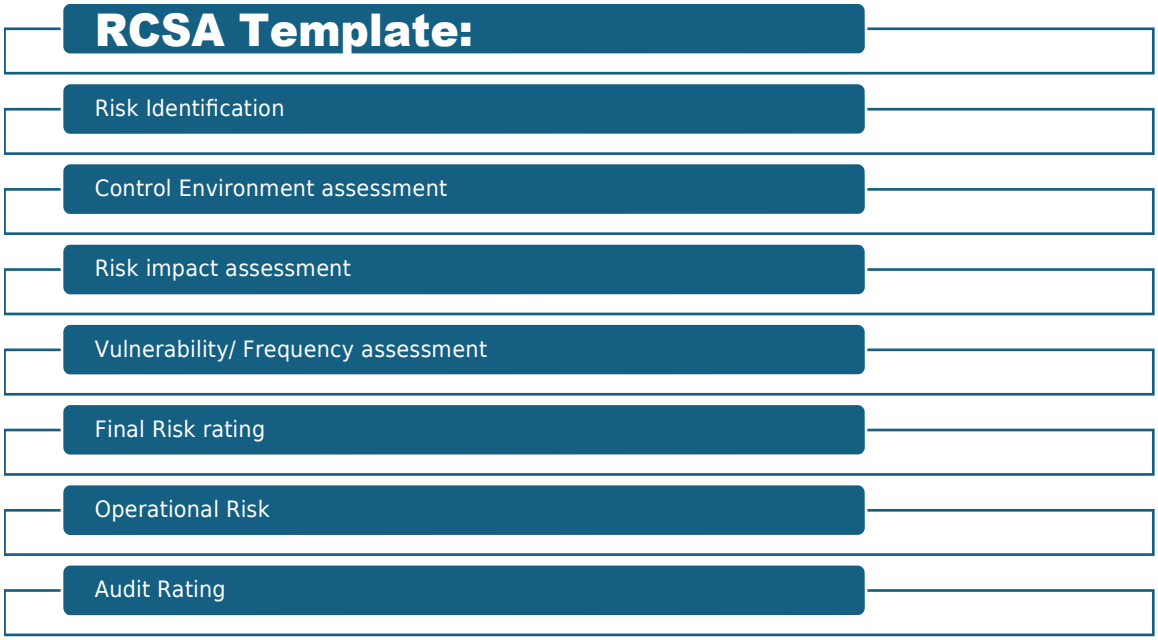
Step 6: Monitor, Document, and Report

An internal database or register should be used to record all risk assessments, controls, and action plans. Regular reporting ensures transparency and helps both management and auditors understand how operational risk is being managed.

Step 7: Review and Update Regularly

RCSA should not be a one-time activity. Banks should set a schedule - annually or semi-annually - to revisit risk assessments, update scores, and reflect any changes in operations, regulation, or technology. Feedback from audits or incidents should be used to improve the next RCSA cycle.

Moreover, the RCSA register is broadly grouped into sections. Each of these sections can further have sub-headers for carrying out the self-assessment as under:



To streamline the RCSA implementation, a standardized template can be adopted. This template helps banks systematically document risks, control measures, assessment outcomes, and improvement actions.

CONCLUSION

This article has highlighted the importance of introducing and strengthening RCSA frameworks in Uzbekistan's banking sector. While many international banks already use RCSA as a routine part of their operational risk strategy, its application in Uzbekistan is still at an early stage. Limited technical infrastructure, lack of standardized methods, and regulatory uncertainty remain key barriers.

However, there is also clear potential. As banking reforms continue and digital solutions are introduced, there is an opportunity to build more effective risk assessment systems. By starting with simple but structured self-assessment tools, and gradually expanding them, banks can improve their understanding and control of internal risks.

The proposed roadmap outlines a practical way forward, from defining risk areas and evaluating controls to monitoring outcomes and updating assessments regularly. Although this study is conceptual in nature, it lays the groundwork for future field-based research and pilot implementations. To strengthen risk management, Uzbek banks should train staff, build a risk-aware culture, and work closely with regulators to embed self-assessment into their practices.

REFERENCES

1. Jacobus, D. (2015). New paradigm of managing risks: Risk and control self-assessment. Agriculture and Agricultural Science Procedia, 3, 32–34. https://doi.org/10.1016/j.aaspro.2015.01.008

2. Basel Committee on Banking Supervision. (2006). International Convergence of Capital Measurement and Capital Standards: A Revised Framework - Comprehensive Version. Bank for International Settlements. https://www.bis.org/publ/bcbs128.htm
3. Cruz, M. G. (2002). Modeling, measuring, and hedging operational risk. Wiley.
4. Mikes, A. (2009). Risk management and calculative cultures. Management Accounting Research, 20(1), 18–40. https://doi.org/10.1016/j.mar.2008.10.005
5. Yulianto, E. (2019). Implementation of Risk Control Self Assessments Using Rapid Application Development Model in Bank Operational Risk Management Process. Journal of Theoretical and Applied Information Technology, 97(11), 2965–2968. Retrieved from https://www.jatit.org/volumes/Vol97No11/7Vol97No11.pdf
6. KPMG. (2023). Risk and Control Self-Assessment: What's Next? Retrieved from https://assets.kpmg.com/content/dam/kpmg/es/pdf/2024/01/risk-control-self-assessment.pdf