



Article

Improving Risk-Based Internal Control Mechanisms to Ensure Financial Security in Insurance Organizations

Islamova Nargiza Mirzaxidovna*

1. Department of Economic Theory independent researcher Tashkent State University of Economics

* Correspondence: nargiza.islomova78@gmail.com

Abstract: The article examines the theoretical, methodological, and practical aspects of improving risk-based internal control mechanisms to ensure financial security in insurance organizations. It substantiates the need to transform the internal control system from retrospective inspection into a preventive management mechanism that identifies threats to financial security in advance, given the specific features of insurance activities related to contingent liabilities, insurance reserves, reinsurance, investment processes, and the acceptance of various risks. The study develops a methodological approach based on a comprehensive assessment of the risk management system, the state of internal control, financial security outcomes, and digital control infrastructure. A mechanism is proposed for determining control priorities based on the impact of risks on capital adequacy, solvency, liquidity, adequacy of insurance reserves, and profitability; identifying financial security zones under stress scenarios; and early detection of adverse trends through key risk indicators (KRIs). As a result, a risk-based internal control mechanism is substantiated that enables the integration of assessment, prioritization, stress testing, digital monitoring, and control response into a single management cycle.

Keywords: financial security, insurance organization, risk, internal control, risk management, solvency, stress testing, KRI, early warning, digital monitoring

Citation: Mirzaxidovna, I. N. Improving Risk-Based Internal Control Mechanisms to Ensure Financial Security in Insurance Organizations. Central Asian Journal of Innovations on Tourism Management and Finance 2026, 7(4), 404-410.

Received: 5th Aug 2026
Revised: 24th Aug 2026
Accepted: 4th Sep 2026
Published: 19th Sep 2026



Copyright: © 2026 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>)

1. Introduction

Insurance organizations perform an important institutional function in the economy by redistributing risks, protecting the property interests of business entities and the population, and covering unexpected financial losses. However, an insurance organization that accepts risks from other economic entities is itself exposed to a high level of financial and non-financial risks. Deterioration in underwriting results, an unexpected increase in insurance claims, a decline in the value of investment assets, liquidity shortages, problems associated with reinsurers, operational disruptions, and non-compliance with regulatory requirements may directly affect the financial condition of an insurer.

Under these conditions, it is insufficient to interpret financial security solely through the amount of capital or the current solvency ratio. The financial security of an insurance organization is a comprehensive condition reflecting the adequacy of capital and reserves, the ability to fulfill obligations fully and on time, the maintenance of sufficient liquidity, the achievement of profitability, and the ability to limit the adverse impact of internal and external risks to an acceptable level.

Digitalization makes this issue even more complex. The expansion of electronic insurance policies, remote services, electronic claims, automated underwriting, digital payments, and data processing systems creates new information opportunities for insurance organizations while also increasing operational, technological, and cyber risks. As of July 2026, the EIOPA Insurance Risk Dashboard assessed digitalization and cyber risk as high-level risks for the European insurance sector. The Dashboard tracks not only the current state of risks, but also their three-month trend and outlook over the next 12 months. [1]

Modern concepts of risk management are also shifting control from recording adverse events after they occur toward identifying risks in advance. ISO 31000:2018 defines risk management as an integrated process encompassing risk identification, analysis, assessment, treatment, monitoring, and communication. [2] The 2018 version was reviewed in 2023 and confirmed as the current version. The COSO ERM model emphasizes the need to manage risk together with strategy and organizational performance. [3]

In the insurance sector, this approach is particularly evident in the Solvency II framework. In accordance with Article 45 of the Directive [4], each insurance and reinsurance undertaking must assess its risks and solvency within the ORSA process, taking into account its individual risk profile, approved risk limits, business strategy, capital requirements, and continuous compliance with technical provisions.

Uzbekistan has also established a legal framework governing internal control and risk management systems in insurance organizations. In the current version of the Law of the Republic of Uzbekistan No. ZRU-730 "On Insurance Activity," [5] Article 48 establishes requirements for insurers' compliance with prudential standards, while Article 51 establishes requirements concerning the internal control and risk management system. The current version of the Law also incorporates amendments dated July 25, 2026. However, the mere existence of regulatory requirements does not by itself ensure the effectiveness of internal control in practice. The control system should not only identify risks, but also assess their impact on financial security, direct control resources toward material risks, model the potential effects of shocks in advance, and respond promptly to adverse changes in risk indicators. Accordingly, the objective of the study is to improve risk-based internal control in insurance organizations by integrating the assessment, determination of control priorities, stress testing, and digital early-warning elements into a single interconnected mechanism for ensuring financial security.

The theoretical foundation of risk management dates to F. Knight, who distinguished risk from uncertainty by relating risk to situations in which probable outcomes can be assessed [6], and to H. Markowitz, who linked risk to expected return through portfolio theory, laying the basis for quantitative risk assessment in financial decision-making [7]. Contemporary frameworks treat risk not as a separate element of organizational activity but as a management category linked to strategy, resources, and performance: ISO 31000 integrates risk management into an organization's strategy, planning, decision-making, and reporting [2], and COSO ERM links risk to strategy-setting and performance management [3]. At group and solvency level, the international principle on enterprise risk management for solvency purposes [8] and the own-risk-and-solvency-assessment framework [9] both require insurers to assess how their own risk profile differs from the assumptions embedded in a regulatory model, rather than relying on current regulatory indicators alone — a demonstration of the need to consider an organization's individual risk characteristics.

International practice also demonstrates the value of a forward-looking, quantitative approach to assessing financial security. EIOPA's 2024 insurance stress test covered 48 insurance undertakings and groups representing 75% of European market assets by the capital component; before the stress, participants' aggregate solvency ratio

stood at 221.8%, and the adverse scenario modeled a reduction of more than EUR 270 billion in capital, with capital and liquidity assessed separately [10]. In 2026 EIOPA published guidance on stress scenarios and indicators for pre-emptive recovery planning, covering system-wide and insurer-specific shocks and their impact on solvency, liquidity, and profitability [11], and specifying indicators for capital and liquidity position, asset quality, profitability, market conditions, and operational events [12]. At the level of an individual organization, S.P. Nelga studied risk-based internal control in insurance and substantiated the integration of risk management, compliance, actuarial, and internal audit functions with a dynamic risk register, key risk indicators, and stress testing linked to strategic objectives [13]. A synthesis of this literature shows substantial methodological development in risk management, internal control, stress testing, and KRI monitoring, but in most cases the assessment of risk, its impact on financial security, control prioritization, resilience to stress, and the link between an early-warning signal and a specific management action are not integrated into a single continuous mechanism — the gap this study addresses.

2. Materials and Methods

The study used systematic and comparative analysis, regulatory and legal analysis, logical generalization, the coefficient method, scoring, scenario analysis, stress testing, and matrix approaches. The key methodological feature is that the study places not the risk itself, but the trajectory of its impact on financial security at the center of the analysis. Capital adequacy, solvency, liquidity, adequacy of insurance reserves, and profitability were adopted as the main outcome parameters characterizing financial security. The material risks of an insurance organization were grouped into underwriting, investment, liquidity, operational, and compliance risks. [14]

The research logic moves from assessing the state of internal control to prioritizing risks, then to assessing future vulnerabilities through stress testing, and finally to early detection of increasing risk based on KRIs. Each subsequent stage uses the results of the previous stage, thereby forming a closed management cycle.

When assessing the effectiveness of internal control, the risk management system, the organizational and functional state of internal control, financial security outcomes, and digital control infrastructure are considered jointly. It is proposed to assign methodological weights of 35%, 30%, 25%, and 10%, respectively. These weights are not regulatory standards, but an author-developed operational scale that should subsequently be calibrated based on expert assessment and empirical validation.

3. Results and Discussion

The research results indicate a direct relationship between the assessment of internal control effectiveness and the achievement of financial security. The formal existence of control procedures does not mean that an organization is financially secure. For example, even when internal audit and compliance functions have been established, an increase in loss ratios, a reduction in the liquidity buffer, or a weakening of reserve adequacy may indicate that the control system is not identifying risks affecting financial security sufficiently early.

Therefore, the assessment of internal control effectiveness should, at the next stage, be linked to the issue of which risks should receive control resources. In practice, when many risks exist, applying the same control intensity to all of them is not economically efficient. Control priority should be determined not only by the probability of risk occurrence and the potential loss, but also by its impact on financial security. This approach makes it possible to determine control intensity based not on the name or classification of a risk, but on its actual impact on the financial security of a particular

insurance organization. For example, an increase in underwriting risk may be transmitted through insurance claims and reserves to profitability and capital, ultimately affecting solvency. Investment risk weakens capital and profitability through a decline in asset values and investment income. Liquidity risk, due to cash-flow mismatches, may create a need to realize assets under unfavorable conditions and subsequently affect capital.

Based on this, controls can be conditionally divided into standard, targeted, enhanced, and urgent regimes. These levels should also be regarded not as rigid regulatory thresholds, but as operational instruments for differentiating control resources. The most important feature of the mechanism is the introduction of the “impact on financial security” stage between risk assessment and the selection of a control measure.

However, determining control priorities based on existing risks does not fully assess preparedness for future adverse shocks. Therefore, after control priorities have been established, it is advisable to use stress testing to assess how the financial security of an insurance organization would change under potential adverse scenarios.

EIOPA’s 2024 stress test demonstrates the practical significance of this approach. The stress test assessed capital and liquidity separately and modeled a reduction of more than EUR 270 billion in the capital of participating insurers under a severe but plausible scenario. [10] At the same time, the application of management actions improved post-stress outcomes. At the level of an individual insurance organization, stress testing may include underwriting shocks, a reduction in premium income, a decline in the value of investment assets, liquidity and reinsurance-related shocks, operational and digital disruptions, and combined scenarios. The 2026 EIOPA guidelines also envisage consideration of system-wide, insurer-specific, and combined scenarios. [12]

It is not advisable to set stress parameters at the same levels for all insurance organizations. For example, automatically increasing claims by 20% or reducing the value of investment assets by 15% does not have the same economic meaning for all portfolios. Therefore, stress parameters should be calibrated on the basis of the organization’s historical data, risk profile, actuarial assessments, applicable regulatory thresholds, and relevant external scenarios. After the stress, capital adequacy, solvency, liquidity, reserve adequacy, and profitability should be recalculated. It is not sufficient to compare them only with their pre-stress values; post-stress indicators should be assessed against target, early-warning, and critical thresholds.

On this basis, four financial security states are distinguished: stable, warning, risky, and critical. In the stable zone, an adequate financial buffer remains even after stress. In the warning zone, regulatory safety has not yet been breached, but the protection buffer is shrinking. In the risky zone, the indicator approaches the critical threshold and preventive action is required. In the critical zone, a regulatory or internal minimum safety threshold is breached. Here, it is advisable to apply **the weakest-link principle** rather than calculate the overall state of financial security as an average score. High profitability cannot compensate for critical liquidity shortages or solvency problems. Therefore, if one of the five parameters enters a critical state, that parameter should become the first object of preventive control.

Nelga linked stress testing to preventive internal control by determining the condition of technical reserves and assessing their impact on solvency. [13] In her study, stress-test results are transformed into management measures such as reviewing capital policy, optimizing reinsurance protection, and adjusting underwriting and tariff policies. In developing this approach from the perspective of financial security, it is advisable not to limit stress-test results to technical reserves or solvency, but to assess the five key parameters jointly and identify the weakest parameter.

While stress testing models a potential future shock, dynamic monitoring is required in day-to-day operations to detect an emerging gradual increase in risk at an early stage. At this point, key risk indicators (KRIs) become the next element of risk-based internal control. A KRI and a financial security indicator are not the same category. Capital adequacy, solvency, and profitability show the financial outcome of risk. An increase in the frequency of insurance events, growth in average claims, delays in reinsurance recoveries, or a successive reduction in the liquidity asset buffer are signals that emerge before the final outcome materializes. Therefore, a two-level information structure is advisable in the digital monitoring system: at the first level, KRIs indicating an increase in risk are monitored; at the second level, financial security parameters reflecting the ultimate effect of risk are monitored. For underwriting risks, KRIs may include the frequency of insurance events, average insurance claims, and loss-ratio dynamics; for investment risk, asset concentration and investment profitability; for liquidity risk, the liquidity asset buffer and net cash flow; for reinsurance risk, delays in the receipt of funds; for operational risk, material incidents and the duration of disruptions in critical information systems; and for compliance risk, unresolved material violations.

The EIOPA Risk Dashboard also assesses not only the static level of risk but its dynamics and future outlook. This approach indicates that, at the organizational level, it is necessary to monitor not only whether a KRI exceeds its threshold, but also whether it demonstrates a persistent adverse trend before reaching the threshold.

Accordingly, it is advisable to use two types of triggers for each KRI: **a threshold trigger**, when the indicator reaches or exceeds the established control threshold; and **a dynamic trigger**, when the indicator moves in an adverse direction over several observation periods. A digital passport may be created for each KRI. It may specify the indicator's economic meaning, calculation method, information source, update frequency, normal range, warning and critical thresholds, risk direction, related financial security parameter, and responsible function. This turns the KRI from a simple statistical indicator into a digital object that generates a control decision. A digital signal should not be limited to appearing on a dashboard. It should be routed to the relevant control function and its execution should be monitored. Under normal conditions, scheduled monitoring continues. When an early-warning signal appears, the causes of deviation are analyzed. Under an enhanced signal, limits, control conditions, or operations are reviewed. Under a critical signal, urgent management intervention and escalation to a higher management level are carried out.

Proper allocation of responsibilities among functions is of fundamental importance. Business units, as direct risk owners, implement control measures. Risk management aggregates signals and assesses their significance. The actuarial function analyzes risks related to underwriting, tariffs, and reserves. The compliance function monitors risks related to regulatory requirements. Internal audit, in turn, does not manage risks directly, but independently assesses the functioning of the system and the adequacy of control measures. [15] Nelga's study also identifies the integration of risk management, compliance, actuarial, and internal audit functions within a unified corporate governance system as an important condition. [13]

An important feature of the proposed approach is that these processes are not separated from one another. Assessment of internal control effectiveness identifies which system elements are weak; assessment of the impact of risk on financial security determines the priority direction for control resources; stress testing shows how the weakness may intensify under an adverse scenario; and KRI monitoring detects early signs in current data that the organization is approaching an adverse scenario.

Summarizing the research findings, four functions were identified in the improved model of risk-based internal control as being closely interconnected: assessment of

current internal control effectiveness, prioritization of risks with a high impact on financial security, modeling financial resilience to adverse scenarios, and early detection of increasing risk based on digital indicators. Integrating these functions into a single mechanism transforms internal control from a post-event inspection process into a preventive management system focused on identifying future financial vulnerabilities in advance and limiting them.

At the same time, the proposed methodological weights, priority ranges, internal boundaries of security zones, and KRI triggers are currently author-defined operational parameters. They cannot be treated as regulatory standards or empirically universal thresholds. In further studies, these parameters should be calibrated using real panel data from insurance organizations in Uzbekistan, actuarial statistics, and expert assessments.

4. Conclusion

The research demonstrates that maintaining the internal control system within a retrospective inspection model is insufficient to ensure financial security in insurance organizations. The nature of the insurance business, based on contingent liabilities and numerous interconnected risks, requires internal control to be organized as a preventive mechanism that identifies risks in advance, assesses their impact on financial security, and establishes control measures proportionate to risk significance. The study substantiates the need to assess internal control effectiveness jointly with risk management, control functions, financial security outcomes, and digital infrastructure. In this context, control priority should be determined not only by the probability of a risk occurring and the potential loss, but also by its impact on capital adequacy, solvency, liquidity, reserve adequacy, and profitability. When assessing the future condition of financial security, it is substantiated that individual and combined stress scenarios should be formed in accordance with the organization's risk profile and that post-stress financial parameters should be assessed across stable, warning, risky, and critical zones. Prioritizing the weakest parameter prevents serious weaknesses in financial security from being concealed by an average overall result.

At the same time, digital monitoring of key risk indicators, automatic detection of their threshold and dynamic changes, routing of signals to the responsible function according to their potential impact on financial security, and subsequent monitoring of the implementation of adopted measures increase the responsiveness of internal control. The main economic effect of digitalization is manifested precisely in reducing the time between the first adverse sign of risk and the control response.

As a result, the risk-based internal control mechanism in insurance organizations takes the form of a continuous management cycle consisting of **assessment** → **identification of financial impact** → **prioritization** → **stress testing** → **early warning** → **preventive action** → **implementation monitoring** → **reassessment**. This approach provides a methodological basis for directing internal control resources toward areas of greatest importance for financial security, maintaining adequate capital and reserves, strengthening liquidity and solvency, and ensuring the long-term financial stability of insurance organizations.

REFERENCES

- [1] European Insurance and Occupational Pensions Authority (EIOPA), "Insurance Risk Dashboard," EIOPA, Frankfurt, Germany, Jul. 2026.
- [2] International Organization for Standardization, *ISO 31000:2018 — Risk Management — Guidelines*, Geneva, Switzerland, 2018.

- [3] Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management – Integrating with Strategy and Performance*. Durham, NC, USA: COSO, 2017.
- [4] European Parliament and Council of the European Union, *Directive 2009/138/EC on the Taking-up and Pursuit of the Business of Insurance and Reinsurance (Solvency II)*, Nov. 25, 2009.
- [5] Law of the Republic of Uzbekistan No. ZRU-730, “On Insurance Activity,” Nov. 23, 2021.
- [6] F. H. Knight, *Risk, Uncertainty and Profit*. Boston, MA, USA: Houghton Mifflin, 1921.
- [7] H. Markowitz, “Portfolio selection,” *The Journal of Finance*, vol. 7, no. 1, pp. 77–91, Mar. 1952.
- [8] International Association of Insurance Supervisors (IAIS), *Insurance Core Principle 16: Enterprise Risk Management for Solvency Purposes*. Basel, Switzerland: IAIS, 2019.
- [9] National Association of Insurance Commissioners (NAIC), *Own Risk and Solvency Assessment (ORSA) Guidance Manual*. Kansas City, MO, USA: NAIC, Dec. 2022.
- [10] European Insurance and Occupational Pensions Authority (EIOPA), “Insurance Stress Test 2024,” EIOPA, Frankfurt, Germany, 2024.
- [11] European Insurance and Occupational Pensions Authority (EIOPA), “Final Report on Guidelines on Indicators in Pre-emptive Recovery Planning – IRRD,” Jul. 8, 2026.
- [12] European Insurance and Occupational Pensions Authority (EIOPA), “Final Report on Guidelines on a Range of Macroeconomic and Financial Scenarios – IRRD,” Jul. 8, 2026.
- [13] S. P. Nelga, “Systema vnutrishnoho kontroliu v upravlinni diialnistiu strakhovoi orhanizatsii” [Internal control system in managing the activity of an insurance organization], Ph.D. dissertation, Specialty 072, Finance, Banking and Insurance, Kyiv, Ukraine, 2026.
- [14] Basel Committee on Banking Supervision (BCBS), *Revisions to the Principles for the Sound Management of Operational Risk*. Basel, Switzerland: Bank for International Settlements, Mar. 2021.
- [15] Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Internal Control – Integrated Framework*. Durham, NC, USA: COSO, 2013.