BANKA QENDRORE E REPUBLIKËS SË KOSOVËS
CENTRALNA BANKA REPUBLIKE KOSOVO
CENTRAL BANK OF THE REPUBLIC OF KOSOVO

Based on Article 35, paragraph 1, subparagraph 1.1, of Law No. 03/L-209 on the Central Bank of the Republic of Kosovo (Official Gazette of the Republic of Kosovo, no. 77 / 16 August 2010), as amended and supplemented by Law No. 05/L-150 on Amending and Supplementing Law No. 03/L-209 on the Central Bank of the Republic of Kosovo (Official Gazette of the Republic of Kosovo, no. 3/17 January 2017), and Article 4, paragraph 3, and pursuant to Article 59 of Law 05/L-045 on Insurance (Official Gazette of the Republic of Kosovo, No. 38 / 24 December 2015), the Board of the Central Bank, in its meeting held on 30th of January 2025, approved the following:

REGULATION ON OPERATIONAL RISK MANAGEMENT OF INSURERS

Article 1
Purpose and scope

1. The purpose of this Regulation is to determine the basic principles for identification, measurement, control and management of insurers' operational risk, its structure and components, as well as the supervisory requirements by the Central Bank of the Republic of Kosovo (CBK).
2. This Regulation applies to insurers and branches of foreign insurers (hereinafter: insurers), licensed by the CBK to carry out insurance activities in the Republic of Kosovo.

Article 2
Definitions

1. All terms used in this Regulation have the same meaning as defined in Article 3 of Law 05/L-045 on Insurance (hereinafter: the Insurance Law) and/or with the following definitions for the purpose of this Regulation:
   1.1. **Operational Risk** – means the risk of loss arising from failed or inadequate internal processes, personnel or system failure, as well as the risks of loss arising from external events;
   1.2. **Function** – means the organizational units within the insurers' organizational structure.

Article 3
Operational risk management system

1. Insurers must establish an operational risk management system, adequate to the nature, scale and complexity of their business, in order to identify, assess, monitor and control/mitigate operational risk.
2. The operational risk management system must contain at least the following elements:
   2.1. Responsibility and control by the Board of Directors;

2.2. Responsibility and control by the Risk Management Committee;

2.3. The role and responsibilities of Senior Management;

2.4. Appropriate organizational structure that clearly defines the authority and responsibilities of everyone within the insurers' structure; and

2.5. Policies, procedures and methods for managing operational risk.

Article 4
Supervision and control

1. The Board of Directors and Senior Managers of insurers should treat operational risk as a major risk and they should accept ultimate responsibility for monitoring the effectiveness of operational risk management within insurers.

2. The Board of Directors of insurers is responsible for the establishment, approval and annual review of operational risk policies. The Board of Directors should supervise Senior Management to ensure the adequate implementation of policies, processes and systems, at all decision-making levels. To this end, the Board of Directors is responsible:

   2.1. for establishing an appropriate organizational structure for operational risk management;

   2.2. for development of general strategies and policies for operational risk management, in accordance with the insurer's strategic goals;

   2.3. for the review and approval of the Senior Management functions, regarding responsibilities and reporting regarding operational risk management, in order to ensure the efficiency of decision-making at the insurer;

   2.4. for the regular review of operational risk reports submitted by senior management, as well as the continuous monitoring and evaluation of the effectiveness of operational risk management;

   2.5. to ensure that senior management is taking necessary measures to identify, assess and mitigate operational risk;

   2.6. to ensure that the insurer's operational risk management system is effectively audited by the insurer's internal audit; and

   2.7. to provide an appropriate reward and punishment system for Senior Management and employees of the insurer, in order to promote the development of an adequate operational risk management system.

3. The insurers' senior management is responsible for implementation of operational risk management strategies, general policies and functioning of systems approved by the Board of Directors of the insurers. To this end, the senior management is responsible:

   3.1. for regular reporting to the Board of Directors regarding ongoing operational risk management;

3.2. for the development and regular review of policies and procedures for operational risk management, in accordance with the overall strategies and policies developed by the Board, overseeing their implementation, and submitting reports on operational risk management on a regular basis to the Board of Directors;

3.3. to sufficiently understand the insurer's operational risk management;

3.4. to clearly define the responsibilities of each function in operational risk management, including definition of reporting lines, the frequency and content of reports, encourage each unit (function) of the insurer to define its own responsibilities, in order to ensure sound performance of the operational risk management system.

3.5. to conduct controls and reviews in the operational risk management system in order to effectively respond to operational risk events resulting from internal changes in: procedures, products, business activities, information technology systems, personnel, external events or other factors.

4. The risk management function within insurers is responsible for establishing and implementing an operational risk management system. The responsibilities of this function regarding operational risk management include:

4.1. drafting specific operational risk management policies, procedures and processes and submitting them to Senior Management and the Board of Directors for review and approval;

4.2. assists other functions of the insurer in identifying, assessing, monitoring and reducing operational risk;

4.3. establishing methods for the purpose of identifying, assessing, reducing (including internal controls) and monitoring operational risk, formulating the reporting process within the insurer regarding operational risk, its organization and implementation;

4.4. establishing basic criteria on operational risk within the insurer, and guiding and coordinating operational risk management;

4.5. organizing training for each function of the insurer regarding operational risk management, as well as helping them improve their capacities for operational risk management and fulfilling their duties;

4.6. controlling and analysing operational risk management practices in other functions of the insurer;

4.7. sending reports on operational risk to Senior Management and the Board of Directors;

4.8. ensuring that systems for operational risk management measurements are monitored.

5. The relevant functions of the insurer should be directly responsible, within their responsibilities, for the management of operational risk. The main responsibilities under this paragraph include:

5.1. appointing designated staff responsible for operational risk management, including overseeing specific policies, procedures and processes for operational risk management;

5.2. following the assessment methods for operational risk management in order to identify and assess operational risk, and to have an effective ongoing procedure for monitoring, controlling, mitigating, and reporting operational risks, and then organizing their implementation;

5.3. to consider the requirements of operational risk management and internal controls, particularly when developing specific business processes for the relevant organizational unit. To ensure that operational risk management personnel within the function (organizational unit) participate in the review of significant procedures, controls, and policies to harmonize them with the insurer's overall operational risk management policies; and

5.4. to monitor the most important risk indicators and regularly report on the status of operational risk management of their organizational function to the other organizational function that plays a leading role in the operational risk management of the insurer as a whole.

6. In addition to adequately managing its own operational risk, the insurer's legal, compliance unit, information technology unit, and human resources units must assist other units in managing operational risk within their capabilities and respective responsibilities.

7. Although the insurer's internal audit unit is not directly responsible for or involved in operational risk management, it should monitor and evaluate the system's operation on a regular basis, as well as oversee the implementation of operational risk management policies. It should conduct an independent assessment of the insurer's operational risk management policies, procedures, and processes and report the findings to the Board of Directors.

8. The insurer should select the most appropriate strategy for managing operational risk. This approach should include: assessing operational risk and internal controls, reporting events that have resulted in losses and gathering data, monitoring key risk indicators, assessing the risk of new products and business practices, testing and auditing internal controls, and reporting operational risk.

9. The insurer should establish a reliable process for monitoring and reporting on operational risk and material losses on a regular basis. For risks with the potential for increased losses, an operational risk early warning system should be established to control risk reduction and reduce the number of events that could result in losses.

10. To effectively identify, control, and report operational risks, the insurer must establish and constantly improve an operational risk management information system. At the very least, this system must record and keep track of the dates of operational risk events and losses. The system must be based on a self-assessment of operational risk and control measures, monitoring of key risk indicators, and the creation of relevant information for an operational risk report.

Article 5
Types of events that can result in losses

1. The types of operational risk events that can result in losses are:

1.1. Internal fraud – includes losses caused by intentional acts of fraud, misappropriation of assets or violation of regulations, laws or policies of the insurer, which involves at least one internal party (employees, senior managers of the insurer) such as: intentional and false reporting of the insurer's financial position, performance of unauthorized transactions of the insurer, unauthorized internal transactions in the account of employees or members of the insurer's

governing bodies, intentional destruction of the insurer's assets, theft, robbery, extortion, embezzlement of the insurer's assets, forgery, intentional tax evasion, unjust enrichment of employees and members of the insurer's governing bodies.

1.2. External fraud – includes losses caused by intentional acts of fraud, embezzlement or evasion of the law by third parties outside the insurer, such as: theft and robbery, forgery, intentional damage to computer systems, information theft.

1.3. Employment practices and occupational safety – includes losses caused by actions inconsistent with labor laws, occupational health and safety, or other agreements from the employment relationship, as well as claims/demands for personal injury payments and/or workplace discrimination.

1.4. Customers, products and business practices – includes losses caused by failure to fulfil obligations to the customer, losses arising from the nature or design of the product, such as: breaches of fiduciary duties, misuse of confidential customer information, money laundering, product defects, exceeding access rights to the insurer's computer program, human or automated calculation errors.

1.5. Physical damage to property - Includes losses caused by physical damage to property resulting from natural disasters or other events such as vandalism, terrorism, etc.

1.6. Business interruption and system failures - includes losses caused by business disruption or system failures such as: complete or partial failure of equipment or programs, telecommunications problems, service interruptions, equipment obsolescence, etc.

1.7. Execution, distribution and management of processes - includes risk events related to transaction processing or the management of processes and relationships with third parties, such as: communication deficiencies, data collection errors (for example, incorrect data), failure to meet deadlines, system malfunctions, accounting errors, reporting errors, deficiencies in legal documentation, etc.

Article 6
Risks from processes, systems, personnel and external risks

1. Process risk – includes the possibility of losses due to careless processing by personnel, errors, or unauthorized activity. Insurers should work on increasing the level of development of process risk management within it, ensuring that each function follows regular self-research of process risks, minimizing losses in the event of errors during processing, carelessness, or unauthorized activities of personnel by drafting contingency plans.

2. Systems risk – includes the possibility of loss due to computer system failures, misuse, or unauthorized use. Stable computer systems should be an essential factor in the effective implementation of the operational risk management strategy in light of technological advances and developments. For this paragraph, the insurer should:

2.1. have contingency plans in place to reduce losses in the event of system failure (collapse);

2.2. take various measures to prevent system failure, including the duplication of various systems and infrastructures, constant maintenance of systems to ensure continuity of operations, and the creation of a disaster prevention system.;

2.3. maintain the confidentiality of customer information and prevent data leaks. Sensitive information must be encrypted, unauthorized access from outside must be blocked, and all necessary measures must be taken to secure the data.;

2.4. have a training plan and hold training sessions to ensure that personnel are fully prepared for emergency situations. To ensure safety, measures should be reviewed based on the most recent technological developments.

3. Personnel risk – is an integral component of the operational risk assessment. The insurer should assess the extent to which its employees may impact the risk of carrying out business operations under the current structure. This includes the insurer's size, the complexity and variety of its products, and the sophistication of the systems it employs to carry out its operations. For the purpose of this paragraph, the insurer should:

   3.1. determine the organizational structure in such a way that the reporting lines of organizational units are clear;

   3.2. Determine the responsibilities of organizational units and job descriptions. The responsibilities of the heads of functions (organizational units), as well as the qualifications of personnel, should be clearly defined;

   3.3. Consider inherent (natural) risk, which includes: the rate of staff turnover, the rate of job openings (competitions), organizational changes, and the size of the staff in relation to the volume of activities;

   3.4. Consider the residual risk, which includes: abuse of the system, abuse of confidential information, vacancies and the length of time they remain until they are filled, the level of internal fraud, the costs of false claims, etc.;

   3.5. Consider recruiting new staff with the required competencies, being attentive to training, equipping staff with the necessary knowledge to perform tasks effectively, and creating a staff mobility program, with the goal of increasing motivation at work.

4. External risks – include risks arising from internal/external crimes (fraud, theft, robbery), natural disasters, terrorism/war, and political risk. This type of risk also includes legal risk, which is the risk of loss because a contract cannot be legally enforced, and also includes the risk arising from insufficient documentation and insufficient authority over the other party.

Article 7
Operational risk reporting

1. The insurer must report to the CBK on an annual basis on policies and procedures for operational risk management and reports related to operational risk.

2. The insurer must immediately report to the CBK about operational risk events if any of the following events occur:

   2.1. financial crimes, in which sums of money are stolen from the insurer’s account, in the event of theft of other assets of the insurer, financial fraud or other cases that represent losses for the insurer;

   2.2. events that result in serious damage or loss of the insurer's important data, books, interruption of operations for 1 (one) day or more, in one or more branches of the insurer.

2.3. the insurer's proprietary information has been stolen, sold, or published without its permission, or any information has been lost that may harm the insurer's financial stability.;

2.4. frequent violation of applicable rules by senior management;

2.5. accidents or natural disasters, caused by any force majeure, which results in economic loss for the insurer. This subparagraph excludes reports on damages arising from insurance activities (damages incurred, damages reported, damages paid);

2.6. other operational risks, which could result in a loss of more than EUR 10 thousand; and

2.7. other material events, as may be required by the CBK on a case-by-case basis.

3. The CBK shall regularly review and assess the insurer’s operational risk management policies, procedures and practices. The review and assessment under this paragraph shall include:

3.1. the effectiveness of operational risk management procedures;

3.2. the insurer's ability to monitor and report operational risk, including key risk indicators and operational risk loss data;

3.3. the insurer’s ability to deal with operational risk events in a timely and effective manner;

3.4. whether the insurer's internal procedures and controls have been reviewed and audited within the operational risk management processes;

3.5. the quality and comprehensiveness of disaster recovery plans and business continuity plans, including analysis of different scenarios;

3.6. other aspects of operational risk management.

Article 8
Enforcement, remedial measures and civil penalties

Any violation of the provisions of this Regulation is subject to corrective and punitive measures, as defined in the Law on the Central Bank of the Republic of Kosovo and the Law on Insurance.

Article 9
Transitional provisions

Full compliance by insurers with all the requirements of this Regulation must be achieved by April 30, 2025.

Article 10
Entry into force

This regulation enters into force 15 days after approval.

Dr.sc. Bashkim Nurboja
Chairman of the Board of the Central Bank of the Republic of Kosovo