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

Pursuant to Article 35, paragraph 1.1 of the Law No. 03/L-209 on Central Bank of the Republic of Kosovo (Official Gazette of the Republic of Kosovo, No.77 / 16 August 2010), Article 20 paragraph 1.3 and Article 85 of the Law No. 04/L-093 on Banks, Microfinance Institutions and Non-Bank Financial Institutions (Official Gazette of the Republic of Kosovo, No.11 / 11 May 2012), the Board of the Central Bank of Republic of Kosovo at the meeting held on November 29, 2012, approved the following:

REGULATION 9
ON OPERATIONAL RISK MANAGEMENT

Article 1
Purpose and Scope

1. Purpose of this Regulation is to provide the basic principles of identification, measurement, control and management of operational risk within banks, its structure and its components, as well as its supervision requirements by the Central Bank of the Republic of Kosovo (CBK).

2. This Regulation applies to all banks and branches of foreign banks (hereinafter: *banks*), licensed by the CBK to operate in the Republic of Kosovo.

Article 2
Definitions

1. All definitions used in this Regulation are as provided for with Article 3 of the Law No.07/L-093 on Banks, Micro-finance Institutions and Non-Bank Financial Institutions (hereinafter: *the Law on Banks*), and/or as further defined herein for the purpose of implementing this Regulation:

a) *Operational Risk* is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from certain external events. This definition includes legal risk, but excludes strategic and reputational risk. Legal risk includes, but is not limited to, exposure to fines, penalties, or punitive damages resulting from supervisory actions, as well as any other kind of settlement with individual parties. Even though reputational and strategic risks are not easily identifiable, banks are expected to develop techniques for managing all aspects of risk.

b) *Material operational risk event* is defined as loss with material value above or equal to 20% (twenty percent) of Tier 1 capital.

Article 3
Requirements

1. Banks, in accordance with this regulation, should establish a system for managing operational risk, appropriate to the nature, extent and complexity of their business in order to effectively identify, assess, monitor and control / mitigate operational risk. This system can be in any form, but must at least contain the following basic elements:

a) Responsibilities and oversight control by the Board of Directors;

b) Responsibilities and oversight control by the Operational Risk Committee;

c) Roles and responsibilities of senior management;

d) Adequate organizational chart that identifies authorities and responsibilities;

e) Policies, procedures and methods for managing operational risk; and

f) Capital provisioning requirements by the bank for operational risk.

Article 4
Supervision and Control

1. The Board of Directors and senior managers of a bank must treat operational risk as a major risk and they must accept the final responsibility of monitoring the efficiency of operational risk management within the bank.

Article 5
Responsibilities of Board of Directors and Operational Risk Committee on Managing Operational Risk

1. The Board of Directors in a bank is responsible for the establishment, approval and annual review of operational risk policies. The Board of Directors should supervise senior management to ensure effective implementation of policies, processes and systems at all decision making levels. Also, the Board of Directors must approve and review the tolerance and appetite for operational risk. The Board of Directors is responsible for:

a) Establishing an adequate organizational chart for the managing of operational risk;

b) Development of strategies and general policies for managing operational risk, in line with the bank's strategic goals;

c) Review and approval of senior management functions, authorization and regulation regarding the reporting of operational risk management, in order to ensure an efficient system of decision making at the bank and ensuring that operational risks facing the bank's operations are controlled within existing capacities;

d) Regular review of the operational risk reports, submitted by senior management, to understand the operational risk management within the bank and senior management must be effective in preventing material operational risk events, as well as monitoring and evaluating the effectiveness of the daily management of operational risk.

e) Ensure that senior management takes necessary measures to effectively identify, assess and monitor, control / reduce operational risk.

f) Ensure that the operational risk management system in the bank is effectively analyzed and audited by internal audit; and

g) Have an adequate system of reward-punishment to effectively promote the development of an operational risk management in the whole bank.

Article 6
Responsibilities of Senior Management

1. Senior Management in a bank is responsible for implementing operational risk management strategies, general policies and functional systems, approved by the Board of Directors.

Senior management should:

a) Report regularly to the Board of Directors, concerning the ongoing management of operational risk.

b) Compile and regularly review policies and procedures of operational risk management, and detailed processes in accordance with the overall strategies and policies developed by the Board, supervise their implementation, and presentation of operational risk management reports, on regular basis to the Board of Directors.

c) Sufficiently understand operational risk management in bank, especially events or programs that cause material operational risk.

d) Clearly define the responsibilities of each department in managing operational risk, as well as defining the reporting lines, the frequency of reporting and the report content; urge each department to define their responsibilities in order to assure sound performance of the operational risk management system.

e) Provide the operational risk management function with the necessary resources, including but not limited to the necessary funds, creation of staff positions needed to be effective, providing training courses for personnel of the operational risk management, delegation of authority for abovementioned personnel in order to fulfill their duties, and

f) Make precise controls and revisions in operational risk management, in order to effectively respond to operational risk events, as a result of internal changes in procedures, products, business activities, systems, information technology, personnel, external events or other factors.

2. Banks should establish a special department which will be responsible for system construction and implementation of operational risk management. This department should be independent from other departments in order to ensure consistency and efficiency of the system. Responsibilities of this department should include:

a) Drafting of policies, procedures and specific processes of operational risk management and delivering these policies to the senior management and Board of Directors for review and approval.

b) Assist other departments to identify, assess, monitor and control / mitigate operational risk.

c) Establish methods for the purpose of identification, assessment, reduction (including internal controls) and monitoring of operational risk, the formulation of a reporting process throughout the bank in terms of operational risk, organization and implementation.

d) Establishment of basic criteria on operational risk throughout the bank; direct and coordinate operational risk management.

e) Organize training for each department in relation to operational risk management and help them to improve their operational risk management capacities and to fulfill their duties.

f) On a regular basis control and analyze operational risk management practices in business departments and in other departments of the bank.

g) On regular basis deliver reports on operational risk to senior management, and

h) Ensure that the systems for the measurement of operational risk management are observed.

3. Relevant departments in the banks should be directly responsible for managing operational risk. The main responsibilities include:

a) Appointment of certain staff charged with operational risk management, including monitoring of policies, procedures and special processes for managing operational risk.

b) Follow-up evaluation methods for operational risk management with the aim of identifying and assessing operational risk across departments, and have a continuous effective procedure for monitoring, controlling/reduction and reporting of operational risks, and then organize their implementation.

c) Takes into account the requirements of operational risk management and internal controls, especially when particular business processes of departments are created, to ensure that operational risk management personnel, of all levels, takes part on reviewing and approving the procedures, controls and important policies, and thus to harmonize with the bank’s general policies in operational risk management; and

d) Monitor key risk indicators and regularly report the situations in operational risk management of their department to the department which is responsible, and take a leading role in the operational risk management throughout the bank.

4. Legal office, compliance office, information technology department and human resources in a bank must, except for proper management of its own operational risk, provide appropriate resources and assistance within their competencies and respective responsibilities to other departments, for the purpose of operational risk management.

5. The Internal Audit Department in a bank does not have direct responsibility nor does it participate in managing operational risk, but it should regularly evaluate how well the system of operational risk management operates, evaluate implementation of operational risk management policies, independently evaluates those policies, procedures and new operational risk management processes and report to the bank's Board of Directors the results of their assessment of the operational risk management system.

6. A bank with a complex and a high level of commercial activity is encouraged to give to an intermediary agency, the auditing and evaluating function of its operational risk management system, on an ongoing basis.

7. A bank must choose the most appropriate approach for the purpose of managing operational risk which may include: assessment of operational risk and internal controls, reporting of events that resulted in loss and data collection, monitoring the key risk indicators, risk assessment of new products and business practices, testing and auditing of internal controls, and reporting of operational risk.

8. A bank with a complex and a high level of commercial activity should adopt more sophisticated methods of risk management (e.g. quantitative methods) to assess each department’s operational risk, maintain a database on operational risk events that resulted in losses and make adjustments in accordance with the characteristics of operational risk, associated with each business line.

9. A bank must develop an effective process to regularly monitor and report on the operational risk status and of any material losses. For risks with increased potential for losses, an early warning system for operational risk should be established to control the risk reduction and reducing various events that can result in losses.

10. A bank shall establish and gradually improve the management information system for operational risk in order to efficiently identify, control and report operational risks. This system, at least, needs to register and save the date events and losses from operational risk. The system must rely on self-assessment of operational risk and control measures, monitoring of key risk indicators and the establishing of relevant information included in an operational risk report.

Article 7
Approaches for Calculating Capital for Operational Risk

1. Capital requirements for operational risk should be the amount calculated using:

a) Basic Indicator Approach

Under the Basic Indicator Approach, the capital requirement for operational risk is equal to 15 % (fifteen percent) of the relevant indicator.

1. The relevant indicator is the average over three years of the sum of net interest income and net non-interest income.

2. The three (3) year average is calculated on the basis of the last three twelve-monthly observations at the end of the financial year. When audited figures are not available, business estimates may be used.

When calculating the sum of net interest income and net non-interest income, banks shall use the following elements:

a) Interest income
b) Interest expenses
c) Dividend income
d) Fee and commission income
e) Fee and commission expenses
f) Net profit/loss on financial operations, including:
- Net income/loss from financial assets and liabilities intended for trading
- Net realized profit/loss from financial assets and liabilities which are not measured at fair value throughout the income statement, if they are the result of trading book items
- Net realized profit/loss from financial assets and liabilities recognized at fair value throughout the income statement, if they are the result of trading book items
- Changes to fair value during the calculation of risk mitigation
- Net profit/loss from exchange rate difference if they are the result of trading book items and if they are not included in the previous indents of point f)

g) Other operating income

During the calculation of the sum of net interest income and net non-interest income, items which by content are considered income from extraordinary or irregular items or income derived from insurance claims, shall be excluded.

Fee and commission expenses to external parties, shall include fees (commissions) paid to a parent or subsidiary of a credit institution or a subsidiary of a parent which is also the parent of a credit institution, while expenses for fees to other external parties are not included in fee and commission expenses. Fee and commission expenses to external parties are included in the basis for calculating capital requirements for operational risk (included in Fee and commission expenses) if it involves payment to an entity which is the subject of supervision (in accordance with the provisions of Directive 2006/48/EC of the European Parliament and of the Council).

3. If for any given observation, the sum of net interest income and net non-interest income is negative or equal to zero, this figure shall not be taken into account in the calculation of the three-year average. The relevant indicator shall be calculated as the sum of positive figures divided by the number of positive figures.

b. Standardized Approach

1. Under the Standardized Approach, the capital requirement for operational risk is the average over three years of the risk-weighted relevant indicators calculated each year across the business lines. In each year, a negative capital requirement in one business line, resulting from a negative relevant indicator may be imputed to the whole. However, where the aggregate capital charge across all business lines within a given year is negative, then the input to the average for that year shall be zero (business lines are defined in the CBK Regulation on Capital Adequacy).

2. Annual capital requirements are calculated as the sum of capital requirements for all business lines.

3. The capital requirements for a specific business line shall be equal to the product of the percentage, defined for that business line and its basis for the calculation of capital requirements for operational risk.

a) The basis for calculating capital requirements for operational risk, calculated by the standardized approach, is calculated separately for each business line and for each year taken into consideration for the calculation of the average, described above.

b) The basis for calculating the capital requirement for operational risk for a specific business line, calculated by the standardized approach, shall be the sum of net interest income and net non-interest income.

c) When audited figures are not available, business estimates may be used.

d) The methodologies for calculating the sum of net interest income and net non-interest income shall be applied, as described above.

4. Banks may select which approach for calculating the capital requirements for operational risk; however, should a bank wish to change its calculations for the capital requirements for operational risk to the other approach, it may do so only with the prior approval from CBK. This approval shall only be granted if there is a strong reason for using the other approach. In any event, for any approved change of calculations, the CBK will determine the date for changing to the other calculation approach.

5. Capital calculations for operational risk should be done as defined in the CBK Regulation on Banks Capital Adequacy.

Article 8
Loss Event Types Classification

Table

Event-Type Category	Definition
Internal Fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/discrimination events, which involves at least one internal party
External Fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party
Employment Practices and Workplace Safety	Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity/discrimination events
Clients, Products & Business Practices	Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product
Damage to Physical Assets	Losses arising from loss or damage to physical assets from natural disaster or other events
Business disruption and system failures	Losses arising from disruption of business or system failures
Execution, Delivery & Process Management	Losses from failed transaction processing or process management, from relations with trade counterparties and vendors

Article 9
Explanatory Notes to Processes, Systems, People and External Risks

1.“Risk from processes" - is the possibility of losses due to careless processing by workers, an accident or any other unauthorized activity. Banks operating in the Republic of Kosovo and licensed by the CBK, should work to increase the sophistication of risk management processes throughout the bank, ensuring that each branch follows a regular personal research risk process; minimization of losses in case of errors during processing or negligence, by drafting contingency plans and complete transfer of risk quantification under management.

2. "Systems Risk" - is the possibility of losses due to failures, misuse or unauthorized use of computer systems.

Stable computer systems are essential for the effective implementation of management strategy in terms of the Information Technology revolution. Banks should have contingency plans to minimize losses in case of failure (collapse) of the system. Developing such a system of risk management systems ensures that the bank as a whole has undertaken adequate risk management.

a) Problems associated with computers in banks now have greater influence in public, with increased risk of systems as a result of the revolution, network expansion and increasing the number of users of personal computers. In order to prevent a system crash, banks should take various measures, including doubling of various systems and infrastructure, constant maintenance of systems to ensure continuity, uninterrupted operations, and establish a system for disaster prevention. Banks must maintain the confidentiality of customer information and prevent disclosure of information, sensitive information must be encrypted, unauthorized access from outside must be blocked, and all known countermeasures, in order to ensure data, must be implemented. Also, each bank should have contingency plans and hold training sessions to ensure full preparation in case of emergencies. To maintain security, countermeasures should be reviewed when the new technology used.

4. “Personnel Risk” is an integral part of operational risk assessment and banks should consider to what extent the bank personnel may affect risk in their execution of business operations through the existing structure.

This includes the size, complexity, and transparency of the bank, the complexity and diversity of its products and the complexity of the systems which uses to perform its activities.

a) Banks should define its organizational structure and reporting lines in order to define the positions of the departments within the bank, the organizational structure of departments and sufficient, clear and direct reporting lines.
b) Banks should consider interventions with other departments in managing what data, reports or risk management responsibilities move across departments; definitions of roles or job descriptions, departmental activities and the role of management should be clearly defined, qualifications of staff and management. Management and key staff should be experienced.
c) Banks should consider also inherent risk which includes: turnover staff rate, job vacancies rate, organizational changes, staff size in relation to the volume of activities and reliance on key staff and management progress.
d) Banks should consider also residual risk which includes: system abuse, reliable information abuse, advertisements for job vacancies and the time left vacant, internal fraud rate, false claims costs, etc.
e) Banks, in managing human resources (people), must take into account that new staff recruitment is done based on competencies required, be cautious about training, train the staff with the necessary knowledge to effectively perform duties and make a program of staff turnover, with the aim of renewing the motivation and the elimination of risk associated with repetitive activities.

5. "External events" are the risks arising from: crimes (theft) from internal/external (fraud, theft, robbery), the elementary events, natural disasters, terror/war and political risks.

This type of risk also includes legal risk, which is the risk of loss because a contract cannot be enforced legally, and also includes the risk that comes as a result of inadequate documentation and insufficient authority to another party.

Article 10
Operational Risk Reporting

1. Banks, must report annually to the CBK on policies and procedures on managing operational risk and the reports about operational risk. Banks that entrust to other agencies its operational risk management system should also disclose those audit reports to the CBK.

2. Banks, immediately, should report to the CBK about operational risk events, if any of the following occurs:

a) Financial crimes, in which more than five thousand (5,000) Euros is stolen from the bank or in the event of stolen bank vehicles or any money stolen from a bank, instances of financial fraud or other cases involving lost monetary amounts over five thousand (5,000) Euros.

b) Events which result in serious damage or loss of important data of the bank, its books, a disruption of operations for more than two (2) to three (3) hours in two (2) or more branches / sub-branches, or interruption of operations for more than five (5) hours in a branch and which affects the normal operations of the bank.

c) Proprietary bank information that was stolen, sold or published without the bank's permission or any lost information which could affect the financial stability of the bank and that could lead to economic disorder.

d) Frequent violations of applicable rules by senior management,

e) Accidents or natural disasters, caused by any power, which results in immediate economic loss of ten thousand (10,000) Euros.

f) Other operational risks, which may result in the loss of more than 0.5% (one-half percent) of the equity of the bank, and

g) Other material events, as may be specified by the CBK.

3. CBK will regularly control and evaluate policies, procedures and practices of operational risk management in banks. The principal events which will be examined and evaluated include:

a) Effectiveness of operational risk management procedures,

b) Ability of the bank to monitor and report operational risk, including key risk indicators (KRI) and data from operational risk losses;

c) Measures of the bank that effectively and in proper time deals with operational risk events and other weak links;

d) Internal control procedures of the bank are reviewed and audited within operational risk management processes;

e) Quality and comprehensiveness of the bank's disaster recovery plans and its business continuity plan, including analysis of different scenarios;

f) Capital provisioning level of adequacy for operational risk, and

g) Other aspects of operational risk management as deemed appropriate.

Article 11
Enforcement, Remedial Measures and Civil Penalties

1. For operational risk problems discovered during a CBK Examination, banks must submit a plan for improvement and take all necessary actions within the time frame stipulated by the CBK.

2. When a material operational risk event occurs, and the bank fails to take effective measures to correct it within the stipulated time, the CBK will take appropriate regulatory action, in accordance with laws and regulations.

3. CBK may take measures under Articles 58, 59 and 82 of Law on Banks if the Banks fail to respect provisions of this Regulation.

Article 12
Abrogation

Upon entry into force of this Regulation, it shall abrogate any other provision that can be in collision with this Regulation.

Article 13
Entry into Force

This Regulation shall enter into force on December 03, 2012.

The Chairman of the Board of Central Bank of the Republic of Kosovo

_____

Sejdi Rexhepi