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

Advisory Letter 2009-02	**June 2009**
Internal Control System	

The purpose of this advisory letter is to provide guidelines for additional assistance to banks and branches of foreign banks, micro-finance institutions, and to other non bank financial institutions as the Central Bank of the Republic of Kosovo deems appropriate, hereafter referred to as "covered institutions", for Internal Control System, based on International best practices, when implementing certain aspects of Internal Control System requirements of Regulation 1999/21 on the Internal Controls and Audit, and Rule XXX on the Internal Control System, authorized under sections 46 of Regulation No. 1999/21 on Bank Licensing, Supervision and Regulation and Section 42 of Law on Central Bank of the Republic of Kosovo.

1. INTRODUCTION

1.1 A system of effective internal controls is a critical component of institution's management and a foundation for the safe and sound operations of the covered institutions. Weak or ineffective internal controls have caused losses in many banks and non bank financial institutions and have contributed to the failure of others around the world. Some of these cases involved could have been prevented or discovered through effective control mechanisms before the losses actually incurred by the institution. Viewing the fact of increasing importance of the effective internal control system in ensuring the prudent and safe operations of covered institutions, the Central Bank of the Republic of Kosovo hereby issues this Advisory Letter.

1.2 While the Central Bank recognizes that not all institutions may implement all aspects of this Advisory Letter, covered institutions are encouraged and required to establish, maintain and operate an effective system of internal controls that is appropriate to the size, nature, scope and risks of their activities. However, even though small institutions are likely to be less formal and less structured, their internal control system should be as effective as those at more complex and larger institutions. The Central Bank will closely monitor and evaluate the quality and effectiveness of covered institution's internal control system.

2. INTERNAL CONTROL OBJECTIVES

Despite the rapid changes in the banking industry, the fundamental concept behind effective internal controls remains the same. The internal controls are intended to ensure covered institutions achieve their goals and long-term profitability targets in a safe, prudent and controllable manner. To be concrete, an effective internal control system can assure covered institutions to meet the following objectives:

- Efficient and effective business operations;
- Accurate records of transactions;
- Reliable and complete financial and management reporting;
- Effective risk management systems; and
- Compliance with applicable laws and regulations, internal policies and procedures.

3. INTERNAL CONTROL PRINCIPLES

A covered institution, when establishing its internal control system, should comply with the following principles:

3.1 Efficient and Effective. Internal control must be consistently applied and well understood by the staff, so that the board and management policies are to be efficiently and effectively implemented. Meanwhile, internal controls should not tolerate any mismanagement by the board and top managers.

3.2 Prudent. The core of internal controls is to effectively mitigate activity risks. Prudence should always be the priority in establishing the internal control system.

3.3 Comprehensive. Internal control policies and procedures should cover all aspects of institution's business and its operations.

3.4 Timely. Internal controls should be established from the very beginning of the business commencement and function properly to send early warning signals allowing the management to take corrective actions to mitigate and avoid the potential risks.

3.5 Independent. The duty of evaluating the effectiveness of internal control system should be separate from that of formulating and executing the internal controls. The quality and appropriateness of internal controls should be evaluated independently.

4. INTERNAL CONTROL COMPONENTS

Internal control consists of five interrelated elements:

- Management oversight and the control culture;
- Risk recognition and assessment;
- Control activities and segregation of duties;
- Accounting, information and communication systems; and
- Monitoring activities and correcting deficiencies.

5. Management oversight and the control culture

5.1 The control environment reflects the Governing Boards' and Management's commitment to internal controls. It provides discipline and structure to the control system. Elements of the control environment include:

- The organizational structure of the institution;
- Management philosophy and operating style;
- The integrity, ethics, and competence of personnel;
- The external influences that affect the institution's operations and risk management practices, e.g., independent audit;
- The attention and direction provided by the Governing Board and its committees;
- The effectiveness of human resources policies and procedures.

5.2 The Governing Board should have responsibility for formulating, approving and annually reviewing the overall business strategies and significant policies of the covered institution; understanding the major risks run by the institution, setting tolerance limits for these risks and ensuring that the senior management takes the steps essential to identify, measure, monitor and control these risks; approving the organizational structure; and clearly defining the authorities and responsibilities, effectively utilizing the work conducted by internal and external auditors, in recognition of the important control function they provide.

5.3 The Governing Board should periodically discuss with management concerning the effectiveness of the internal control system; timely review the evaluation procedure and results of internal controls; instantly ensure management's prompt follow-up on recommendations and concerns expressed by stakeholders, regulators, shareholders and customers on internal control weaknesses; and periodically review the appropriateness of the institution's strategy and risk limits.

5.4 Senior management should have responsibility for carrying out the directives of the Governing Board, including the implementation of strategies and policies. Senior management should maintain an organizational structure that clearly assigns responsibility, authority and reporting relationships. The allocation of duties and responsibilities should ensure that there are no gaps in reporting lines and that an effective level of management control is extended to all levels of the institution and its various activities. Delegation is an essential part of the management. It is important for the senior management to oversee the managers to whom they have delegated these responsibilities to ensure that they take the duties properly.

5.5 Senior management should be responsible for developing processes that identify, measure, monitor and control risks, and developing processes that recruit, remunerate, motivate and reward capable staff to attract those qualified to be with the institution.

5.6 An essential element of an effective control system is a strong control culture. The Governing Board and senior management are responsible for promoting high ethical and integrity standards, and for establishing a culture within the organization that emphasizes and demonstrates to all levels of personnel the importance of internal controls. All personnel at a covered institution need to understand their role in the internal control process and be fully engaged in the process.

5.7 In reinforcing ethical values, covered institutions should avoid policies and practices that may inadvertently provide incentives or temptations for inappropriate activities. Performance targets or other operational results should not be achieved at the price of ignoring the long-term risks.

6. *Risk Recognition and Assessment*

6.1 Risk recognition and assessment is the process established by the Governing Board and management to identify and analyze risks that could keep the institution from achieving planned objectives. The assessment should help determine what the risks are, how they should be managed, and what controls are needed. Risks can arise or change due to factors such as:

- A change in the institution's operating environment;
- New personnel;
- New or revamped information systems;
- Rapid growth;
- New technology;
- New or expanded lines of business, products, or activities;
- Mergers or other corporate restructuring, and
- Changes in accounting requirement.

6.2 A risk assessment should identify and evaluate the internal and external factors that could adversely affect the achievement of the institution's performance, information and compliance objectives. This assessment should cover all risks facing the covered institution (that is, credit risk, country and transfer risk, market risk, liquidity risk, operational risk, and reputation risk).

6.3 The risk assessment should be conducted at all level of individual businesses and across the wide spectrum of activities. Effective risk assessment addresses both measurable and non-measurable aspects and weighs costs of controls against the benefits they provide.

6.4 The risk assessment should also determine which risks are controllable and which are not. For those risks that are controllable, the covered institution must assess whether to accept those risks or the extent to which it wishes to mitigate the risks through control procedures. For those that cannot be controlled, the covered institution

must decide whether to accept these risks or to withdraw from or reduce the level of business activity concerned.

6.5 Internal controls may need to be revised to appropriately address any new or previously uncontrolled risks. For example, as new financial innovation occurs, a covered institution needs to evaluate new financial instruments and market transactions and consider the risks associated with these activities.

7. *Control Activities and Segregation of Duties*

7.1 Control activities include the policies, procedures and practices established to help ensure that personnel carry out the Board's and management directives. These activities help to ensure that the Board and management manage and control risks that could affect the operating performance or cause financial loss. Policies governing control activities should ensure that covered institution's officers who perform internal control functions in addition to their operational duties do not evaluate their own work.

7.2 Control activities are applied at various organizational and functional levels and include:

- *Operational performance reviews.* These control activities include risk assessments and reviews of actual financial performance versus budgets, forecasts, and prior-period performance as well as operational activities control. In performing these reviews, the covered institution relates various sets of data to one another. The covered institution use comparisons to analyze its actual versus projected or required performance to identify reasons for significant variances and to determine whether any specific activity should be adjusted.

- *Information processing.* Information systems control activities can be broadly grouped into two categories: general controls and application controls. General controls commonly include controls over data center operations, system software acquisition and maintenance. These controls apply to mainframes, servers, end users workstations, and internal or external networks. Application controls apply to programs the institution uses to process transactions and help ensure that transactions are valid, properly authorized and accurate.

- *Compliance with exposure limits.* The establishment of prudent limits on risk exposures is an important aspect of risk management. For example, compliance with limits for exposure to borrowers and other counter parties reduces the covered institution's concentration of credit risk and helps to diversify its risk profile. Consequently, an important aspect of internal controls is a process for reviewing compliance with such limits and follow-up on instances of non-compliance.

- *Physical controls.* Generally, these activities ensure the physical security of covered institution assets. They include safeguarding assets and records, limiting access to computer programs and data files, and periodically comparing actual asset or liability values with those shown on control records.

- *Approvals and authorizations.* Appropriate authority delegation shall not compromise necessary approval and authorization. Requiring approval and authorization for certain limits ensures that management is aware of the transaction or situation so as to enhance the accountability system.

- *Verification and reconciliation.* Verification of transaction details, activities and the output of various processing and management systems are very important for the covered institution to ensure accuracy and reliability of operational, financial and management reports. Reconciliations shall be carried out periodically in order to identify activities and records that need rectification or other kind of actions. Consequently, any exceptional or extraordinary result of these verifications and reconciliations should be reported timely to the appropriate level of management.

- *Segregation of duties.* Covered institutions establish segregation of duties by assigning different people the responsibilities for authorizing transactions, recording transactions, and maintaining custody of assets. Such segregation is intended to make it impossible for any person to be in a position to both perpetrate and conceal errors or irregularities in the normal course of his or her duties. Areas of potential conflicts of interest should be identified, minimized and subject to careful independent monitoring.

7.3 Control activities are most effective when they are viewed as an integral part of, rather than an addition to, the daily activities of the covered institution. It is not sufficient for senior management to simply establish appropriate policies and procedures for the various activities and divisions of the institution. They must regularly ensure that all areas of the institution are in compliance with such policies and procedures and also determine that existing policies and procedures remain adequate.

8. *Accounting, Information and Communications Systems*

8.1 Accounting information and communication systems identify, capture and exchange information in a form that enables personnel to carry out their responsibilities. Accounting systems include methods and records that identify, assemble, analyze, classify, record and report a covered institution transactions. Information systems produce reports on operations, finance, risk management and compliance that enable the Board and management to take important decisions. Communication systems impart information throughout the institution and to external parties such as regulators, examiners, shareholders and customers.

8.2 An effective internal control system requires that there are adequate and comprehensive internal accounting, financial, operational and compliance data, as well as external market information about events and conditions that are relevant to decision making. Information should be reliable, timely, and accessible and provided in a consistent manner.

8.3 An effective internal control system also requires the establishment and maintenance of management information systems that cover the full range of the covered institution activities. These systems, including those that hold and use data in an electronic form, must be secure, monitored independently and supported by adequate contingency arrangements.

8.4 An effective internal control system also requires effective communication channels to ensure that all staff fully understand and adhere to policies and procedures affecting their duties and responsibilities and that other relevant information is reaching the appropriate personnel.

8.5 The senior management should be responsible for establishing a communication path, ensuring the relevant information is reaching the right personnel, and establishing an organizational structure to facilitate the adequate flow of information, either upward, downward, or across organization.

9. *Monitoring Activities and Correcting Deficiencies*

9.1 This includes at least five areas:

- The overall effectiveness of the covered institution internal control system should be monitored on an on-going basis. On-going monitoring can have the advantage of quickly detecting and correcting the deficiencies in the system, and facilitating the senior management to take actions at the earliest time. Some of the key risks should be part of the daily activities of the covered institution. Meanwhile, the external auditors play an important role in monitoring the institution's internal control policies and procedures. External auditor's functioning in this field is, viewed by the Central Bank, an integral part of its quality assessment.

- Internal audit should function independently. The internal auditors should report to the Governing Board, either directly or through audit committee, as deemed appropriate by individual institutions. The Governing Board is responsible for establishing and monitoring effective audit functioning, and determines how intensive auditing must be to effectively test and monitor internal controls and to ensure the reliability of the covered institution's financial statements and reporting. A clear and focused internal audit program can be a key defense against control breakdowns or fraud by providing independent assessments of the internal control system's quality and effectiveness. Due to the important nature

of this function, internal audit must be staffed with competent, appropriately trained staff that has a clear understanding of their role and responsibilities.

- Monitoring the effectiveness of internal controls can be done by personnel from several different areas, including the business function itself, internal audit and financial control, etc.

- Internal control deficiencies, whether identified by business line, internal audit, or other control personnel, should be reported timely to the appropriate management level, with serious matters reported to senior management and the Governing Board.

- The management should rectify the deficiencies identified on a timely basis. It is also important that the Governing Board and senior management periodically receive reports summarizing all control issues and establish a system to track the internal control weakness.

9.2 Establishment of Specialized Committees

The Central Bank believes it is necessary for a covered institution to establish the following specialized committees, in accordance with section 20 of UNMIK Regulation 1999/21, and structures having similar functions, including:

- An *Audit Committee*. It is important that the audit committee report directly to the Governing Board. This allows for the proper functioning of corporate governance by giving the Board unbiased information. The committee provides oversight of the covered institution internal and external auditors, approves their appointments and dismissal, approves their compensation structure, reviews and approves audit scope and frequency, and ensures the management take prompt and proper corrective actions to address control weaknesses, non-compliance with policies, laws and regulations, and other problems identified by the auditors.

- *Asset and Liability Management Committee*. The members of the committee should represent both the asset sides and the liability sides of the balance sheet. Typically, it includes the chief executive officer, the chief financial officer, the treasurer, the chief credit officer, and the officer in charge of the deposit-taking. Other members, from the business lines, are highly encouraged.

- *A Risk Management Committee.* It provides oversight of senior management's activities in managing credit, market, liquidity, operational, legal and other risks of the covered institution. Members of the committee should come from management of major business lines. Representatives from certain particular departments, e.g. credit administration and audit are extremely important.

In addition, covered institutions can establish the following committees, as deems necessary:

- *A Compensation Committee.* This committee provides oversight of remuneration of senior management and other key personnel and ensures a consistent compensation with the covered institution's culture, strategy, vision and control environment. The Board should approve the relevant remuneration policies and packages based on the committee's recommendations.

- *A Nomination Committee.* It provides important assessment of Board effectiveness and directs the process of renewing and replacing Board members. The committee should ensure that only the most competent individuals are appointed to the Board and key management positions. It is responsible for making recommendations to the Board on all new appointments of directors and senior executives. The Board should approve appointments based on the committee's recommendations.

10. *Internal Audit Function*

10.1 The internal audit function is an independent authority which provides reasonable assurance that operations and their associated risks are being effectively and efficiently managed. Compared with the previous internal audit accounting based principal, now it covers all units and processes of the organization with a growing authority and responsibility.

10.2 An effective internal audit function is a valuable source of information for covered institution's management as well as supervisors, about the quality of a covered institution's internal control system.

10.3 *The following prerequisites are critical for ensuring an effective internal audit function:*

Permanent Function. Internal audit should be a permanent function that is proportionate to the covered institution's size and the nature of its operations. Senior management shall provide appropriate resources and staffing to the internal audit function in order to achieve its objectives.

.

Independent Function. The internal audit department shall be independent which shall operate under the direct oversight of the covered institution's Governing Board, audit committee and Chief Executive Officer. The head of internal audit department should have the authority to initiate direct communication with the Board, the audit committee or the Chief Executive Officer, as well as the external auditor. At least a portion of the regular audit committee meeting should be held with the internal auditor and independent of bank management, which must be documented in the audit committee minutes. The covered institution's internal audit function must be independent of the activities audited and from the day to day internal control processes.

Internal Audit Charter. Internal audit charter is a fundamental document that enhances the standing and authority of the internal audit function. The charter should be drawn up, and periodically reviewed by the internal audit department, approved by the senior management and subsequently confirmed by the Board of Directors or its audit committee.

a) *The internal audit charter shall establish*:

- Objectives and scope of the internal audit function
- Internal audit department's position and reporting line within the organization, its powers, responsibilities and relations with other control functions
- Accountability of the head of internal audit department

b) *The charter gives the internal audit department the right:*

- of initiative and authorizes it to have direct access to and communicate with any member of staff
- to examine any activity or entity of the covered institution
- to access any records, files or data of the covered institution, including management information and the minutes of all consultative and decision-making bodies, whenever relevant to the performance of its assignments.

Objectivity. The internal audit function must be objective and disclose all material facts known to them, that if not disclosed, may distort the reporting of activities under review. The internal auditors should not assess those activities for which they had day to day responsibility within the previous year.

Professional Competence. Professionally competent and motivated internal auditors are essential for an effective internal audit department. Professional competence should be maintained through systematic continuous training of each member of staff. All staff members of the internal audit department should have a sufficient up-to-date knowledge of auditing techniques and banking activities. Internal auditors should only engage in those services for which they have the necessary knowledge, skills and experience.

The risk based audit model. During the course of the business cycle, the internal audit department has access to relevant information, including business objectives, executive committee minutes, risk control reports, financial reports and incident reports. This information is used by internal audit to develop the risk based audit model, a systematic assessment of the risks and control levels in a covered institution's activities and entities. The risk based audit model is a key input to the development of the annual audit plan.

Risk-based annual audit plan. The internal audit department defines an audit universe, from which the audit plan is developed. The internal audit department should have

access to any records, files or data of the covered institution including management information and minutes of the consultative and decision-making bodies, and its scope of investigation must include every activity of the covered institution. The internal audit department shall prepare a risk-based audit plan on an annual basis, for all assignments to be performed.

a) *The Audit plan must be realistic and detail the following*:

- the scope and timing of planned internal audit assignments;
- the staffing and requirements to perform these assignments and their qualifications and expertise;
- a time budged for other assignments and activities such as specific examinations, consulting engagements and training.

b) The audit plan should be regularly reviewed and updated when necessary, by the internal audit department and should be approved by the covered institution's Governing Board and the audit committee. This approval implies that the covered institution will make the appropriate resources available to the internal audit department.

10.4 *Types of Audit*

a) In general, audit services can be divided into three types:

Financial audits. The analysis of the economic activity of an entity as measured and reported by accounting methods.

Compliance audits. The review of both financial and operating controls and transactions to see how well they conform with established laws, standards, regulations and procedures.

Operational audits. The comprehensive review of the varied functions within an institution to appraise the efficiency and economy of operations and the effectiveness with which those functions achieve their objectives.

b) *Audit Reports*. An audit report should be accurate, objective, clear, concise, constructive and complete; it should include the audit's objectives and scope as well as applicable conclusions, recommendations and action plans.

Generally, an audit report consists of two parts:

1. An executive summary that is communicated to management and members of the audit committee and, when relevant or requested to the external auditors, which contains an overall audit opinion and main findings and recommendations.

2. A detailed report that is provided to the auditee. The report elaborates on findings, risks and issues, as well as recommendations to address the findings and to mitigate the identified risks. Usually, the detailed report is provided to management, members of audit committee, supervisors and the external auditor on request.

10.5 The internal audit department should follow up to verify that its recommendations are implemented. The status of actions taken to address recommendations is communicated to senior management and to the Governing Board or its audit committee.

11. General Guidance

This Advisory Letter has been developed using *Framework for Internal Control Systems in Banking Organizations*, September 1998, and *Internal Audit in Banks and the Supervisor's Relationship with Auditors*, August 2001, issued by *Basel Committee on Banking Supervision.* For further guidance, covered institutions can consult papers issued by the Basel Committee on Banking Supervision (*www.bis.org*), and the regulatory manuals from internationally recognized regulators such as: Committee of European Banking Supervision (*www.c-ebs.org),* Comptroller of the Currency *(www.occ.treas.gov),*Federal Reserve Board of the Governors *(www.federalreserve.gov*), and the Financial Services Authority *(www.fsa.gov.uk).*