National Bank of the Republic of Macedonia
Supervisory Policy Manual

Title: M-1 Sound Corporate Governance Practices

Date: FINAL

Purpose: Explanation and guidance for sound Corporate Governance practices

Issue Type: Guidance

Supersedes Previous Issue: Supervision Circular No. 4, Corporate Management Systems in Banks, dated December, 2002

Application: All Licensed Institutions

Contents:

1. Introduction
2. The Meaning of Corporate Governance
3. Supervisory Board
   3.1. Overview
   3.2. Characteristics of a Member of the Supervisory Board
   3.3. Primary Responsibilities of the Supervisory Board and its Members
   3.4. Policy Development
   3.5. Reports and Information to be Submitted to the Supervisory Board
4. Risk Management Committee
5. Auditing Committee and Internal Audit Function
   5.1. Overview
   5.2. Auditing Committee
   5.3. Internal Audit Function
6. Board of Directors
7. Compliance Function
   7.1. Introduction
   7.2. Responsibilities of the Supervisory Board Concerning Compliance
   7.3. Responsibilities of the Board of Directors Concerning Compliance
   7.4. Compliance Function Principles

1. Introduction

1.1. The National Bank of the Republic of Macedonia (NBRM) is especially concentrated on establishing solid grounds for licensed institutions' sound management and corporate governance practices. Hereby, the NBRM within its risk-based supervision framework will closely evaluate an institution's corporate governance practices.

1.2. Effective corporate governance practices, which are critical to the proper functioning of the financial sector and the economy as a whole, are essential to achieving and maintaining public trust and confidence in the Macedonian financial system. Poor corporate governance may contribute to a licensed institution's failure. This can result in significant public costs and consequences due to the potential impact on the deposit insurance system and the possibility of broader macroeconomic implications, such as contagion risk and the impact on payment systems. Additionally, poor corporate governance can lead markets to lose confidence in the ability of an institution to properly manage its assets and liabilities, including deposits, which could in turn trigger a deposit run or liquidity crisis.

1.3. The references used in preparing this guidance are as follows:

- Respective provisions from the Law on Banks;
- "Enhancing Corporate Governance for Banking Organizations", Basel Committee on Banking Supervision, (February, 2006);
- "Internal Audit in Banks and the Supervisor's Relationship with Auditors," Basel Committee on Banking Supervision, (August, 2001); and
- "Compliance and compliance function in banks" Basel Committee on Banking Supervision, (April, 2005).

1.4. This guidance provides the basic directions for establishing an efficient corporate governance process, especially stressing the definition of the rights and responsibilities of an institution's members of the Supervisory Board (Board) and Board of Directors (Directors). This guidance does not aim to cover all aspects of corporate governance, but rather serves as a guide for better understanding of the rights and responsibilities of persons responsible for an institution's corporate governance process.

1.5. This Guidance covers the following concepts of good corporate governance practices:

- The meaning of corporate governance;
- Place, role and responsibilities of the Supervisory Board;
- Place, role and responsibilities of the Risk Management Committee;
- Place, role and responsibilities of the Auditing Committee;
- Board of Directors; and
- Compliance function.

2. The Meaning of Corporate Governance

2.1. The "OECD Principles of Corporate Governance," revised April 2004, defines corporate governance as involving "a set of relationships between a company's management, its board, its shareholders, and other stakeholders. Corporate governance also provides the

structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined. Good corporate governance should provide proper incentives for the board and management to pursue objectives that are in the interests of the company and its shareholders and should facilitate effective monitoring. The presence of an effective corporate governance system, within an individual company and across an economy as a whole, helps to provide a degree of confidence that is necessary for the proper functioning of a market economy."

2.2. From a financial industry perspective, corporate governance involves the manner in which the business and affairs of individual institutions are governed by their Boards and Directors; affecting how institutions:

- Set corporate objectives (including generating economic returns to owners);
- Manage the day-to-day operations of the business;
- Consider the interests of recognized stakeholders;
- Align corporate activities and behaviors with the expectation that the institution will operate in a safe and sound manner, and in compliance with applicable laws and regulations; and
- Protect the interests of depositors.

2.3. With respect to financial institutions, good corporate governance requires an understanding of how the Board and Directors (and other persons of special rights and responsibilities) conduct the institution's affairs and daily activities, placing emphasis on:

2.3.1. *Defining the strategic goals of the institution*. All activities of an institution should be conducted in accordance with pre-defined strategic goals, which serve as a framework within which the institution operates.

2.3.2. *Determining the responsibilities and authorities in decision making through a well defined corporate structure*. The Board should precisely define the rights and responsibilities of its members and Directors. The lack of well-defined responsibilities could create confusion, i.e. multiple lines of responsibilities could impede executives and employees from accomplishing assigned tasks. Directors are responsible for establishing a transparent corporate structure from which it can be clearly understood the level of responsibilities and authorities, lines of control, and the evaluation of performance. The corporate structure should also facilitate efficient internal and external control systems and an integrated risk management process.

2.3.3. *Managing the daily activities of the institution.* Management is composed of a group of individuals responsible for all the institution's daily operations. Given that management is a crucial component of sound corporate governance, the "four eyes" principle must be considered when making "important managerial decisions". The Board and Directors should avoid the following types of individuals as potential managers:

- An individual who has a large number of tasks concentrated in his/her everyday work activities and does not appropriately delegate. This person is constantly over worked and lacks time to carry out all of assigned activities. Such an individual has the potential for making mistakes and reaching wrong decisions;

- An individual responsible for managing a certain area in which he/she lacks knowledge and experience;
- An individual that is unprepared or fails to carry out proper internal control procedures; or
- An individual who is unwilling or unable to exercise effective control over the activities of apparent "star" employees. This is especially problematic where managers fail to question employees who generate returns (profits) that are out of line with reasonable expectations for fear of losing either revenue or the employee.

2.3.4. *Defining the relations between Directors, the Board and the Auditors of the institution.* The role of the auditors is an integral part in the process of good corporate governance. Internal and external auditors represent very important agents of the Board. This especially refers to the auditors' role of independently evaluating and verifying information submitted to the Board and Directors. The efficiency of Directors and the Board will be increased through:

- Recognizing the importance of the audit function and internal control processes, and communicating their importance throughout the institution;
- Increasing the independence of internal auditors;
- Considering in a timely and efficient manner auditors' findings;
- Establishing a direct independent line of communication from the chief internal auditor to members of the Board; and
- Engaging a competent and independent external auditor.

2.3.5. *Adopting a code of ethics and other standards of "good behavior" for all employees, including persons with special rights and responsibilities.* The Board should implement a set of precisely defined moral and ethical values for all employees to follow, including individuals with special rights and responsibilities. Each institution should produce a "code of ethics" that guides employee conduct. It is especially important that the "code of ethics" address corruption, self-dealing and any other illegal, unethical or questionable behavior in the institution's internal and external activities. Additionally, salary compensation for managers and key personnel should emphasize ethical behavior and establish incentives for appropriate risk taking. The Board should review and approve Directors salaries, bonuses and benefits, at least annually; ensuring compensation adequately motivates them to carry out their responsibilities in the best interests of the institution, shareholders and depositors.

2.3.6. *Understanding the institution's operational structure.* The Board and Directors should understand the institution's operational structure, including where the institution operates in jurisdictions, or through structures, that impede transparency. In this regard, the Board, or Directors consistent with guidance from the Board, should ensure the institution has appropriate policies and procedures to:

- Set forth clear corporate governance expectations and responsibilities for all relevant entities and business lines within the organization;
- Regularly evaluate the need to operate in jurisdictions or through complex structures that reduce transparency;

- Identify, measure and manage all material risks, including legal and reputation risks, arising from activities that reduce transparency;
- Establish appropriate processes for the approval of transactions and new products, especially related to activities that reduce transparency(e.g. applicable limits, measures to mitigate legal or reputation risks, and information requirements);
- Define and understand the purpose of such activities, and ensure that the actual exercise of these activities is consistent with their intended purpose;
- Ensure that these activities have well developed internal controls and are within the scope of internal and external audit reviews; and
- Ensure that information regarding these activities and associated risks is readily available and appropriately reported to the Board and NBRM, including adequate information regarding the purpose, strategies, structures, volume, risks and controls around such activities.

2.3.7. *Establishing information systems for public disclosure.* Efficient corporate governance presupposes establishing accurate and timely information concerning the institution's financial condition, corporate structure, Board and Directors. Appropriate public disclosure facilitates market discipline and thereby sound corporate governance. The following is a recommended list of information, related specifically to the corporate governance framework, an institution may choose to disclose to the public:

- The full (annual) financial statement, with supporting notes and schedules, available to depositors and other customers (e.g. on the institution's website and/or in the institution's premises) in order to provide them with a clear and comprehensive picture of the financial standing of the institution and enable them to exercise market discipline;
- Board structure (e.g. bylaws, size, membership, selection process, qualifications, other directorships, criteria for independence, material interests in transactions or matters affecting the institution, and committee membership, charters and responsibilities) and Directors structure (e.g. responsibilities, reporting lines, qualifications and experience);
- Basic ownership structure (e.g. major share ownership and voting rights, beneficial owners, major shareholder participation on the Board or in Directors positions, shareholder meetings);
- Organizational structure (e.g. general organizational chart, business lines, subsidiaries and affiliates, management committees);
- Information about the incentive structure of the institution (e.g. remuneration policies, director and executive compensation, bonuses, stock options);
- The institution's code or policy of business conduct and/or ethics (including any waivers, if applicable), as well as any applicable governance structures and policies (in particular, the content of any corporate governance code or policy and the process by which it is implemented, as well as a self-assessment by the Board of its performance relative to this code or policy); and
- The institution's policies related to conflicts of interest, as well as the nature and extent of transactions with affiliates and related parties (which may be in aggregate form for routine lending to employees), including any institution matters for which

members of the Board or Directors have material interests either directly, indirectly, or on behalf of third parties.

3. Supervisory Board

3.1. Overview

3.1.1. The Board (which is comprised of at least five, but not more than nine members) has one of the most important roles in corporate governance. It is primarily responsible to the shareholders of the institution as their representative, but is also responsible to other stakeholders (i.e. depositors, creditors, regulators and the community in general). The primary responsibilities of the Board are to:

- Hire competent management. Board appoints and dismisses members of the institution's Board of Directors and Risk Management Committee;
- Develop adequate plans and policies. Board approves the institution's development plan, financial plan, annual plan of the Internal Audit Department, etc.;
- Ensure risks are properly managed;
- Monitor and oversee the institution’s business activities and operations;
- Establish an adequate internal control system that detects and prevents problems and ensures compliance with laws and regulations; and
- Ensure the institution’s financial stability.

The Supervisory Board shall also perform the following activities:

- Approves the information security policy;
- Approves the institution's risk management policies;
- Discusses the reports on the activities of the institution's Board of Directors, Risk Management Committee, Auditing Committee, Compliance Officer/Department, report of the auditing company, reports delivered by the National Bank, the Public Revenue Office and other competent bodies and proposes, i.e. undertakes measures and activities for overcoming the identified shortcomings and weaknesses in the institution's operations; and
- Approves the institution's Code of Conduct.

The Supervisory Board should make a self-assessment of its operations from the aspect of the individual members and jointly at least once a year.

3.1.2. *The Board and Directors must operate together in order to promote the best interests of the institution.* Therefore, it is necessary to hold regular meetings of the Board with the institution’s Directors (as well as with internal and external auditors). This allows the Board to establish and adopt adequate policies, promote effective communication, and provide the most efficient evaluation of accomplishing established goals. However, members of the Board must have a precise understanding of their independent function in corporate governance. *It is very important that both bodies understand that Directors work for the Board i.e. the Board does not work for Directors.* When Directors dictate the activities that should be carried out by the Board, the Board neither fulfills its responsibilities, nor does it serve the good of the institution and properly represent the shareholders. The Board should conversely exempt itself from involvement in the daily management of the institution.

3.1.3. In order to oversee the institution's business activities and operations, and to evaluate Directors performance, the Board must receive timely information, and be able to develop its own opinion independent of Directors. Board members should be elected on the basis of their knowledge and experience that contribute to the smooth operation of the Board as a whole. The involvement on the Board of qualified individuals, who are not members of the institution's Directors, can strengthen the independence and the objectivity of decision-making. Furthermore, qualified members can bring new perspectives from other businesses that improve the institution's strategic direction.

3.2. **Characteristics of a Member of the Supervisory Board**

3.2.1. These characteristics should be considered when nominating members of the Board:

- Capable of exercising judgment independent of the views of management, political interests or inappropriate outside interests, and who possesses wisdom, honesty, and strong personal integrity. In addition, Board members have a responsibility to protect the institution from illegal or inappropriate actions or influences of dominant or controlling shareholders that are harmful to, or not in the best interest of, the institution and its shareholders;
- Knowledge of the finance industry and the laws and regulations governing the institution, as well as knowledge of the environment the institution operates in, especially the segments that use the services of the institution. As a result of their "status" within different economic segments that use the institution's services, Board members can and should contribute in attracting new clients for the institution;
- Readiness to put the institution's interests above their personal interests, i.e. readiness to avoid conflicts of interest. When a conflict of interest occurs, a Board member should disclose this fact and withdraw from decision-making due to his/her inability to provide the necessary level of objectivity. Furthermore, clients whose loans are classified in categories D and E are not desirable as Board members; and
- Readiness to dedicate enough time for preparation and regular participation in Board meetings, i.e. active fulfillment of expected responsibilities and obligations.

3.3. **Primary Responsibilities of the Supervisory Board and its Members**

3.3.1. Hire competent Directors, and assure Directors employ qualified employees capable to carry out assigned tasks. If it is evident that Directors do not fulfill their responsibilities as expected, the Board should give instructions for overcoming weaknesses or find a competent replacement.

3.3.2. Evaluate, at least once a year, Directors performance. The performance evaluation should stress what has been accomplished according to plans and what could have been done better. It is especially important to provide motivation to Directors and other key personnel to work for the best interests of the institution. The system of compensation should be consistent with the institution's code of ethics, goals, strategy and market environment.

3.3.3. Ensure an appropriate management succession plan is in place.

3.3.4. Set strategic goals and values. It is difficult to conduct the activities of an institution when there are no strategic objectives or guiding corporate values. Therefore, the Board should establish strategic objectives and high standards of professional conduct that will direct the ongoing activities of the institution, taking into account the interests of shareholders and depositors. The Board should take steps to ensure that these objectives and standards are widely communicated within the institution.

3.3.5. Establish clear lines of responsibility. An effective Board establishes clear lines of authority and key responsibilities for itself and Directors. Undefined or multiple lines of responsibility results in confusion and may cause problems due to untimely or delayed decisions. Directors are responsible for creating an effective corporate structure and lines of authority, in order to properly and efficiently conduct the daily operations of the institution.

3.3.6. Adopt and periodically review all policies.

3.3.7. Assess periodically the effectiveness of their own governance practices, including nomination and election of Board members, their management of conflicts of interest, a determination of weaknesses, and corrective action as necessary.

3.3.8. Ensure risks are properly managed. By definition, the institution in its activities undertakes different types of inherent risks. The Board should know the risks involved in the institution's operations, and the potential effects these risks may have on income and capital. The Board should also know the basic methods Directors uses to identify, measure, monitor and control risks. The identified risk categories that an institution's Board, Directors and risk management systems should address are:

- Credit Risk
- Liquidity Risk
- Market Risk (including Interest Rate, Foreign Exchange, and Price Risks)
- Operations Risk
- Information Technology Risk
- Legal Risk
- Strategic Risk and
- All other risks not mentioned above.

3.3.9. Understand and manage the risks associated with outsourcing any of the institution's key functions. The accountability of the Board and Directors of the institution cannot be delegated to the entities providing the outsourced services. Outsourcing of operational functions in relation to internal audit, compliance, risk management, or of other operational functions, does not eliminate the Board's obligations and responsibilities with respect to maintaining adequate oversight functions.

3.3.10. Monitor the institution's activities. Although the Board relies on the ability of Directors in conducting daily activities, the Board remains responsible for the operations and the financial activity of the institution. The Board should monitor the institution's operations through reports provided by Directors, however, it must be

certain the reports are accurate, complete and all-inclusive. The Board has the right and the responsibility to ask for accurate and complete information in order to fulfill its responsibilities. Therefore, it is of special importance to review reports produced and activities conducted by internal and external auditors, since they conduct an independent evaluation of information and operations of the institution.

3.3.11. Monitor and evaluate the operations of the institution. Establishing stable operations is the basic responsibility of the Board. For this purpose, the Board should receive adequate financial information and analysis, based upon which the following questions can be answered:

- Did Directors reach the goals set in the planning process? If not, what are the reasons?
- Is the plan unrealistic due to changes in the market environment?
- Does income show constant growth or is it characterized by large fluctuations?
- Is income a result of the implementation of planned strategies or is it a result of transactions designed to increase short-term profits with simultaneous increased risk in the long-term?
- Does the institution have sufficient capital to support inherent risks and the risks undertaken based on business strategies?
- Are Board reports correct with respect to the total and real estimation of balance sheet and off balance sheet positions?

3.3.12. Ensure Directors carry out their responsibilities to comply with all laws and regulations.

3.3.13. Perform the following regulatory requirements:

- Establish the institution's business policy and interest rate policy;
- Organize the Shareholders Assembly (specifies the agenda, prepares the proposed acts that are adopted by the Assembly, submits operational reports to the Assembly, proposes a decision on the use and allocation of realized profits (i.e. covering losses, dividend payment, etc.);
- Organize the Risk Management Committee;
- Organize the Auditing Committee and audit function of the institution, approve the scope of the internal auditor's work activities and the resources necessary to carry out the activities, approve the annual plan of the Internal Audit function, propose appointment of suitable external auditor, and analyze all audit results. The Board approves the internal audit policy and procedures, supervises the appropriateness of the procedures and the efficiency of the operations of the Internal Audit Department and reviews its reports;
- Determine the list of net debtors;
- Decide on the issuance of long-term securities;
- Carry out other operations foreseen within the institution's statute as well as issues that are not the responsibility of the Shareholder's Assembly;
- Approve the institution's plans and programs of activities, and general acts, other than acts adopted by the institution's General Meeting of Shareholders;

- Approve the annual account and the financial statements of the institution;
- Approve the exposure to individual entity exceeding 10% of the institution's own funds;
- Approve the acquiring capital parts and purchase of securities higher than 5% of the institution's own funds, other than purchase of securities issued by the National Bank and the Republic of Macedonia;
- Approve the annual report on the institution's operations and submits written opinion thereon to the institution's Meeting of Shareholders;
- Provide written opinion on the annual report of the Internal Audit Department to the General Meeting of Shareholders of the institution; and
- Approve the Rules and Procedures for the operations of the Auditing Committee.

3.4. **Policy Development**

3.4.1. The following describes the more important institutional policies the Board must develop and adopt:

- *Risk Management Policy*[1]. This policy should encompass all risk categories, providing direction to Directors and other risk takers in the institution. The policy should detail the processes used to identify, measure, control, and monitor all major risks the institution takes on. The following are examples of key policies that stem from the overall Risk Management Policy.
- *Credit Portfolio Management Policy.* This policy, should include at a minimum:
  - Clearly defined authorizations for loan approvals;[2]
  - Types of loans that are approved;
  - Parameters for diversification of loans according to types, activities and regions;
  - Limits for loan concentrations;
  - Instructions on loans to employees;
  - Content of loan requests;
  - Loan analysis and criteria for loan approval;
  - Loan administration practices; and
  - Procedures evaluating compliance with laws, regulations and internal loan policies.

  Members of the Board are not expected to be experts in the loan process. Still, they can contribute to the process in which Directors and/or the Credit Committee approve loans. Their knowledge and experience can assist, especially in approving large loans proposed by Directors.
- *Asset Management Policy*. This policy should include directions for the maintenance of an adequate level of liquidity, limits on increases of the institution's assets based on available capital, approved list of investments, limits for off-balance sheet exposure, etc.

---

[1] The titles of policies for individual institutions may be different from those which are used in this text and depends on the way they are defined by the institution.

[2] Loans, for this purpose, includes other forms of credit exposure as regulated by the Law on Institutions.

- *Investment Policy*. This policy should determine the basic types of investments that the institution should carry from the aspect of quality, maturity and marketability.
- *Ethical Standards of Conduct Policy.* Elements that this policy should contain, at a minimum, are:
  - Instructions for approving loans to shareholders, persons with special rights and responsibilities, and employees (financing for employees should be limited and in accordance with market conditions; reports on employee loans should be submitted to the Board; and employee loans should be subject to auditing by the internal and external auditors);
  - Procedures for identifying present and potential conflicts of interest. These procedures should ensure that transactions with related parties, in particular with shareholders, Directors or members of the Board and other related companies, are made on an arms-length basis and are not made on terms contrary to the interest of the institution, its shareholders and depositors;
  - Procedures for dealing with classified information;
  - Procedures for preventing the use of internal information for personal interests;
  - Limitations on the receipt of gifts and other valuables from clients and other persons who do business with the institution; and
  - Procedures for monitoring compliance with this policy, as well as measures to be undertaken in the event of noncompliance.

3.5. Reports and Information to be Submitted to the Supervisory Board

3.5.1. In terms of regularly informing the Board about the institution's operations, a standardized package of reports should be prepared and submitted to Board members. The package should include:

- An agenda;
- Minutes of the previous meetings of the Board and Board Committees;
- A summary by Directors of important activities carried out since the last Board meeting; and
- Basic financial data on the Institution's operation.

3.5.2. The following lists the basic financial information that should be received, at a minimum, by every member of the Board. Besides determining the current financial condition of the institution, adequate financial information should provide the possibility for evaluating trends in financial performance. This means receiving comparative financial reports with sufficient financial and non-financial support information. Board reports should include:

- Balance Sheets, Off-balance Sheets, and Income Statements with comparative data from the same date of previous year, most recent year-end, and budget projections;
- Breakdown by class of loans, identified by management versus categorized by the NBRM;
- Breakdown of matured loans;

- Breakdown of written off claims[3] and recoveries;
- Internal audit reports; and
- Supervision reports issued by the NBRM.

3.5.3. The following lists the basic financial indicators the Board, at a minimum, should understand and monitor:

- Estimation of capital position
- Guaranteed capital/Risk weighted assets
- Own funds/Total assets
- Estimation of assets quality
- Credit exposure in the risk categories C, D and E/Total credit exposure
- Credit exposure in the risk categories C, D and E/Guaranteed capital
- Allocated special reserve for potential losses/Total credit exposure
- Credit exposure in the risk categories C, D and E/Allocated special reserve for potential losses
- Net profit/Average assets (ROAA)
- Net profit/Average capital (ROAE)
- Net interest margin (difference between interest income and interest expense)/Average earning assets
- Non-interest income/Total income
- Operating expenses
- Average assets/Number of employees
- Average salary expense/Number of employees
- Amount of the special reserve (current provision expense should be compared with previous year's and this year's budgeted provision expense)
- Liquid assets/Total assets (Liquid assets are cash, securities maturing in >1 year for which it is estimated that they can be transformed into cash, and sight deposits at other banks.)
- Liquid assets/Volatile deposits (Based on monitoring the trend of certain deposits and the behavior of depositors, management should be able to determine the amount of stable (core) and volatile deposits, regardless of the deposit's contractual maturity date.)
- Net loans/Stable (core) deposits
- Net loans/Total deposits

3.5.4. Issues that should also be discussed during Board meetings at a minimum include:

- Important changes in laws and regulations;
- New policies and procedures;
- Community relations;

[3] Pursuant to supervisory requirements, "claims" include all claims including those recorded in off-balanced sheet accounts (because for two quarters they are classified in risk category "E").

- Introduction of new business products;
- Important changes in the composition of staff;
- Legal proceedings against the institution; and
- Purchase and sale of fixed assets.

3.5.5. At least once a year the following issues should be discussed and decided on:
- Dividends;
- Strategic planning;
- Financial projections and budget;
- Review of employees` salaries and benefits;
- Review and revising, if needed, of all the institution's policies; and
- Annual audit program, both internal and external audit.

4. Risk Management Committee

4.1. Pursuant to the Law on Banks, the institution is obliged to establish a Risk Management Committee, with the primary function of establishing policies and procedures for identifying, measuring, controlling and monitoring the risks inherent in the institution's operations. As mentioned above, one of the main duties of the Board is to provide for safe and sound operations, and be aware of all risks. Directors, the Internal Audit Function (Division), the Audit Committee, and the Risk Management Committee facilitates this understanding through directly reporting to the Board. As a committee of the Board, the Risk Management Committee keeps Board members informed and provides input into Board decisions. To assist in fulfilling the Risk Management Committee's responsibilities, it must work closely with the institution's Risk Management Department,[4] and other departments of the institution responsible for managing and controlling day-to-day risks.

4.2. The Risk Management Committee is actually an extension of the Board, being organized by the Board and consisting of at least three, but not more than nine, members. The members shall be highly qualified, competent and active. The members of the Risk Management Committee shall be elected from among the persons with special rights and responsibilities employed in the institution. One of the members of the institution's Directors shall be a member of the Risk Management Committee. The committee's duties include:

- Establishing and monitoring policies and procedures for effective Credit risk management, including:
  - Establishing and monitoring the implementation of regulations issued by the NBRM pertaining to credit. The NBRM is authorized to issue regulations on the basic elements of a credit policy, treatment of matured loans, loan prolongation procedures, interest capitalization, roll-over loans, the procedure for writing off of loss loans, the classification of credit risk (identification and measure of credit risk), etc.;
  - Analyzing the classification of assets and the adequacy of special reserves. Certain loan clients (i.e. large exposures, insiders, and clients of special interest, etc.) should

[4] The concept of Risk Management is further detailed in other NBRM circular letters.

be analyzed, classified and monitored on an ongoing basis[5]. The Board should receive routine reports on such borrowers to include:
  - Credit exposure and risk category for each client;
  - Newly approved loans and other forms of credit exposure by each client and their determined risk classification;
  - Comparative data of the performances of certain clients (indicating the percentage payment of interest in relation to principle, the trend of credit exposure by each client); and
  - A detailed financial analysis, if necessary, of the credit worthiness and performances of a client with a detailed explanation and justification of the risk classification.
- Recommending measures and activities for the collection of loans that have gained the status of bad and doubtful. Within the institution, a special department may be formed whose primary goal would be the collection of bad and doubtful loans. A report on bad and doubtful loans including their collection efforts should be submitted to the Risk Management Committee in order for it to determine management's effectiveness in this area;
- Approving each client with outstanding credit balances over 10% of guaranty capital;
- Reviewing transactions with, on a quarterly basis, of persons connected with the institution, and submitting a report to the Supervisory Board by 15th of the month following the reporting period; and
- Analyzing early warning signals pertaining to credit risk, such as:
  - Higher percentages of non-performing claims (C, D and E) compared to industry averages;
  - Credit documentation deficiencies;
  - Stagnant or increasing level of doubtful claims;
  - High concentration of loans to groups of enterprises or to certain industries;
  - Reduction in the level of allocated special reserves against the increase in the level of doubtful loans; and
  - Rapid loan growth.

- Establishing and monitoring asset and liability management procedures and policies. This requirement is based on the identification, measurement and control of liquidity risk. In this area, the Risk Management Committee shall establish internal procedures and policies on liquidity risk management based on the recommended best practices established by the NBRM. At a minimum the Risk Management Committee must monitor early warning signals such as:
  - Declines in liquid assets and/or reliable funding sources;
  - Unacceptable negative and/or positive maturity gaps between assets and liabilities;
  - Failure to meet projections; and
  - Aggressive marketing for deposits and/or increased borrowings.

[5] According to NBRM regulations, the classification of credit risk exposure of certain clients is carried out at least quarterly, as well as during the approval of any new type of credit exposure..

- Developing and monitoring the implementation of policies and procedures covering all risks, but at a minimum the seven major risk categories identified by the NBRM. As in the case of credit risk and liquidity risk, the Risk Management Committee should establish appropriate policies and procedures for identifying, monitoring, measuring and controlling all risks. The more important elements that should be included in these policies and procedures are: identifying separate types of risks, defining methods to measure risks, defining internal exposure limits, determining short- and long-term strategies for managing certain types of risks the institution is exposed to, and finding mechanisms for mitigating or reducing risk exposure;
- Monitoring the efficiency of the internal control systems in risk management; and
- Providing recommendations to the Board concerning issues that are under authority of the Risk Management Committee.

5. Auditing Committee and Internal Audit Function

5.1. Overview

5.1.1. The Board is responsible for establishing and implementing a comprehensive and effective audit function. This requires establishing an Auditing Committee of the Board and a separate Internal Audit Function (Division).

5.2. Auditing Committee

5.2.1. The Auditing Committee is a Board committee that oversees the institution's audit function and ensures that Directors develop and comply with sound internal control procedures and practices. The Auditing Committee assists the Board in obtaining insight and fulfilling its responsibility to maintain the quality and integrity of accounting practices and internal controls, by ensuring that the institution receives timely and effective internal and external audits.

5.2.2. *The composition of the Auditing Committee*. In compliance with the Law on Banks, the Shareholders Assembly appoints the members of the Audit Committee. The Auditing Committee consists of at least five members[6]. The majority members in the Auditing Committee shall be elected from among the members of the Board, and the other members shall be independent members. Because of the potential conflict of interest, a member of the Auditing Committee should not be the authorized external auditor or an employee of the Internal Audit Division. At least one member of the Auditing Committee must be a certified (authorized) auditor or accountant. The Auditing Committee has the right to order special audits and engage experts paid by the institution. Meetings of the Auditing Committee may be attended, as needed, by members of the institution's Board, Directors, other managers, representatives of the Internal Audit Division, and/or the external auditor.

5.2.3. *Establishing the Auditing Committee.* The establishment of the Auditing Committee should be regulated in writing, indicating the composition of the Auditing Committee,

[6] At least three members in a savings bank.

its responsibilities, and the manner of reporting to the Board and Shareholders Assembly. This policy should be approved by the Board and subject to periodical revisions. Minutes of Auditing Committee meetings should also be routinely submitted to and reviewed by the Board.

5.2.4. *Responsibilities of the Auditing Committee*. The basic responsibilities of the Auditing Committee are as follows:

- Discuss the financial statements of the institution and make sure that the disclosed financial information on the institution's operations is accurate and transparent as specified by accounting regulations and international accounting standards,
- Establish adequate accounting and internal control procedures that ensure compliance with applicable laws and regulations. The committee will review and make assessment of the internal control systems. The committee should oversee the implementation of international accounting standards within the institution. If there are problems or weaknesses identified by auditors regarding accounting practices, and/or compliance with policies and regulatory requirements, this committee shall ensure that Directors take timely and appropriate corrective measures;
- Establish and oversee the Internal Audit Function (Division). Hires division employees, sets salaries and benefits, conducts employee performance reviews, approves the scope of audits, ensures the division's independence, and receives and reviews internal audit reports;
- Approves the annual audit plan with ratification by the Board. The internal auditor submits to the committee and the Board on a quarterly basis a report commenting on the adequacy of the institution's internal control system, any identified weaknesses, and progress in meeting the audit plan;
- Reviews and provides recommendations on proposals submitted by Auditing Houses for carrying out the external audit of the institution;
- Receives and reviews the official written statement by external auditors concerning potential conflicts of interest, i.e. any relations between the external auditors and the institution, the institution's clients, Board members, Directors and shareholders; and an estimation of the potential influence of these factors on the external auditor's objectivity and independence;
- Proposes an audit company. The Committee will also review and discuss with Directors the external audit's scope and recommended revisions to financial reports; and
- Discusses the reports of the Risk Management Committee.

5.2.5. *Auditing Committee Communication.* The Auditing Committee informs the Board of issues concerning the fulfillment of its responsibilities, important issues stemming from the internal and external auditor functions, issues concerning accounting procedures, the adequacy of internal control systems, and other issues which are relevant for the Board to carry out its responsibilities. The Auditing Committee informs the Shareholders Assembly of its activities at least once a year.

5.3. Internal Audit Function (Department)[7]

5.3.1. *The composition of the Audit Function and the basic principles of internal audit.* The Board, organizes the Internal Audit Function (Department), determines its operations and necessary resources. Within the organizational framework, internal audit personnel can not perform any other function within the institution and at least one of the audit personnel must be a certified (authorized) auditor. The principles upon which the operation of the internal audit is based on are: continuity, expertise, competency of employees, and independence in their activities. The internal auditor reports directly to the Auditing Committee and the Board.

5.3.2. *The responsibilities of the Internal Audit Function..* The basic responsibilities of the internal auditor are as follows:

- Determines the adequacy and efficiency of internal control systems;
- Assesses the adequacy of risk management policies and procedures;
- Assesses the adequacy of management information systems;
- Assesses the accuracy and the authenticity of accounting records and financial reports;
- Tests transactions and internal control procedures;
- Monitors compliance with laws and regulations, the institution’s code of conduct, and evaluates the effectiveness of and compliance with the institutions’ policies and procedures. The Internal Audit Department shall immediately notify the Board and Directors if, during the audit, it identifies: (1) violation of the risk management standards which is likely to deteriorate the institution's liquidity and solvency, and (2) that the Board of Directors violates the institution's regulations, general acts and internal procedures;
- Determines the accuracy, authenticity and timeliness of the submission of regulatory reports to relevant government institutions;
- Conducts various investigations within the institution;
- Assesses the anti-money laundering systems;
- Assesses the services the institution obtains from its supporting service companies; and
- Provides consulting and advice on the development of adequate internal controls, financial reporting, organizational issues, risk management, the introduction of new products, etc.

6. Board of Directors

6.1. According to the Law on Banks, an essential body of the institution is the Board of Directors (which is comprised of at least two, but not more than seven members). The Law introduces the so-called principle of “four eyes”, meaning that Directors’ responsibilities are carried out by at least two persons, equally responsible for the institution’s operations and business practices. The implementation of the “four eyes” principle is a requirement of sound

[7] The definition of internal control and the range of competency of the Internal Auditor (Department or Unit) are listed in more detail in the document A-1 Internal Controls and Audit Function.

internal control systems, which presupposes the rule of mutual evaluation and control. The principle of "four eyes" should not be considered only in conducting Directors' responsibilities, but should be applied throughout the institution.

6.2. The "four eyes" principle does not mean that every decision should be approved by the two members of the Board of Directors. However, the "four eyes" principle must be in place when deciding upon the activities involving high risk operations. Within its policies, the Board should anticipate what situations warrant the employment of the "four eyes" principle. Such activities would include approving credit exposures over a set limit, borrowing over a certain amount from foreign institutions, taking significant market risk or other risk positions, etc. The institution's policies should define the areas of responsibility for each member of the Board of Directors.

6.3. The Law on Banks sets the basic criteria and conditions a person being considered as a Director must meet in order to receive approval by the NBRM. The basic criteria addresses three preconditions: experience, knowledge and reputation, i.e. personal integrity.[8]

6.4. The responsibilities of Directors are summarized as follows:

- Manage the institution's operations;
- Establish adequate organizational and control systems. The basic components of adequate organizational and control systems are:
  - Defining clear lines of responsibilities for Directors and middle management;
  - Maintaining suitable premises including furniture, fixtures and equipment;
  - Providing continuous training of employees;
  - Developing clearly defined reporting lines;
  - Exercising appropriate delegation and division of responsibilities; and
  - Defining information flow.
- Appoint and dismiss other members of the management team according to established policies;
- Represent and act on behalf of the institution. The Board should develop policies determining which member of the Board of Directors represents the institution in certain matters;
- Develop the institution's business policy and development plan, financial plan of the institution, compile a list of net debtors, develop an information security policy for the institution, develop a code of conduct for the institution;
- Executes the decisions of the Shareholders Assembly and the Board, i.e. Directors are responsible for implementation. In this regard, the responsibility of Directors concerning the legality of the institution's operations does not reduce the collective responsibility of the members of the Board.

7. Compliance Function

[8] The detailed criteria to be fulfilled by a potential Executive Management candidate may be found in an Instruction of the Licensing Manual No.1713 from 28.05.2001

7.1. **Introduction**

7.1.1. Compliance risk is defined as the risk of legal or regulatory sanctions, material financial loss, or loss to reputation an institution may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organization standards, and codes of conduct applicable to its banking activities (together, "compliance with laws, rules and standards").

7.1.2. Compliance starts at the top. It will be most effective in a corporate culture that emphasizes standards of honesty and integrity and in which the Supervisory Board and Board of Directors lead by example. It concerns everyone within the institution and should be viewed as an integral part of the institution's business activities.

7.1.3. Compliance with laws, rules and standards generally cover matters such as observing proper standards of market conduct, managing conflicts of interest, treating customers fairly, and ensuring the suitability of customer advice. They typically include specific areas such as the prevention of money laundering and terrorist financing, and may extend to tax laws that are relevant to the structuring of banking products or customer advice. An institution that knowingly participates in transactions intended to be used by customers to avoid regulatory or financial reporting requirements, evade tax liabilities or facilitate illegal conduct will be exposing itself to significant compliance risk.

7.1.4. Compliance laws, rules and standards have various sources, including primary legislation, rules and standards issued by legislators and supervisors, market conventions, codes of practice promoted by industry associations, and internal codes of conduct applicable to the staff members of the institution. For the reasons mentioned above, these are likely to go beyond what is legally binding and embrace broader standards of integrity and ethical conduct.

7.1.5. Compliance should be part of the culture of the organization; it is not just the responsibility of specialist compliance staff. Nevertheless, an institution will be able to manage its compliance risk more effectively if it has a compliance function in place.

7.1.6. An institution should organize its compliance function and set priorities for the management of its compliance risk in a way that is consistent with its own risk management strategy and structures. The officer, i.e. the department staff for compliance, shall perform solely the activities of identification and monitoring the risks arising from non-compliance of the institution's operations with regulations and shall be independent in the performance of activities within their competence. Regardless of how the compliance function is organized within an institution, it should be independent and sufficiently resourced, its responsibilities should be clearly specified, and its activities should be subject to periodic and independent review by the internal audit function.

7.2. **Responsibilities of the Supervisory Board Concerning Compliance**

7.2.1. The institution's Supervisory Board is responsible for overseeing the management of the institution's compliance risk. The Board should approve the institution's

compliance policy, including a formal document establishing a permanent and effective compliance function. At least once a year, the Board or a committee of the Board should assess the extent to which the institution is managing its compliance risk effectively.

7.2.2. As is the case with other categories of risk, the Board is responsible for ensuring that an appropriate policy is in place to manage the institution's compliance risk. The Board should oversee the implementation of the policy, including ensuring that compliance issues are resolved effectively and expeditiously by Directors with the assistance of the compliance function. The Board may, of course, delegate these tasks to an appropriate Board level committee (e.g. Auditing Committee).

7.3. **Responsibilities of the Board of Directors Concerning Compliance**

7.3.1. The institution's Board of Directors shall, depending on the type, scope and complexity of activities performed by the institution, appoint a Compliance Officer or organize a Compliance Department. The institution's Directors are responsible for establishing a permanent and effective compliance function within the institution as part of the institution's compliance policy.

7.3.2. The institution's Directors are responsible for the effective management of the institution's compliance risk.

7.3.3. The institution's Directors are responsible for establishing and communicating a compliance policy, for ensuring that it is observed, and for reporting to the Supervisory Board on the management of the institution's compliance risk.

7.3.4. The institution's Directors are responsible for establishing a written compliance policy that contains the basic principles to be followed by management and staff, and explains the main processes by which compliance risks are to be identified and managed through all levels of the organization. Clarity and transparency may be promoted by making a distinction between general standards for all staff members and rules that only apply to specific groups of staff.

7.3.5. The duty of the Directors to ensure that the compliance policy is observed entails responsibility for ensuring that appropriate remedial or disciplinary action is taken if breaches are identified.

7.3.6. The Directors should, with the assistance of the compliance function:

- At least once a year, identify and assess the main compliance risk issues facing the institution and the plans to manage them. Such plans should address any shortfalls (policy, procedures, implementation or execution) related to how effectively existing compliance risks have been managed, as well as the need for any additional policies or procedures to deal with new compliance risks identified as a result of the annual compliance risk assessment;
- At least once a year, report to the Supervisory Board or a committee of the Board on the institution's management of its compliance risk, in such a manner as to assist

Board members to make an informed judgment on whether the institution is managing its compliance risk effectively; and

- Report promptly to the Supervisory Board or a committee of the Board on any material compliance failures (e.g. failures that may attract a significant risk of legal or regulatory sanctions, material financial loss, or loss to reputation).

7.3.7. The Directors should take the necessary measures to ensure that the institution can rely on a permanent and effective compliance function that is consistent with the following principles.

7.4. Compliance Function Principles

7.4.1. *The institution's compliance function should be independent.* The concept of independence involves four related elements, each of which is considered in more detail below. First, the compliance function should have a formal status within the institution. Second, there should be a group compliance officer or head of compliance with overall responsibility for coordinating the management of the institution's compliance risk. Third, the compliance function staff, and in particular, the head of compliance, should not be placed in a position where there is a possible conflict of interest between their compliance responsibilities and any other responsibilities they may have. Fourth, the compliance function staff should have access to the information and personnel necessary to carry out their responsibilities.

7.4.2. The concept of independence does not mean that the compliance function cannot work closely with management and staff in the various business units. Indeed, a co-operative working relationship between the compliance function and business units should help to identify and manage compliance risks at an early stage. Rather, the various elements described below should be viewed as safeguards to help ensure the effectiveness of the compliance function, notwithstanding the close working relationship between the compliance function and the business units. The way in which the safeguards are implemented will depend to some extent on the specific responsibilities of individual compliance function staff.

7.4.3. *Status*. The compliance function should have a formal status within the institution to give it the appropriate standing, authority and independence. This may be set out in the institution's compliance policy or in any other formal document. The document should be communicated to all staff throughout the institution. The following issues with respect to the compliance function should be addressed in the document:

- Its role and responsibilities;
- Measures to ensure its independence;
- Its relationship with other risk management functions within the institution and with the internal audit function;
- In cases where compliance responsibilities are carried out by staff in different departments, how these responsibilities are to be allocated among the departments;
- Its right to obtain access to information necessary to carry out its responsibilities, and the corresponding duty of the institution's staff to co-operate in supplying this information;

- Its right to conduct investigations of possible breaches of the compliance policy and to appoint outside experts to perform this task, if appropriate;
- Its right to be able freely to express and disclose its findings to Directors, and if necessary, the Supervisory Board or a committee of the Board;
- Its formal reporting obligations to Directors; and
- Its right of direct access to the Supervisory Board or a committee of the Board.

7.4.4. *Access to information and personnel*. The compliance function should have the right on its own initiative to communicate with any staff member and obtain access to any records or files necessary to enable it to carry out its responsibilities. The compliance function should be able to carry out its responsibilities on its own initiative in all departments of the institution in which compliance risk exists. It should have the right to conduct investigations of possible breaches of the compliance policy and to request assistance from specialists within the institution (e.g. legal or internal audit) or engage outside specialists to perform this task if appropriate.

7.4.5. The compliance function should be free to report to the Supervisory Board on any irregularities or possible breaches disclosed by its investigations, without fear of retaliation or disfavor from management or other staff members. The officer, i.e. the manager of the unit, shall, at least once a month, report to the Board of Directors and the Supervisory Board. Although its normal reporting line should be to the Board of Directors, the compliance function should also have the right of direct access to the *Supervisory Board* or to a committee of the Board, bypassing normal reporting lines, when this appears necessary. Further, it may be useful for the Board or a committee of the Board to meet with the head of compliance at least annually, as this will help the Board or Board committee to assess the extent to which the institution is managing its compliance risk effectively.

7.4.6. *Resources*. The institution's compliance function should have the resources to carry out its responsibilities effectively. Resources provided for the compliance function should be both sufficient and appropriate to ensure that compliance risk within the institution is managed effectively. In particular, compliance function staff should have the necessary qualifications, experience and professional and personal qualities to enable them to carry out their specific duties. Compliance function staff should have a sound understanding of laws, rules and standards and their practical impact on the institution's operations. The professional skills of the compliance function staff, especially with respect to keeping up-to-date with developments in laws, rules and standards, should be maintained through regular and systematic education and training.

7.4.7. *Compliance function responsibilities.* The responsibilities of the institution's compliance function should be to assist the Board of Directors in managing effectively the compliance risks faced by the institution. Its specific responsibilities are set out below. If some of these responsibilities are carried out by staff in different departments, the allocation of responsibilities to each department should be clear. Not all compliance responsibilities are necessarily carried out by a "compliance department" or "compliance unit". Compliance responsibilities may be exercised by staff in different

departments. In some institutions, for example, legal and compliance may be separate departments; the legal department may be responsible for advising management on the compliance with laws, rules and standards and for preparing guidance to staff, while the compliance department may be responsible for monitoring compliance with the policies and procedures, and reporting to management. In other institutions, parts of the compliance function may be located within the operations risk group or within a more general risk management group. If there is a division of responsibilities between departments, the allocation of responsibilities to each department should be clear. There should also be appropriate mechanisms for co-operation among each department and with the head of compliance (e.g. with respect to the provision and exchange of relevant advice and information). These mechanisms should be sufficient to ensure that the head of compliance can perform his or her responsibilities effectively.

7.4.8. *Advice*. The compliance function should advise the Board of Directors on compliance with laws, rules and standards, including keeping them informed of developments in the area.

7.4.9. *Guidance and education*. The compliance function should assist the Board of Directors in:

- Educating staff on compliance issues, and acting as a contact point within the institution for compliance queries from staff members; and
- Establishing written guidance to staff on the appropriate implementation of laws, rules and standards through policies and procedures and other documents such as compliance manuals, internal codes of conduct and practice guidelines.

7.4.10. *Identification, measurement and assessment of compliance risk*. The compliance function should, on a pro-active basis, identify, document and assess the compliance risks associated with the institution's business activities, including the development of new products and business practices, the proposed establishment of new types of business or customer relationships, or material changes in the nature of such relationships. If the institution has a new products committee, the compliance function staff should be represented on the committee. The compliance function should also consider ways to measure compliance risk (e.g. by using performance indicators) and use such measurements to enhance compliance risk assessment. Technology can be used as a tool in developing performance indicators by aggregating or filtering data that may be indicative of potential compliance problems (e.g. an increasing number of customer complaints, irregular trading or payments activity, etc). The compliance function should assess the appropriateness of the institution's compliance procedures and guidelines, promptly follow up any identified deficiencies, and where necessary, formulate proposals for amendments.

7.4.11. *Monitoring, testing and reporting*. The compliance function should monitor and test compliance by performing sufficient and representative compliance testing. The results of the compliance testing should be reported up through the compliance function reporting line in accordance with the institution's internal risk management procedures. The head of compliance should report on a regular basis to the Board of Directors on

compliance matters. The reports should refer to the compliance risk assessment that has taken place during the reporting period, including any changes in the compliance risk profile based on relevant measurements such as performance indicators, summarize any identified breaches and/or deficiencies and the corrective measures recommended to address them, and report on corrective measures already taken. The reporting format should be commensurate with the institution's compliance risk profile and activities.

7.4.12. *Statutory responsibilities and liaison.* The compliance function may have specific statutory responsibilities (e.g. fulfilling the role of anti-money laundering officer). It may also liaise with relevant external bodies, including regulators, standard setters and external experts.

7.4.13. *Compliance program.* The responsibilities of the compliance function should be carried out under a compliance program that sets out its planned activities, such as the implementation and review of specific policies and procedures, compliance risk assessment, compliance testing, and educating staff on compliance matters. The compliance program should be risk-based and subject to oversight by the head of compliance to ensure appropriate coverage across businesses and co-ordination among risk management functions.

7.4.14. *Relationship with the Internal Audit.* The scope and breadth of the activities of the compliance function should be subject to periodic review by the internal audit function. Compliance risk should be included in the risk assessment methodology of the internal audit function, and an audit program that covers the adequacy and effectiveness of the institution's compliance function should be established, including testing of controls commensurate with the perceived level of risk. This implies that the compliance function and the audit function should be separate, to ensure that the activities of the compliance function are subject to independent review. It is important, therefore, that there is a clear understanding within the institution as to how risk assessment and testing activities are divided between the two functions, and that this is documented (e.g. in the institution's compliance policy or in a related document such as a protocol). The audit function should, of course, keep the head of compliance informed of any audit findings relating to compliance.