National Bank of the Republic of Macedonia
Supervisory Policy Manual

Title: LeR-1 Legal Risk Management

Date: FINAL

Purpose: To set out the approach which the NBRM will adopt in the supervision of legal risk in licensed institutions and to provide guidance to licensed institutions on the key elements of effective legal risk management.

Issue Type: The references used in preparing this Supervisory Guidance are as follows: Respective provisions from the Banking Law ("Official Gazette of the Republic of Macedonia" No. 63/2000, 37/2002, 51/2003 and 85/2003); Company Law (Official Gazette of the Republic of Macedonia" No. 28/2004 and 84/2005); Security Law (Official Gazette of the Republic of Macedonia" No.95/2005); Payment Operations Law (Official Gazette of the Republic of Macedonia" No. 32/01, 50/01, 52/01, 103/01, 37/02, 61/02, 42/03 and 13/06) and Foreign Exchange Operations Law (Official Gazette of the Republic of Macedonia" No.34/01, 49/01, 103/01,54/02 and 51/03) , as well as, Manual for regulating the operations of the general supervisory issues unit, dated November, 2005.

Supersedes Previous Issue: None

Application: All licensed institutions (*banks and savings houses)*

Contents:

1. Introduction

1.1. Definition of Legal Risk

1.1.1. Legal risk is the current or prospective risk to earnings and capital arising from violations or non-compliance with laws, rules, regulations, agreements, prescribed practices, or ethical standards, as well as from the possibility of dubious interpretation of effective laws or rules. Institutions are exposed to legal risk due to relations with a great number of stakeholders, e.g. customers, counter parties, intermediaries, etc., as well as regulators, tax authorities, local authorities and other authorized agencies.

1.1.2. Legal risk arises from the necessity of the institution to conduct its transactions in conformity with the business and contractual legal principles applicable in each of the jurisdictions where the institution conducts its business. As well as, when there is a possibility that the institution's failure to meet legal requirements may result in unenforceable contracts, litigation, or other adverse consequences. Legal risk can lead to fines and penalties, payment of damages, deteriorating position in the market, reduced expansion potential, and lack of contract enforceability.

1.1.3. Legal risk can also lead to a diminished reputation, also known as Reputation risk, arising from an adverse perception of the image of the institution by customers, counter parties, shareholders, or regulators. This affects the institution's ability to establish new relationships or products, or service existing relationships. This risk may expose the institution to administrative, civil and criminal liability, financial loss or a decline in its customer base.

1.1.4. Legal risk is difficult to measure, but it can be defined, understood and controlled within the institution's capacity and its readiness to confront non-legal performance. Legal risk can occur whether deliberate or unintentional. Therefore, supervisors must communicate with the institution's senior management and encourage them to mitigate or eliminate legal risk.

1.1.5. Appropriate action for the institution to take would include: reducing exposures of sources of legal risk, an appropriate legal risk management process and strengthening the compliance function in the institution.

1.2. Background

1.2.1. The purpose of this supervisory guidance is to provide an integrated review of all aspects related to legal risk management, including reputation risk management, as well as to provide guidelines for effective implementation of the legal risk management process in the overall process of the institution's risk management. The provisions of the Banking Law and other laws and regulations, the recommendations of the Basle Committee for Banking Supervision, as well as the experience and the practice of foreign supervisory bodies underlie the preparation of this document.

1.2.2. The institution should identify sources of legal risk. For instance, common sources of legal risk are:

- Violations or noncompliance with laws and regulations and prescribed standards;

- Lack of or inadequate compliance with contractual obligations and other legal documentation;
- Inadequate identification of rights and responsibilities between the institution and its customers;
- Complaints by customers and other counterparties;
- Harming the interests of third parties;
- Litigation procedures, potential exposure (including cost of litigation) and nature of pending or threatened litigation;
- Involvement in money laundering, insider trading, violation of taxation rules, forgery and damage from computer hacking by the institution, its intermediaries or its customers; and/or
- Limited knowledge and postponed response by management to implement legal and reputation risk management.

1.2.3. Legal risk is particularly concerned with the lack of contract enforceability. Contracts without protective clauses for the institution and that contain unenforceable provisions; can result in significant losses to the institution. The institution should evaluate the enforceability of its agreements before individual transactions are completed. Clear documentation is an essential element of enforceability; poor or inadequate documentation can expose institutions to risks such as:

- Unintentionally agreeing to a standard of performance that cannot be provided;
- Questions of authority that limits the institution's ability to enforce performance by the counterparty;
- Counterparty does not have sufficient authority to enter into transaction; and/or
- Selection of a distant or hostile jurisdiction that makes enforcement difficult.

1.2.4. The institution should follow several steps in managing legal risk. The institution should define a framework for legal risk management (roles and responsibilities, polices and procedures, definition and objectives), assess and measure legal risk, as well as report and control legal risk.

1.2.5. Legal risk should be considered as part of and/or in relation with other risks such as: operational risk, liquidity risk, credit risk, and strategic risk.

1.2.6. The institution should adopt contingency plans for the restoration of its activities in cases such as default of third parties that are significant to the institution and/or diminishes its public reputation.

2. Requirements for Effective Legal Risk Management

2.1. Elements of an Effective Risk Management System (ERMS)

2.1.1. The institution should establish and maintain a legal risk management system. An effective ERMS requires:

- Designing and adopting legal risk management policies and procedures;
- Establishing a proper organizational structure, including strengthening the institution's legal/compliance function;
- Establishing comprehensive internal controls and an effective audit function; and

- Developing an adequate legal risk management process (risk identification, assessment, measurement, monitoring and control).

2.1.2. Each institution should have an ERMS compatible to its size, nature, and the complexity of its activities and adaptable to changes in the Macedonian legislation.

2.2. **Legal Risk Management Policy (LRMP)**

2.2.1. A Legal Risk Management Policy (LRMP) should be part of the overall risk management policy of the institution, and should precisely determine all important processes and procedures in minimizing the institution's legal risk exposure. The LRMP should be clearly formulated and in writing. The policy must contain, at least the following[1]:

- Definition of legal risk;
- Objectives of legal risk management;
- Procedures for identifying, assessing, monitoring, controlling and managing legal risk;
- Well defined authorities, responsibilities and information flows for legal risk management at all management levels; and
- Clear statement of the institution's accepted tolerance for legal risk exposure.

2.2.2. Procedures for legal risk should contain at a minimum:

- Definition of the required legal documents establishing the collateral on loans for clients. These also include verification, by the institution's legal expert, of the legitimacy of the collateral on the basis of the available documentation.

- Definition of standard procedures for foreclosures. These procedures should define: the responsible person for providing the proof of ownership of foreclosed property on behalf of the institution, the manner of realizing the collateral, the initial price, and the manner of selling non-movable assets.

- Standardized contracts for similar institution's products, clients, and other services with third parties. The terms or conditions of a contract (price, due date for fulfilling contract requirements, protective clause for the institution, etc.) should be confirmed by the institution's legal expert. Special attention should be paid to the procedures for changing the terms of a signed contract. The institution's legal expert should also confirm annexes to any contract.

- Legal due diligence of the institution's major clients and counterparties, vendors and outsourcing companies.

- Documentation standards for all initiated court proceedings against or on behalf of the institution. Permanent and accurate information and documents of the institution's effectiveness in court proceedings is also needed. Institution's legal experts should keep a list of all court proceedings with their opinion on the possible result of the case

[1] Provision of the Czech National Bank No. 2 on the Internal control system of a bank, February 2004

(whether in their opinion the court judgment will be in the institution's favor or not), as well as, a list of court cases that in the name of the institution are lead by outside attorneys. In addition, the institution should separately retain data describing the types of claims for which the institution has usually initiated litigation and in which cases the institution was sued.

- Definition of the major mitigating actions to legal risk (e.g., through reviewing contract terms by experienced lawyers, restricted dealings to reputable counterparts, placing limits on exposure to legal interpretations, etc.).

- Clear documentation standards for the institution's shareholders. Accurate and current information about: shareholders book and registration, their declared affiliated entities in accordance with NBRM legal requirements, verifications of the changes in shareholders, and authorized shareholder representatives. If the shareholder goes into a bankruptcy procedure, the institution is obliged to maintain information on the bankruptcy proceeding, the court decision, or other relevant documentation.

- Documentation standards for all decisions of the governor of the NBRM issued against the institution, all-prior approved licenses and written communications among the NBRM and the institution.

- Documentation standards for all necessary information and data for the persons with special rights and responsibilities, that verifies that there are no legal impediments for these persons to perform their function, stipulated under the Banking Law.

- Registration requirements for all information and documentation supporting banking activities by another entity for the institution on a contractual basis (outsourcing).

- Procedures for safeguarding of original legal documents.

- Regular compliance checks.

2.3. The Role of Management Bodies

2.3.1. The prerequisites for effective implementation of the legal risk management policy is the function of active Supervisory Board and Board of Directors oversight, and the establishment of a proper organizational structure that can ensure the fulfilment of the legal risk management policy. As well as, establishing proper communication between all bodies and persons involved in legal risk management.

2.3.2. *Supervisory Board*

2.3.2.1. The Supervisory Board should be aware of the major aspects of the institution's legal risk as a separate risk category that should be managed. The Board is responsible to define the legal risk management system and ensure that the system is aligned with overall business activities. The Board should provide the Board of Directors with clear guidelines and directions regarding the principles defined in the legal risk management policy and approve the corresponding policies and procedures developed by Directors. The Board is responsible for establishing a management structure capable of implementing the institution's legal risk management process. The Board should periodically review the institution's legal risk management policy to ensure proper guidance is provided for effectively managing the institution's legal risk.

2.3.2.2. The Board should ensure that the institution's legal risk management system is subject to implementation by the Board of Directors and a qualified compliance officer/staff, and controlled by an effective and comprehensive internal audit.

2.3.3. ***Board of Directors***

2.3.3.1. The Board of Directors is responsible for running the institution on a day-to-day basis, to manage and monitor the institution's overall risk environment. Directors are responsible for the effective management of the institution's legal risk, as well as:

- Implementing the legal risk management system approved by the Board;
- Establishing a written compliance policy, as a part of the legal risk policy or as separate internal document;
- Establishing an effective organizational structure for legal risk management, and be in regular contact with employees that are directly responsible for conducting legal risk management (institution's compliance staff and lawyers);
- Ensuring that all employees are working in order to protect the institution's reputation;
- Ensuring that sufficient human and technical resources are devoted for legal risk management; and
- Ensuring ongoing compliance training that covers legal requirements for all business lines, particularly when entering new markets or offering new products.

2.3.3.2. A written compliance policy should explain the main processes by which compliance risk is to be identified and managed through all levels of the institution's organizational structure. This document should also define the compliance function as an independent function, with specific roles and responsibilities of the compliance staff, and detailing the compliance officer's communication methods with the management and staff in the various business units.

2.3.4. ***Risk Management Committee***

2.3.4.1. The Risk Management Committee, as a specialized body of the Board established to monitor and assess the level of the institution's risk exposure, and is responsible for:

- Developing procedures and practices for implementing the legal risk policy;
- Following the NBRM rules and procedures concerning legal risk management;
- Assessing sources of legal risk;
- Establishing cost and benefit analysis for the effects of legal risk management;
- Establishing adequate reporting systems that will ensure timely monitoring of legal risk exposures and elimination of any possible legal and reputation problems;
- Providing the necessary conditions for the implementation of the Legal Risk Management process; and

- Establishing an action plan that will ensure an institution's readiness to respond to compliance, legal or regulatory events that could significantly impact the institution reputation.

2.3.5. ***Internal Audit Department and Internal Controls***

2.3.5.1. Institutions should have proper internal control systems that integrate legal risk management into its overall risk management process.

2.3.5.2. The audit of legal risk management should be incorporated into the annual plan of the Internal Audit Department.

2.3.5.3. The Internal Audit Department should, within its scope of operations, cover the following aspects of legal risk management:

- Verifying that legal risk management policies and procedures have been implemented effectively across the institution;
- Assessing the effectiveness of controls for mitigating fraud and risks to reputation;
- Determining that senior management takes appropriate corrective action when compliance failures are identified;
- Ensuring that the scope and frequency of the audit plan/program is appropriate to the risk exposures;
- Monitoring legal risk profiles on an on-going basis; and
- Analyzing the timeliness and accuracy of legal risk reports to senior management.

2.4. **Strengthening the Institution's Legal/Compliance Function**

2.4.1. The compliance staff is responsible for identifying and monitoring the institution's legal risk indicators, to advise the institution's staff on new laws, regulations and standards, and being responsible for monitoring and managing reputation risk arising from a lack of the institution's compliance with laws and regulations.

2.4.2. Especially, the compliance staff should provide opinions on compliance issues as new products are developed or as additional financial banking activities are promoted by the institution. Before the institution presents new products or services, the compliance staff is obliged to give an opinion as to how much the new products or services will expose the institution to legal and reputation risks.

2.4.3. The size of the institution and the complexity of its business activities dictate the scope of the compliance function and staffing requirements (number and competencies) of a compliance function unit. Not all compliance responsibilities are necessarily carried out by a compliance unit. Compliance responsibilities may be exercised by staff in different departments, such as, legal department, anti-money laundering department, department for protection of customers and client's complaints, or some or all compliance responsibilities may be conducted by the compliance unit/department.

2.4.4. Each institution should have a position - head of compliance - that will be responsibility to coordinate the identification and management of the institution's compliance risk. The head of compliance should be able to carry out his/her responsibilities on his/her own initiative in all departments of the institution in which compliance risk exists.

2.4.5. Regardless of how the compliance function[2] is organized within the institution, it should be independent, with sufficient resources and clearly specified activities. The compliance staff, especially the head of compliance, should not be in a position where there may arise a conflict of interest between their compliance responsibilities and any other responsibilities they may have.

2.4.6. The head of the compliance function should submit monthly reports to the Board of Directors and the Risk Management Committee.

3. Legal Risk Management Process

3.1. Risk Identification and Assessment[3]

3.1.1. In order to understand its legal risk profile an institution should identify the sources of legal risk that it is exposed to and assess its vulnerability to these risks. If a new legal risk is not recognized, the institution's legal experts may never thoroughly review the existing contracts. Thus, the institution should identify and assess the legal risk inherent in all existing or new, rules, procedures, internal processes, activities, contracts and court cases.

3.1.2. Having identified the potential sources of legal risk, the institution needs to define the appropriate approach to assessing each identified source of risk. There are various tools used for identifying and assessing legal risk, such as:

- Self-Assessment - An institution assesses its operations and activities against a list of potential risk vulnerabilities. This process is internally driven and often incorporates checklists to identify the strengths and weaknesses of the legal risk environment.
- Risk Indicators - Risk indicators are statistics or matrices that can provide insight into an institution's risk position. These indicators tend to be reviewed on a periodic basis (such as monthly, quarterly, etc.) to alert the institution to changes that may be indicative of risk concerns. Such indicators may include the volume and/or frequency of law violations, frequency of complains, number of initiated litigation procedures, payments of damages, fines and court expenses, unfavorable court verdicts or number of finalized court cases on a periodical basis, and frequency of actual or suspected fraud or money laundering activities. These indicators should provide good incentives, tying risk to capital to desirable improvement in the compliance function.
- Risk Mapping - In this process, various departments or units are outlined by risk types (for example credit unit/department can be outlined by the risk of the lack of contract enforcement or dubious interpretation of the agreements). This exercise can disclose areas of weakness and help to identify priorities for management action.

3.2. Legal Risk Measurement

3.2.1. Evaluation Factors

[2] Basel Committee on Banking Supervision-Compliance and the compliance function in banks, April 2005 , Bank for International Settlements
[3] Hong Kong Monetary Authority-Supervisory Policy Manual, OR-1, V.1-28.11.05

3.2.1.1. It is difficult to quantify legal risk, because it is hard to predict how lawmakers will interpret the law and how courts will solve the cases. Consequently, it is much easier for institutions to ignore the usefulness of quantitative limits to control exposure. Quantitative limits are used to control the size of risk which can be determined based on the degree of economic benefit relative to the apparent degree of legal uncertainty.

3.2.1.2. One of the major legal risk concerns is the lack of contract enforceability, along with the resulting amount of litigation costs and potential market or public perception of the institution's reputation. Legal risk is also concerned with the impact of noncompliance with laws and regulations, fraud and operational failures.

3.2.2. **Contract Enforceability**

3.2.2.1. Unenforceable terms or conditions of a contract (due to legal defects) can prove a more serious problem than the underlying credit risk (when the counterparty does not have the financial capacity to perform on a contract). There is a constant need to limit risk exposure due to contract interpretation. Therefore, the institution must mitigate this risk by having qualified lawyers review contract terms, and by using standardized contractual language as much as possible.

3.2.3. **Litigation Management**[4]

3.2.3.1. Litigation is generally recognized as being costly, unpredictable and inefficient. There are direct and indirect litigation costs. Costs for attorneys, for experts, support staff, court expenses, etc. are direct litigation costs, and they can be easily calculated. There are also significant indirect litigation costs, such as:

- Employees with important responsibilities are forced to spend time searching for documents, preparing for and participate in meetings with lawyers, testifying at trial, etc.;
- Litigation and the threat of litigation can also result in more than the usual conservative risk avoidance toward business conduct; and
- There is always the damage that litigation causes to the relationship between the litigants (the plaintiff and the defendant).

3.2.3.2. When considering any litigation, the plaintiff calculates (maybe inaccurately) what the likely gain will be from the litigation versus the direct and indirect costs of declaring and pursuing its claims. Institutions should be able to calculate the point at which it makes economic sense to settle rather than litigate, similar to any other economic decision. For example, attorneys before the start of the litigation process, calculate the case value by forming opinions about the likelihood for success on each claim, estimate the range of potential damages that a court/jury might award for each, and then combine all these probabilities to arrive at a case value to make trial and settlement decisions.

[4] The Role of Risk Analysis in Dispute and Litigation Management, 2004 American Bar Association

3.2.3.3. The institution should be interested to litigate in a cost-effective manner. The institution should determinate how much risk the institution's litigation and other legal matters pose its financial condition, and identify weaknesses and corrective action necessary to minimize these risks.

3.2.4. **Compliance Risk Measurement**

3.2.4.1. The compliance function should also consider ways to measure compliance risk by using performance indicators, such as the increasing number of: customer complaints, corrective measures taken against the institution, or litigation procedures as a result of noncompliance with laws and regulations. All these may indicate potential compliance problems.

3.2.4.2. Compliance risk can be also measure by regular legal reviews on different institution’s products and services, and their relevant documentation in order to ensure that all contracts are in conformity with laws and regulations. This review may take place on each transaction individually or may cover the legal adequacy of standardized documentation and procedures.

3.2.5. **Institution's Reputation**

3.2.5.1. The biggest threats to reputation are seen to be a failure to comply with legal obligations, failure to deliver minimum standards of service and product quality to its customers, as well as, a breakdown in the institution's operational practices (failure in technology or communications).

3.2.5.2. Institutions need to be sure that contract provisions are not only legally enforceable, but also that the process of enforcing their legal rights will not damage their business reputation. All transactions need to be reviewed by management from the viewpoint of whether the transaction is one that the client fully understands and can reasonably be interpreted as a sensible action for the client to take.

3.2.5.3. From a reputation risk management perspective the institution should evaluate all actions that affects relationship with customers (branch opening or closing, changes in interest rate policy or banking hours), as those actions will likely to generate public reaction.

3.2.5.4. It may be difficult to measure the reputation risk exposure in exact amount of money, but it can be classified into various levels of severity and probability. The institution should at least, attempt to rate threats against the institution’s reputation on a simple numerical scale and after that use the results as a guide to the allocation of institution resources. Consequently, management should know what are the institution’s capabilities in the following areas: communicating with customers, monitoring threats to reputation before the institution presents new products or services, and ensuring ethical practices throughout the supply chain.

3.2.5.5. The institution should conduct surveys on perceptions of customers and the influence of the media on the institution's reputation at least once a year.

3.3. **Risk Monitoring and Control**

3.3.1. Institutions are responsible for monitoring their legal risk profiles on an on-going basis. In monitoring their legal risk, institutions are responsible for reviewing defined legal risk indicators in order to provide management with early warning. Monitoring should be an integrated part of an institution's activities. The results of these monitoring activities should be included in regular management and Board reports.

3.3.2. Institutions should have processes and procedures in place to control legal risk. For all sources of legal risk that have been identified, the institution should decide whether to use appropriate procedures to control legal and reputation risks or bear the risk. For the risk that can not be controlled, the institution should decide whether to accept the risk, reduce the level of business activity involved or withdraw from this activity completely. There should be a constant review of the institution’s progress towards meeting legal objectives, and checking for compliance with policies and procedures and defined duties and responsibilities.

4. **Supervisory Approach in Assessing Legal Risk**

4.1. Supervisors determine the adequacy and effectiveness of an institution’s legal risk management process and the level of legal and reputation risk exposure. Supervisors, through close communication with the head of the legal department and the head of compliance, review the work of the institution’s compliance function. Supervisors begin their control by identifying an institution’s major sources of legal risk exposure, areas of potential or high legal and reputation risk and areas not recently reviewed. (Review the internal audit work first and determine scope of examination).

4.2. Supervisors observe and review appropriate example of contracts among the institution and its clients, the institution’s litigation procedures, complaints by customers, outsourcing activities, compliance problems, shareholders activism, senior management incentives, institution’s code of conducts, institution’s employment practices, areas of potential conflict of interest, affiliated persons according the NBRM regulations, etc. They also analyze the legal and reputation risk tolerances of the Board and Directors to determine if they follow effective legal risk measurement, monitoring, and control practices and procedures.

4.3. When reviewing an institution’s legal risk management system, and legal and reputation risk exposures, supervisors consider the following:

- Adequacy and effectiveness of legal risk management system;
- Adequacy and effectiveness of LRMP;
- Adequacy and effectiveness of Board and Directors’ oversight;
- Effectiveness of an institution’s compliance function;
- Adequacy of internal reviews and audits of the legal risk management process;
- Knowledge of personnel and their ability to identify and manage sources of legal risk;
- Level of risk that the institution’s litigation, compliance and reputation problems and other legal matters, pose to the institution’s financial condition;
- Level of threatened or pending litigation or claims against the institution and their potential effect on the institution’s capital and earnings;
- Adequacy of internal measurement, monitoring and control of legal risk; and

- Management's efforts to define threats against institution's reputation.

4.4. Supervisors document all working papers that support conclusions on the institution's legal risk management assessment. Especially documented are personal data and qualifications of the institution's staff with special rights and responsibilities and all evidence that support the institution's noncompliance with laws and regulations.

5. Other Issues

5.1. *Registry of Legal Original Documents*

5.1.1. The institution should establish a database of its legal documents. This database should contain at least: type of legal documents (internal acts, contracts, memorandum of understanding, etc.), period of document validation, and responsible department/unit for document enforcement.

5.2. *Resources*

5.2.1. The institution should have the resources to carry out its legal risk management system effectively. In particular, the compliance function staff should have the necessary qualifications, experience, and professional and personal qualities in order to carry out their duties. The compliance function staff should have a sound understanding of compliance laws, rules, and standards particularly important for the institutions operations.

5.2.2. The Head of compliance is a person with special rights and responsibilities in the institution.

5.2.3. The institution should organize permanent and systematic education and training for their legal staff.

5.3. *Corporate Governance Practices*

5.3.1. A successful legal risk management system is closely connected with the quality of an institution's corporate governance practices. Effective organizational structure and sound relationships between institution's management, the Board, and shareholders are important for maintaining a positive reputation. Good corporate governance should introduce more accountability, trust, and confidence in the institution's management bodies and other stakeholders, resulting in a higher probability that the institution will perform its activities according laws and regulations.

5.3.2. Each institution needs to implement legal risk management system as a means of self-governance/self supervision.

Appendix A: Correlation of Legal Risk with Other Risks

A1. Legal risk can be classified in different ways. The institution can suffer losses on legal contracts in one of three ways:

- Obligations detailed in contracts may be performed exactly as expected, but changes in economic conditions might make the sum of all contractual actions an undesired outcome. This is a form of market risk.
- The institution may be misled about what the contractual actions are or the consequences of these actions. This is operational risk.
- The other party of the contract may fail to perform as specified. This is credit risk.

A2. According to some scholars, operational risk always includes legal risk. They argue that legal risk together, or as a part of operational risk, has become an increasing issue over the last few years as institutions:

- Initiate internal reorganization;
- Adopt techniques that are developed to mitigate other forms of risks (e.g. collateralization, netting and asset securitization, etc.); or
- Outsource some of their major functions.

A3. Legal risk can be seen as a strategic risk, affecting a strategic decision by a company to move into a particular area of business.

A4. Reputation risk as a component of legal risk, cannot be managed in isolation from other forms of risks, since all risk can have an impact on reputation, which in turn can impact the institution's brand, earnings and capital.