National Bank of the Republic of Macedonia
Supervisory Policy Manual

Title: ITR-1 Information Technology Risk

Date: FINAL

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

Issue Type: Supervisory Guidance

Supersedes Previous Issue: None

Application: All licensed institutions and supervision personnel

Contents:

1. Introduction
2. Supervisory Board and Board of Directors Oversight
3. Effective Risk Management Process
4. Organizational Structures for Managing Information Technology Risk
5. Supervisory Review of Information Technology Risk
   - 5.1. Overview
   - 5.2. Risk Assessment
   - 5.3. Implementation of Administrative, Technical and Physical Controls
   - 5.4. Information Technology Security
   - 5.5. Management Information System (MIS)
   - 5.6. Planning and Project Management
   - 5.7. Development
   - 5.8. Large-Scale Systems
   - 5.9. Acquisitions
   - 5.10. Maintenance
   - 5.11. Patch Management
   - 5.12. E-banking
   - 5.13. Retail Banking

1. Introduction

1.1. *Information Technology risk* is the current or prospective risk to earnings and capital arising from inadequate information technology and processing in terms of manageability, exclusivity, integrity, controllability, continuity and data security. The NBRM seeks to establish solid standards for the information system security. The application of such standards will ensure higher security of the information stored in the information system and higher degree of data integrity in different types of processing. The information systems of licensed institutions need to be available and accessible to the staff and the clients for smooth performance of banking operations, as well as to management for making prudential decisions, within their business needs and authorizations.

1.2. Historically, the information technology risk environment for institutions in Macedonia has been fairly low. However, institutions become more exposed to information technology risk due to greater reliance on information technology for providing traditional banking services and introducing new and more complex financial products.

1.3. Information is one of a financial institution's most important assets. Protection of information assets is necessary to establish and maintain trust between the financial institution and its customers. Timely and reliable information is necessary to process transactions and support financial institution and customer decisions. A financial institution's earnings and capital can be adversely affected if information becomes known to unauthorized parties, is altered, or is not available when needed.

1.4. A financial institution establishes and maintains truly effective information security when it continuously integrates processes, people, and technology to mitigate risk in accordance with risk assessment and acceptable risk tolerance levels. Financial institutions protect their information by instituting a security process that *identifies* risks, forms a strategy to *manage* the risks, *implements* the strategy, *tests* the implementation, and *monitors* the environment to control the risks.

1.5. Management of information technology in financial institutions is critical to the performance and financial success of an institution. Sound management of technology involves more than containing costs and controlling operational risks. An institution capable of aligning its information technology infrastructure to support its business strategy adds value to its organization and positions itself for sustained success. The Supervisory Board (Board) and Board of Directors (Directors) should understand and take responsibility for information technology management as a critical component of their overall corporate governance efforts.

1.6. Due to the reliance on technology, effective information technology management practices play an integral role in achieving many goals related to corporate governance. The ability to manage technology effectively in isolation no longer exists. Institutions should integrate information technology management into the strategic planning function of each line of business within the institution.

1.7. An institution's Boards and Directors should establish information technology oversight by ensuring:

- Strong involvement and awareness by the Board of information technology activities;
- Development and enforcement of sound policies and procedures;
- Implementation and maintenance of an effective risk management process;
- Competent and sufficient staff to perform their mission;
- Effective Management Information Systems (MIS); and
- Sound project management structure.

2. Supervisory Board and Board of Directors Oversight

2.1. Effective Board and Directors oversight of the institution's information technology risk activities is the cornerstone of an effective risk management process. It is the responsibility of the Board and Directors to understand the nature and level of information technology risk being taken by the institution and how that risk fits within the overall business strategies of the institution and the mechanisms used to manage that risk. Effective risk management requires an informed Board, capable management, and appropriate staffing.

2.2. The Board must:

- Establish and guide the institution's strategic direction and tolerance for information technology risk and identify the senior managers who have the authority and responsibility for managing this risk.
- Monitor the institution's performance and overall information technology risk profile, ensuring that the level of information technology risk is maintained at prudent levels.
- Ensure that senior managers implement sound fundamental principles that facilitate the identification, measurement, monitoring, and control of information technology risk.
- Ensure that adequate resources are devoted to information technology risk management.
- Hold managers responsible the implementation and promotion of the institution's information system security policy.
- Develop the information system security policy and review/approve at least once a year.
- Provide guidelines and recommendations to Directors and other senior managers on maintaining a secure information system by:
    - Requiring the establishment of a central surveillance and coordination process;
    - Defining appropriate roles and responsibilities;

- Requiring a suitable method of risk measurement;
- Approving appropriate monitoring and testing techniques;
- Requiring acceptable reporting methodology; and
- Establishing a system for the effective identification, monitoring and control of all risks.

2.3. Directors are responsible for ensuring that information technology risk is managed for both the long range and day-to-day. In managing the institution's activities, senior managers should:

- Develop and implement procedures and practices that translate the Board's goals, objectives, and risk tolerances into operating standards that are well understood by all personnel and that are consistent with the Board's intent.
- Ensure adherence to the lines of authority and responsibility that the Board has established for measuring, managing, and reporting information technology risk exposures.
- Oversee the implementation and maintenance of management information and other systems that identify, measure, monitor, and control information technology risk.
- Establish effective internal controls (including audit) over the information technology risk management process.

2.4. Audit, either internal and/or external, should provide an independent assessment of the information technology risk management framework. Institutions should have in place adequate audit coverage to verify that information technology risk management policies and procedures have been implemented effectively across the institution. The Board (either directly or indirectly through its audit committee) should ensure that the scope and frequency of the audit program is appropriate to the risk exposure inherent in the institution's activities. Any operational issues identified and reported in the audit process should be addressed by Directors in a timely and effective manner, or raised to the attention of the Board, as appropriate.

3. Effective Risk Management Process

3.1. Effective control of information technology risk requires a comprehensive risk management process that ensures the timely identification, measurement, monitoring, and control of risk. The formality of this process may vary, depending on the size and complexity of the institution. Regardless of the mechanism used, an institution's information technology risk management procedures or processes should establish the following:

3.2. *Responsibility and authority* for identifying the potential information technology risk arising from new or existing products or activities; establishing and maintaining an information technology risk measurement system; formulating and executing strategies; and authorizing policy exceptions.

3.3. *An information technology risk measurement system that is* able to identify and quantify the major sources of information technology risk in a timely manner.

3.4. *A system for monitoring and reporting risk exposures.* Directors and the Board, or a committee thereof, should receive reports on the institution's information technology risk profile at least once a year, but more frequently if the character and level of risk requires it. These reports should allow senior managers and the Board to evaluate the amount of information technology risk being taken, compliance with established risk limits, and whether management's strategies are appropriate in light of the Board's expressed risk tolerance.

3.5. *Risk limits and controls* on the nature and amount of information technology risk that can be taken. When determining risk exposure limits, Directors should consider the nature of the institution's strategies and activities, its past performance, the level of earnings and capital available to absorb potential losses, and the Board's tolerance for risk.

3.6. *Internal control procedures (including audit).* The oversight of Directors and the Board is critical to the internal control process. In addition to establishing clear lines of authority, responsibilities, and risk limits, managers and the Board should ensure that adequate resources are provided to support risk monitoring, audit, and control functions. The persons or units responsible for risk monitoring and control functions should be separate from the persons or units that create risk exposures.

4. Organizational Structures for Managing Information Technology Risk

4.1. For the purpose of efficiently monitoring an institution's information technology activities, most frequently a special committee, often called the Information Technology Steering Committee (Committee), is established. The Committee's goal is to assist the Board in the decision-making process as it pertains to information technology issues. The Committee should be composed of least one Director and representatives of the institution's organizational units. Members of the Committee can also be external specialists. This Committee should submit reports to the Board on the status of the institution's information technology and what issues are of concern. The Committee should provide effective planning and monitoring of the capacities and performances of the information technology system; and prepare adequate information for the Board in order to facilitate the decision-making process. Also, the Committee may:

- Monitor the development of information technology strategic plans;
- Approve and monitor the engagement of information technology outsourcing activities;
- Approve and monitor main projects, budgets, priorities, standards, procedures and performances of the information technology area; and
- Coordinate the priorities between the information technology area and other departments.

4.2. Directors or the Board should appoint one or more information security officer (ISO). The ISO is responsible for and oversees the security of information systems. The ISO should have a good understand of information systems and information technology risks, as well as the institution's organizational layout in order to be able to perform all expected tasks. The Board and Directors should develop and implement an information security policy for the entire institution with clear differentiation of the responsibilities and appropriate duties of certain persons pertaining to information system security. The responsibilities concerning the information system security should be segregated from the information technology organizational unit and assigned to different sectors, depending on the size, complexity, and type of operations the institution performs.

5. Supervisory Review of Information Technology Risk Management

5.1. Overview

5.1.1. Supervisors determine the adequacy and effectiveness of an institution's information technology risk management process, the level and trend of risk exposure, and the adequacy of risk mitigation due to the risk management process. The remainder of this guidance discusses the various areas that supervisors will address during their review.

5.1.2. Supervisors determine, normally through discuss with management, the major sources of information technology risk exposure and evaluate whether the institution's measurement systems provide a sufficient basis for identifying and quantifying the major sources of threat exposure to the organization. They also analyze the integrity and effectiveness of information risk control and management processes to ensure that practices comply with the stated objectives and risk tolerances of the Board and Directors.

5.1.3. In forming conclusions about the safety and soundness of the institution's information technology risk management and exposures, supervisors consider:

- The complexity and level of risk posed by the current information technology system;
- The adequacy and effectiveness of Board and Directors oversight;
- Management's knowledge and ability to identify and manage sources of information technology risk;
- The adequacy of internal measurement, monitoring, and management information systems;
- The adequacy and effectiveness of risk limits and planned controls;
- The adequacy of internal reviews and audits of the information technology risk management process; and

- The adequacy and effectiveness of risk management practices and strategies as evidenced in past and projected performance.

5.2. Risk Assessment

5.2.1. Institutions should maintain a risk assessment process that drives technology selection and controls implementation. The risk assessment process should incorporate specific assessments conducted for functional responsibilities such as security, business continuity, and vendor management. Risk assessment involves four critical steps:

- Ongoing data collection from new initiatives or monitoring of existing activities;
- Risk analysis regarding the potential impact of the risks;
- Prioritization of controls and mitigating actions; and
- Ongoing monitoring of risk mitigation activities.

5.2.2. Directors should ensure satisfactory monitoring and reporting of information technology activities and risk. These practices should include:

- Reviewing routinely business plan goals and strategies relative to information technology;
- Developing benchmarks for reviewing performance;
- Establishing and reviewing service level agreements with critical vendors and third parties; and
- Implementing a quality control or quality assurance program to monitor and test products and practices.

5.3. Implementation of Administrative, Technical and Physical Controls

5.3.1. Directors should implement satisfactory control practices as part of the overall information technology risk mitigation strategy. These practices should include:

- Establishing internal controls that effectively mitigate the identified risks associated with information technology processes such as system and security administration, systems development, information technology operations, outsourced functions, vendor management, and other information technology risk areas;
- Ensuring controls over MIS to provide management with accurate and timely information to make informed decisions;
- Adopting and enforcing information technology policies and standards;
- Establishing standards for hiring, changing duties, and terminating information technology personnel, including internal staff, consultants, temporary employees, and other external parties;
- Training and assessing programs to maintain information technology expertise levels;
- Reviewing annually information technology insurance coverage and needs;

- Developing formal business continuity plans for each critical area of operations; and
- Overseeing and managing of third-party relationships.

5.4. **Information Technology Security**

5.4.1. Supervisors check whether institutions meet information security requirements and objectives by reviewing and analyzing:

- *Availability* - The ongoing availability of systems addresses the processes, policies, and controls used to ensure authorized users have prompt access to information. This objective protects against intentional or accidental attempts to deny legitimate users access to information and/or systems.
- *Integrity of Data or Systems* - System and data integrity relate to the processes, policies, and controls used to ensure information has not been altered in an unauthorized manner and that systems are free from unauthorized manipulation that will compromise accuracy, completeness, and reliability.
- *Confidentiality of Data or Systems* - Confidentiality covers the processes, policies, and controls employed to protect the information of customers and the institution against unauthorized access or use.

5.4.2. The security process should be in place to implement and achieve its security objectives. The process should be designed to identify, measure, monitor and control the risks to system and data availability, integrity, and confidentiality; and ensure accountability for system actions. The process should include five areas:

- *Information Security Risk Assessment* - A process to identify threats, vulnerabilities, attacks, probabilities of occurrence, and outcomes.
- *Information Security Strategy* - A plan to mitigate risk that integrates technology, policies, procedures and training. The plan should be reviewed and approved by the Board.
- *Security Controls Implementation* - The requirements covering acquisition and operation of technology, the specific assignment of duties and responsibilities to managers and staff, the deployment of risk-appropriate controls, and assurance that management and staff understand their responsibilities and have the knowledge, skills, and motivation necessary to fulfill their duties.
- *Security Testing* - The use of various methodologies to gain assurance that risks are appropriately assessed and mitigated. These testing methodologies should verify that significant controls are effective and performing as intended.
- *Monitoring and Updating* - The process of continuously gathering and analyzing information regarding new threats and vulnerabilities, actual attacks on the institution or others combined with the effectiveness of the existing security controls. This information is used to update risk

assessment, strategy, and controls. Monitoring and updating makes the process continuous instead of a one-time event.

5.4.3. Institutions should ensure clear and well-defined responsibilities and expectations exist between risk management and information technology functional areas. The critical functional areas include:

- Risk management functions including information technology audits, information security, business continuity, outsourcing, and regulatory compliance; and
- Information technology functions including project management, human resources, operations and MIS.

5.5. **Management Information System (MIS)**

5.5.1. Directors should design the institution's MIS to:

- Facilitate the management of all business activities;
- Provide management with an adequate decision support system by providing information that is timely, accurate, consistent, complete, and relevant;
- Deliver complex material throughout the institution;
- Support the organization's strategic goals and direction;
- Ensure the integrity and availability of data;
- Provide an objective system for recording and aggregating information;
- Reduce expenses related to labor-intensive manual activities; and
- Enhance communication among employees.

5.5.2. Compromise of any of the following elements hinders the usefulness of MIS.

- *Timeliness* - To facilitate prompt decision-making, an institution's MIS should be capable of providing and distributing *current* information to appropriate users. Developers should design information technology systems to expedite the availability of reports. The system should support quick data collection, prompt editing and correction, and meaningful summaries of results.
- *Accuracy* - A sound system of automated and manual internal controls should exist. All information should receive appropriate editing, balancing, and internal control checks. The Board should ensure a comprehensive internal and external audit program exists to ensure the adequacy of internal controls.
- *Consistency* - To be reliable, data should be processed and compiled consistently and uniformly. Variations in data collection and reporting methods can distort information and trend analysis. In addition, management should establish sound procedures to allow for system changes. These procedures should be well defined, documented, and communicated to appropriate employees. Management should also establish an effective monitoring system.

- *Completeness* - Decision makers need complete information in a summarized form. Management should design reports to eliminate clutter and voluminous detail to avoid information overload.
- *Relevance* –Information that is inappropriate, unnecessary, or too detailed for effective decision-making has no value. MIS should be relevant to support its use to management. The relevance and level of detail provided through MIS directly correlates to what the Board, Directors, senior managers, departmental or mid-level managers, etc., need to perform their jobs.

5.5.3. Directors should identify, measure, control, and monitor technology to avoid risks that threaten the safety and soundness of an institution. The institution should *plan* for the use of technology, *assess* the risk associated with technology, *implement* the technology, and establish a process to *measure and monitor* risk that is taken on. All organizations should have:

- An effective planning process that aligns information technology and business objectives;
- An ongoing risk assessment process that evaluates the environment and potential changes;
- Technology implementation procedures that include appropriate controls; and
- Measurement and monitoring efforts that effectively identify ways to manage risk exposure.

5.6. **Planning and Project Management**

5.6.1. The Board and Directors should implement an information technology planning process that:

- Aligns information technology with the corporate wide strategic plan;
- Aligns information technology strategically and operationally with business units;
- Maintains an information technology infrastructure to support current and planned business operations;
- Integrates information technology spending into the budgeting process and weighs direct and indirect benefits against the total cost of ownership of the technology; and
- Ensures the identification and assessment of risk before changes or new investment in technology.

5.7. **Development**

5.7.1. Institutions should establish appropriate systems and application development methodologies. The methodologies should match a project's characteristics and risks and require appropriate:

- Project plans;
- Definitions of project expectations;
- Project standards and procedures;

- Definitions of project phase deliverables, including assurance that deliverables will meet any applicable legal and regulatory requirements;
- Security, audit, and automated-control features;
- Quality assurance, risk management, and testing standards and procedures;
- Involvement by all affected parties; and
- Project communication techniques.

5.8. **Large-Scale Systems**

5.8.1. Large-scale integrated systems are comprised of multiple applications that operate as an integrated unit. The systems are designed to use compatible programming languages, operating systems, and communication protocols to enhance interoperability and ease maintenance requirements. Effectively implementing large-scale integrated systems is a complex task that requires considerable resources, strong project and risk management techniques, and a long-term commitment from Boards and Directors. Although the anticipated benefits of integrated systems may be compelling, there are significant challenges associated with the development process. Some organizations underestimate the demands of such projects, incur significant financial losses, and ultimately abandon the projects. Supervisors encountering organizations that are implementing large-scale integrated systems will thoroughly review all life cycle procedures. The reviews include an assessment of the Board's understanding of project requirements and commitment to the project. Supervisors will also closely review the qualifications of the project manager, the adequacy of project plans, and the sufficiency of risk management procedures.

5.9. **Acquisitions**

5.9.1. Institutions should establish appropriate acquisition methodologies. The methodologies should match a project's characteristics and risks and require appropriate:

- Project plans;
- Project standards and procedures;
- Quality assurance, risk management, and testing standards and procedures;
- Definitions of product requirements;
- Involvement by all affected parties;
- Vendor, contract, and license reviews; and
- Escrow documentation.

5.10. **Maintenance**

5.10.1. Institutions should establish appropriate maintenance methodologies. The methodologies should match a project's characteristics and risks and require appropriate:

- Project planning;

- Maintenance standards and procedures;
- Major, routine, and emergency change controls;
- Patch management controls;
- Involvement by all affected parties;
- Documentation standards;
- Library and utility controls; and
- Quality assurance and risk management standards and procedures.

5.11. **Patch Management**

5.11.1. Vendors frequently develop and issue patches to correct software problems, improve performance, and enhance security. Institutions should have procedures in place to identify available patches and to acquire them from trusted sources. Procedures for identifying software vulnerabilities and patch information include subscribing to patch alert e-mail lists and monitoring vendor and security related websites. Management should regularly obtain bulletins about product enhancements and security issues as well as available patches and upgrades from its vendors or other trusted information security sources. When an available patch is identified, management should evaluate the impact of installing the patch by assessing technical, business, and security implications. *If management identifies a significant patch but decides not to install it, they should document their reasons for not installing*. *In order to minimize operational disruptions, management should test all patches prior to implementation*. Additionally, management should appropriately backup files and programs and have established back-out procedures in place before implementation.

5.12. **E-banking**

5.12.1. Directors should choose the level of e-banking services provided to various customer segments based on customer needs and the institution's risk assessment considerations. Institutions should reach this decision through a Board approved, e-banking strategy that considers factors such as customer demand, competition, expertise, implementation expense, maintenance costs, and capital support. Once an institution implements its e-banking strategy, the Board and Directors should periodically evaluate the strategy's effectiveness.

5.12.2. In managing the risk associated with e-banking services, the institution should develop clearly defined e-banking objectives by which the Board and Directors can evaluate the success of e-banking strategies. In particular, institutions should pay attention to the following:

- Costs involved in monitoring e-banking activities or costs involved in overseeing e-banking vendors and technology service providers;
- Design, delivery, and pricing of services adequate to generate sufficient customer demand;

- Retention of electronic loan agreements and other electronic contracts in a format that will be admissible and enforceable in litigation; and
- Adequacy of technical, operational, compliance, or marketing support for e-banking products and services.

5.12.3. Institutions that outsource e-banking technical support must provide sufficient oversight of service providers' activities to identify and control the resulting risks. The key to good oversight typically lies in effective MIS. However, for MIS to be effective the financial institution must first establish clear performance expectations. Wherever possible, these expectations should be clearly documented in the service contract or an addendum to the contract. Effective and timely MIS can alert the serviced institution to developing service, financial or security problems at the vendor — problems that might require execution of contingency plans supporting a change in vendor or in the existing service relationship.

5.13. **Retail Banking**

5.13.1. Institutions engaged in retail payment systems should establish an appropriate risk management process that identifies, measures, and limits risks. Directors and the Board should manage and mitigate the identified risks through effective internal and external audit, physical and logical information security, business continuity planning, vendor management, operational controls, and legal measures. Institutions should tailor their risk management strategies to the nature and complexity of their participation in retail payment systems, including any support they offer to clearance and settlement systems. Institutions must comply with the legal framework as well as with clearinghouse, bankcard association, and regulatory requirements associated with retail payment transactions.