National Bank of the Republic of Macedonia
Supervisory Policy Manual

Title: A-1 Internal Controls and Audit Function

Date: FINAL

Purpose: Explanation of NBRM Supervision Approach to the evaluation and supervision of an institution's internal controls and audit function.

Issue Type: Guidance, in conjunction with the Supervisory Circular No.1 on the internal control systems, the structure of the internal audit, the role of the external audit and the relationship among the internal audit, the external audit and the banking supervision (revised text) , dated April 2005.

Supersedes Previous Issue: None

Application: Supervisory Personnel and all Licensed Institutions

Contents:

1. Introduction
2. Internal Controls
    - 2.1. Overview
    - 2.2. Regulatory Requirements
    - 2.3. Internal Control Components
    - 2.4. Supervisory Board and Board of Directors Oversight
    - 2.5. Supervisory Approach in Assessing Internal Control
3. Internal and External Audit Function
    - 3.1. Overview
    - 3.2. Audit Evaluation
    - 3.3. Supervisory Board and Board of Directors Oversight
    - 3.4. Risk Assessment and Risk-based Auditing
    - 3.5. Supervisory Approach to Assessing Audit Function
4. Internal Audit Function
    - 4.1. Overview
    - 4.2. Oversight and Structure
    - 4.3. Internal Audit Program
    - 4.4. Independence
    - 4.5. Competence
    - 4.6. Operations of Foreign Banking Organizations
5. External Audit Function
    - 5.1. Overview
    - 5.2. Types of External Auditing Programs
    - 5.3. Audit Opinions
    - 5.4. Special Situations
    - 5.5. Independence
    - 5.6. Competence
    - 5.7. Information System/Technology Audits
    - 5.8. Policy on Coordination and Communication Between External Auditors and Supervisors

1. Introduction

1.1. Effective internal controls are the foundation of safe and sound banking; and well-planned, properly structured auditing programs (internal and external) are essential to strong risk management and comprehensive internal control systems. While the internal control system and the audit function are related, they are two distinct processes.

1.2. Internal controls represent an ongoing "process" which is applied at all institutional levels by the Supervisory Board (Board), Board of Directors (Directors) and all employees. A properly designed and consistently enforced system of operational and financial internal control helps an institution's Board and Directors safeguard the institution's resources, produce reliable financial reports, and comply with laws and regulations. Effective internal control also reduces the possibility of significant errors and irregularities and assists in their timely detection when they do occur.

1.3. The internal audit provides an objective and independent evaluation of the adequacy and efficiency of the internal control system, accuracy of accounting records and financial statements, adherence to internal policies and procedures, and compliance with laws and regulations. It also determines the general efficiency of the institution's operations. The internal audit is an independent unit within the institution and separated from other institutional units, both from a functional and organizational perspective. The internal audit function is, hierarchically, located above other operational units, and reports directly to the Board and Auditing Committee. The size of the institution and the complexity of its business activities dictate the scope of the internal audit and staffing requirements (number and competencies) of an internal audit unit.

1.4. The external audit complements the institution's internal audit function, strengthens internal controls, and contributes to safe and sound operations. The external audit, conducted by a qualified and licensed auditor or audit firm, also provides an independent and objective view of an institution's activities, including processes relative to financial reporting. It provides a reasonable assurance to the Board and Directors about the effectiveness of internal controls over financial reporting, the accuracy and timeliness in recording transactions, and the accuracy and completeness of financial and regulatory reports. External auditors also provide guidance to Board and Directors in maintaining the institution's risk management processes. On an annual basis, institution's are required to obtain an independent external audit opinion as to whether or not financial statements fairly present, in all material respects, the institution's financial position and results of operations, and are prepared in conformity with generally accepted accounting practices. Effective internal and external audit programs are also a critical defense against fraud.

1.5. This guidance discusses the characteristics of effective controls and audit functions, and assists in the evaluation of the quality and effectiveness of internal controls and the internal and external audit programs. It describes the roles and responsibilities of the Board and Directors in safeguarding the institution's resources, producing reliable financial reports, and complying with laws and regulations.

2. Internal Controls

2.1. Overview

2.1.1. Effective internal control provides a reasonable assurance that an institution's risk management systems are effective and its operations are efficient; and that recorded transactions are accurate and financial reporting is reliable. Effective internal controls also provide assurances that the institution's employees comply with laws and regulations and internal policies and procedures.

2.1.2. Control systems can assist the institution's management in measuring performance, making decisions, evaluating processes, and limiting risks. Good internal control can assist management in achieving its objectives; and avoid surprises, detect mistakes and fraud or deliberate noncompliance with policies. However, even effective and well-designed control systems can fail because personnel still must execute most control systems and even well trained personnel with the best of intentions can become distracted, careless, tired, or confused. Therefore internal control must be consistently applied and well understood by all staff members if Board and Directors policies are to be effectively implemented.

2.1.3. Controls typically (1) limit authorities, (2) safeguard access to and use of records and the institution's assets, (3) separate and rotate duties, and (4) ensure both regular and unscheduled reviews, including testing. An institution's Board and Directors cannot delegate their responsibilities for establishing, maintaining, and operating an effective system of internal control. Hence, the Board must ensure that Directors regularly verifies the integrity of the institution's internal control systems.

2.2. Regulatory Requirements

2.2.1. Institutions must adhere to certain regulatory requirements regarding internal control. These requirements direct institutions to operate in a safe and sound manner, accurately prepare their financial statements, and comply with laws and regulations. Safety and soundness standards establish certain managerial and operational standards for all institutions, including standards for internal control. An institution should have internal controls that are appropriate to its size and the nature, scope, and risk of its activities, and that provide for:

- An organizational structure that establishes clear lines of authority and responsibility for monitoring adherence to prescribed policies.
- Effective risk assessment.
- Timely and accurate financial, operational, and regulatory reports.
- Adequate procedures to safeguard and manage assets.
- Compliance with applicable laws and regulations.

2.2.2. When an institution fails to meet these standards, the NBRM may require Directors to submit a compliance plan to address internal control deficiencies. If the institution fails to submit a satisfactory plan, the NBRM must, by law, order the institution to correct the deficiency.

2.2.3. As part of the internal control process, all institutions are required to employ an independent audit on an annual basis and submit a report to the NBRM that includes:
- Annual audited financial statements.
- A statement of management's responsibilities for preparing financial statements, establishing and maintaining internal control and procedures for financial reporting, and complying with safety and soundness laws concerning loans to insiders and dividend restrictions.
- Management's assessment of the effectiveness of the institution's internal control and procedures for financial reporting as of the end of the fiscal year, and management's assessment of the institution's compliance with designated laws and regulations during the most recent fiscal year.
- A report by the independent auditor attesting to management's assertions regarding internal control and procedures for financial reporting.

2.3. **Internal Control Components**

2.3.1. The formality of any control system will depend largely on an institution's size, the complexity of its operations, and its risk profile. Less formal and structured internal control systems at small institutions can be as effective as more formal and structured internal control systems at larger and more complex institutions. Nevertheless, every effective control system should have:
- A control environment.
- Risk assessment.
- Control activities.
- Accounting, information, and communication systems.
- Self-assessment or monitoring.

2.3.2. The **control environment** reflects the Board's and Directors' commitment to internal control. It provides discipline and structure to the control system. Elements of the control environment include:
- The Organizational structure of the institution. (Is the institution's organization centralized or decentralized? Are authorities and responsibilities clear? Are reporting relationships well designed?)
- Management's philosophy and operating style. (Are the institution's business strategies formal or informal? Is its philosophy and operating style conservative or aggressive? Have its risk strategies been successful?)
- The integrity, ethics, and competence of personnel.
- The external influences that affect the institution's operations and risk management practices (e.g., independent audits).
- The attention and direction provided by the Board and its committees, especially the auditing or risk management committees.
- The effectiveness of human resources policies and procedures.

2.3.3. **Risk assessment** is the identification, measurement, and analysis of risks, internal and external, controllable and uncontrollable, at individual business levels and for the institution as a whole. Management must assess all risks facing the institution because

uncontrolled risk-taking can prevent the institution from reaching its objectives or can jeopardize its operations. Effective risk assessments help determine what the risks are, what controls are needed, and how they should be managed.

2.3.4. **Control activities** are the policies, procedures, and practices established to help ensure that personnel carry out Board and Directors directives at every business level throughout the institution. These activities help ensure that the Board and Directors act to control risks that could prevent an institution from attaining its objectives. They should include:

- Reviews of operating performance and exception reports. For example, Directors regularly should review reports showing financial results to date versus budget amounts, and the loan department manager should review weekly reports on delinquencies or documentation exceptions.
- Approvals and authorization for transactions and activities. For example, an appropriate level of management should approve and authorize all transactions over a specified limit, and authorization should require dual signatures.
- Segregation of duties to reduce a person's opportunity to commit and conceal fraud or errors. For example, assets should not be in the custody of the person who authorizes or records transactions.
- Requirement that officers and employees in sensitive positions be absent for two consecutive weeks each year.
- Design and use of documents and records to help ensure that transactions and events are recorded. For example, using pre-numbered documents facilitates monitoring.
- Safeguards for access to and use of assets and records. To safeguard data processing areas, for example, an institution should secure facilities and control access to computer programs and data files.
- Independent checks on whether responsibilities are fulfilled and recorded amounts are accurate. Examples of independent checks include account reconciliation, computer-programmed controls, management review of reports that summarize account balances, and user review of computer generated reports.

2.3.4.1. Institutions are required to develop and maintain written procedures or controls for all major areas and activities. Personnel must also understand control procedures and follow them conscientiously.

2.3.5. **Accounting, information, and communication systems** capture and impart pertinent and timely information in a form that enables the Board, Directors, and employees to carry out their responsibilities. Accounting systems are the methods and records that identify, assemble, analyze, classify, record, and report an institution's transactions. Information and communication systems enable all personnel to understand their roles in the control system, how their roles relate to others, and their accountability. Information systems produce reports on operations, finance, and compliance that enable Directors and the Board to effectively administer the affairs of the institution. Communication systems impart information throughout the institution and to external parties such as shareholders, customers, NBRM supervisors, and other government entities.

2.3.6. **Self-assessment or monitoring** is the institution's own oversight of the control system's performance. Self-assessments are evaluations of departmental or operational controls by persons within the area. Ongoing monitoring should be part of the normal course of daily operations and activities. Internal and external audit functions, as part of the monitoring system, also provide independent assessments of the quality and effectiveness of a control system's design and performance. All institutional personnel should share responsibility for self-assessment or monitoring; everyone should understand his or her responsibility to report any breaches of the control system. Strong control cultures typically incorporate qualified personnel, effective risk identification and analysis, clear designation and appropriate separation of responsibilities, accurate and timely information flow, and established monitoring and follow-up processes.

2.4. **Supervisory Board and Board of Directors Oversight**

2.4.1. The success of a positive control environment is the commitment by the Board and Directors to strong controls. An institution's Board and Directors are responsible for establishing and maintaining effective internal control that meets statutory and regulatory requirements and responds to changes in the institution's environment and conditions. They must ensure that the system operates as intended and is modified appropriately when circumstances dictate. The Board and Directors must make sure that the institution's information systems produce pertinent and timely information in a form that enables employees, auditors, and supervisors to carry out their respective responsibilities.

2.4.2. The Board, which oversees the control system in general, approves and reviews the business strategies and policies that govern the system. They are also responsible for understanding and setting acceptable risk limits for the institution's major business activities, establishing organizational control structure, and making sure Directors identify, measure, monitor, and control risks and monitor internal control effectiveness. The Board should (1) discuss periodically the internal control system's effectiveness with Directors; (2) review internal control evaluations conducted by Directors, auditors, and supervisors in a timely manner; (3) monitor Directors' actions on auditors' and supervisor's internal control recommendations and concerns; and (4) periodically review the institution's strategy and risk limits. The Board may delegate these duties to an auditing committee, risk committee, or both; but the Board is ultimate responsible.

2.5. **Supervisory Approach in Assessing Internal Control**

2.5.1. Evaluating internal control is fundamental to the NBRM overall supervisory process. The NBRM internal control assessments, along with its assessments of the institution's audit programs, help leverage NBRM resources, establish the scopes of supervisory activities, and contribute to developing strategies for an institution's ongoing supervision. Supervisors base the scope, type, and depth of an internal control review on the institution's size, complexity, scope of activities, and risk profile, as well as on the NBRM assessment of the institution's audit functions.

2.5.2. ***Supervisory Principles***

2.5.2.1. When reviewing an institution's internal controls, supervisors consider the following:

- **Integration.** Supervisors integrate and coordinate internal control reviews for all areas examined, especially the audit area.
- **Analysis.** Supervisors review and analyze available information to identify systemic control issues, to gauge changes in the institution's control environment and overall risk profile, and to evaluate controls in general. Useful sources of information include discussions with Directors, organization charts, procedural manuals, operating instructions, job specifications and descriptions, directives to employees, flow charts, internal and external audit reports and management letters, and other control and risk assessment material.
- **Communication.** NBRM staff maintain ongoing and clear communications with the institution's personnel. Supervisors hold periodic meetings with institutional personnel or committees closely associated with risk control functions (e.g., audit or risk committees, risk managers, control officers, auditors, etc.). Communication regarding NBRM internal control supervision and findings occur throughout an examination or supervisory cycle. Examination reports and other written communications to an institution include comments about the adequacy of the institution's control functions and summarize other appropriate findings and conclusions.
- **Linkage.** The quality and reliability of an institution's internal control function are factors in CAMEL ratings (especially for the management component). The NBRM also incorporates findings about internal control adequacy in risk assessments and risk profiles.
- **Documentation.** Supervisors prepare documentation in the form of working papers, which contain essential information to support conclusions about the evaluation of internal control. The level of detail is commensurate with the risks facing the institution and provide an audit trail that supports examination conclusions. The supervisor generates and retains only those documents necessary to support the scope of the review, significant conclusions, ratings changes, or changes in risk profile.

2.5.3. *Internal Control Evaluation*

2.5.3.1. Evaluating internal control involves (1) identifying the internal control objectives relevant to the institution, department, business line, or product; (2) reviewing pertinent policies, procedures, and documentation; (3) discussing controls with appropriate levels of personnel; (4) observing the control environment; (5) testing transactions as appropriate; (6) sharing findings, concerns, and recommendations with the Board and Directors; (7) determining that the institution has taken timely corrective action on noted deficiencies; and (8) determining whether management performs a satisfactory assessment of the institution's control structure.

2.5.3.2. In reviewing internal control in a specific area of the institution, a supervisor identifies key control personnel and positions by asking the following questions:

- Is this a critical position? Can a person in this position make a significant error that will result in the inaccurate recording of transactions? Can he or she enter false information or gain control of assets?

- If an error or irregularity occurs, would normal controls promptly disclose it? Would controls prevent or detect significant errors or irregularities?
- Is it possible for a person to conceal an error or irregularity, and are there controls in place to minimize this possibility?

2.5.3.3. Primarily, the supervisor's concern is with personnel who have influence over financial records and access to assets. Persons in these positions could be involved in information processing (computer programmers) or investment and trading activities (traders, buyers, and sellers). Once those positions have been identified, the supervisor must determine whether internal controls will either prevent errors and irregularities or uncover them promptly. One example of such controls is the requirement that employees in key or influential positions be absent two consecutive weeks each year.

2.5.3.4. Supervisors ensure that employee duties and responsibilities are properly segregated to minimize the possibility of errors and irregularities. For example, in the investment area, the following duties should be strictly segregated: executing securities transactions, approving transactions, accessing securities record keeping, and posting or reconciling related accounting records. Supervisors investigate any activity in which controls do not prevent persons from having both custody and record keeping responsibilities for assets and determine whether mitigating factors exist.

2.5.3.5. Segregation of duties can break down when controls do not keep pace with an institution's growth and diversification, practices become lax, or personnel use their knowledge or influence to circumvent control. Before reaching conclusions about a specific area's internal control, supervisors consider circumstances that may cause employees or officers to take undue risks. The supervisor is especially alert to circumstances in which the personal financial interests of key officers or employees depend directly on the financial condition of the institution. Sound internal control ensures that conflicts of interest are minimized or controlled. Both manifest and potential conflicts of interest are considered in the overall assessment of internal control. In addition, the supervisor is alert to deviations by personnel from established policies, practices, and procedures. Such deviations may exist when:

- Instructions and directives are not reviewed and revised regularly to reflect current practices.
- Employees use shortcuts to perform their tasks, circumventing internal control procedures.
- Changes in organization or activities are not reflected in policies or procedures.
- Employees' duties are changed significantly in ways that may affect internal control policies.

2.5.3.6. The proliferation of computer systems and personal computers (PCs) requires increased controls over computer operations. Because institutions depend on computers, embezzlement or misuse of funds is often a computer crime. The list of persons whose computers have access to assets or financial records can often be

long; it includes computer operators, programmers, their supervisors, and others. Institutions should impose sophisticated controls not only on mainframe operations but also on the systems and records maintained on PCs, local area networks (LANs), and wide area networks (WANs). Controls on these systems are of paramount importance; and supervisors determine appropriate controls are in place over information processing, whether automated or manual.

2.5.3.7. Such controls ensure the integrity of management information systems, accounting books, and records. Employees should enter pertinent information into processing systems in a timely manner, and appropriate personnel should independently test that information for accuracy. Personnel should maintain trial balances and subsidiary ledgers and reconcile those ledgers to general ledgers in a timely manner, investigate and resolve any differences noted, and ensure appropriate personnel review and approve completed reconcilements in a timely manner. Procedures should also exist to test the accuracy of spreadsheets and reports created by individual users.

2.5.3.8. A significant deficiency in a control system is a deficiency in risk management. For example, the failure to process transactions in an accurate, thorough, and timely manner (a failure of internal control) exposes the institution to potential losses. Other examples of such deficiencies are inadequate underwriting standards and failure to follow established underwriting standards, both of which expose the institution to credit risk losses. Such failures may lead to compliance errors, inaccurate management information systems, material misstatements in financial statements, and employee fraud that expose the institution to strategic and legal risks.

2.5.4. *Supervisory Process and Validation*

2.5.4.1. During every supervisory cycle, the NBRM assesses the adequacy of an institution's internal control as *strong*, *satisfactory*, or *weak*. Supervisors begin their control assessment by reviewing the work of the institution's internal audit or other control review functions, generally as part of pre-examination planning. Supervisors make a preliminary assessment of internal control reliability and identify control problems, areas of potential or high risk, and areas not recently reviewed. That assessment influences how much validation work supervisors perform during supervisory activities.

2.5.4.2. Validation encompasses inquiry, observation, and testing as appropriate, of the institution's control systems. How thoroughly a supervisor validates internal control for a specific examination area depends on how much supervisory concern he or she has about that area. Generally, supervisors begin with a discussion with persons responsible for control management to gain an overall understanding of and insight into the institution's control system. As warranted, supervisors perform independent verification or testing of internal control integrity if substantive issues surface that raise questions about the adequacy or effectiveness of the control systems.

3. Internal and External Audit Function

3.1. Overview

3.1.1. Well-planned, properly structured auditing programs are the responsibility of the Board and Directors. They cannot delegate this responsibility and must establish, maintain, and operate effective audit programs. Audit programs are performed by independent and competent staff who are objective in evaluating the institution's control environment. Effective audit programs:

- Provide objective, independent reviews and evaluations of the institution's activities, internal controls, and management information systems (MIS).
- Help maintain or improve the effectiveness of risk management processes, controls, and corporate governance.
- Provide reasonable assurance about the accuracy and timeliness with which transactions are recorded and the accuracy and completeness of financial and regulatory reports.

3.1.2. Audit programs may comprise several individual audits that provide various types of information to the Board about the institution's financial condition and effectiveness of internal control systems. The most common types of audits are financial, operational, compliance, and information systems or technology audits.

3.1.2.1. ***Financial audits*** review an institution's financial statements, a specific account, or a group of accounts within the financial statements. The purpose of this audit is to determine whether the financial statements fairly present the financial position, results of operations, and cash flows as of a certain date or for a period ending on that date. Independent audit firms or auditors perform this type of audit primarily to render an opinion about whether the financial statements are presented fairly and in accordance with generally accepted accounting principles. An internal auditor may assist the external auditor during such an audit.

3.1.2.2. ***Operational audits*** review a specific department, division, or area of an institution. This type of audit includes a review of policies, procedures, and operational controls (e.g., loan review) to determine whether risk management, internal controls, and internal processes are adequate and efficient. Operational audits generally include procedures to test integrity of accounts, regulatory reports, and other aspects of operations. These audits may also include a review of management and employee compliance with policies and procedures.

3.1.2.3. ***Compliance audits*** determine whether the institution is complying with internal procedures, internal controls, and applicable laws and regulations.

3.1.2.4. ***Information system or technology audits*** assess the controls over an institution's electronic data processing and computer areas. These audits focus on management, development and acquisition, support and delivery, data security, and physical security. Information system or technology audits might also include a review of computer and client/server systems, end-user reports, electronic funds transfer, and service provider activities.

3.1.3. An institution's audit programs should include each of these types of audits, although the level of formality and detail will vary. Auditors may perform these audits separately or blend elements of each to achieve overall audit objectives. In some institutions, the

external auditors may perform some of the work that is traditionally thought to be internal audit work or rely on the work of the internal auditor. Regardless of who performs the work, the institution's size, complexity, scope of activities and risk profile should determine the extent of its audit program.

3.2. **Audit Evaluation**

3.2.1. Characteristics and practices of effective internal and external audit programs rely on the quality and scope of the audit program and whether:

- The Board or its auditing committee reviews and approves audit policies at least annually.
- The Board or its auditing committee monitors the implementation of the audit program and its audit schedule.
- The internal and external audit functions are sufficiently independent and their staffs are competent.
- The audit's scope and frequency, risk assessments, plans, and work programs are appropriate.
- Audit findings are promptly communicated to the Board or its auditing committee and appropriate management.
- The Board and Directors properly follow up on the results of audits and appropriately monitor any significant issues.
- Internal and external auditors maintain an appropriate level of professional standards and training/development.

3.3. **Supervisory Board and Board of Directors Oversight**

3.3.1. An institution's Board is responsible for establishing and maintaining effective audit functions that satisfy statutory, regulatory, and supervisory requirements. The Board cannot delegate these responsibilities. However, they may delegate the design, implementation, and monitoring of specific internal controls to management and the testing and assessment of internal controls to auditors and others. The Board or auditing committee minutes should reflect decisions regarding audits, such as external audit engagement terms (including any decision to forgo an external audit), the scope of audits to be performed, or why an audit of a particular area is not necessary. The Board is specifically responsible for reviewing and approving audit strategies, policies, programs, and organizational structure. The Board should also monitor the effectiveness of the audit function.

3.3.2. The formality and extent of an institution's internal and external audit programs depend on the institution's size, complexity, scope of activities, and risk profile. The Board must carefully consider how extensive the audit program must be to effectively test and monitor internal controls and ensure the reliability of the institution's financial statements and reporting. The Board (and audit management) must ensure that the institution's audit programs test internal controls to identify:

- Inaccurate, incomplete, or unauthorized transactions;
- Deficiencies in the safeguarding of assets;
- Unreliable financial and regulatory reporting;

- Violations of laws or regulations; and
- Deviations from the institution's policies and procedures**.**

3.3.3. At least annually, Directors should identify the major risks faced by the institution to assist the Board or the auditing committee in establishing appropriate audit coverage. The Board or auditing committee should also ensure that internal and external auditors are independent of the institution's Directors and are objective. The auditing committee should be involved in hiring senior internal audit personnel, setting compensation for internal audit staff, reviewing audit plans, and evaluating the performance of internal auditors. It should seek to retain personnel who are qualified to audit the activities in which the institution engages, evaluate internal controls, and determine whether management is properly following up on the auditor's or the NBRM recommendations and concerns. The committee should also meet with supervisors as necessary to review reports and discuss findings.

3.3.4. The Board must be aware of all risks and control issues for the institution's operations, including risks in new products, emerging technologies, information systems, and electronic banking. Control issues and risks associated with increasing reliance on technology include increased user access to information systems, reduced segregation of duties, a shift from paper to electronic audit trails, a lack of standards and controls for end-user systems, and increased complexity of contingency plans and information system recovery plans.

3.3.5. Audit management is responsible for implementing board-approved audit directives. They oversee audit operations and provide leadership and direction in communicating and monitoring audit policies, practices, programs, and processes. Audit management should establish clear lines of authority and reporting responsibility for all levels of audit personnel and activities. They also should ensure that members of the audit staff possess the necessary experience, education, training, and skills to properly conduct assigned activities.

3.4. **Risk Assessment and Risk-based Auditing**

3.4.1. The NBRM encourages risk assessment and risk-based auditing for all institutions. Risk assessment is the means by which an institution identifies and evaluates the quantity of the institution's risks and the quality of its controls. Through risk-based auditing, the Board and auditors use the results of the risk assessments to focus on the areas of greatest risk and to set priorities for audit work. An effective risk-based auditing program will cover all of an institution's activities. The frequency and depth of each area's audit will vary according to the area's risk assessment.

3.4.2. Properly designed risk-based audit programs increase audit efficiency and effectiveness. The sophistication and formality of risk-based audits will vary for individual institutions depending on its size, complexity, scope of activities, capabilities of staff, quality of control functions, geographic diversity, and technology used. All risk-based audit programs should:

- Identify all of an institution's businesses, product lines, services, and functions.

- Identify the activities within those businesses, product lines, services, and functions that the institution should audit.
- Include profiles of significant business units, departments, and products that identify business and control risks and document the structure of risk management and internal control systems.
- Use a measurement or scoring system to rank and evaluate business and control risks of significant business units, departments, and products.
- Include a risk-based audit plan that establishes audit schedules, audit cycles, work program scope, and resource allocation for each area to be audited.
- Implement the audit plan through planning, execution, reporting, and follow-up.
- Have systems that monitor risk assessments regularly and update them at least annually for all significant business units, departments, and products.

3.4.3. An effective scoring system is critical to a successful risk-based audit program. In establishing a scoring system, the Board and Directors must consider all relevant risk factors so that the system minimizes subjectivity, is understood, and is meaningful. Major risk factors commonly used in scoring systems include the nature of transactions (e.g., volume, size, liquidity); the nature of the operating environment (e.g., complexity of transactions, changes in volume, degree of system and reporting centralization, economic and regulatory environment); internal controls, security, and MIS; human resources (e.g., experience of management and staff, turnover, competence, degree of delegation); and Directors oversight of the audit process. The Board should approve written guidelines on the use of risk assessment tools and risk factors.

3.4.4. Auditors will use the guidelines to grade or assess major risk areas. These standards generally define the basis for the institution's weights and scores (e.g., the basis could be normal industry practices or the institution's own experiences). They also define the range of scores or assessments (e.g., low, medium, and high, or a numerical sequence, for example, 1 through 5). The written guidelines should specify:

- The length of the audit cycles based on the scores or assessments. Audit cycles should not be open-ended. For example, some institutions set audit cycles at 12 months or less for high-risk areas, 24 months or less for medium-risk areas, and more than 24 months for low-risk areas. However, individual judgment and circumstances at each institution will determine the length of its audit cycles.
- Guidelines for when risk assessments can be overridden, who has override approval authority (i.e., Board, auditing committee, or audit management), and for reporting and documenting overrides. Overrides of risk assessments should be more the exception than the rule.
- The timing of risk assessments for each department or activity. Normally risks are assessed annually, but they may need to be assessed more often if the institution or one of its products experiences excessive growth, or staff or activities change significantly.
- Minimum documentation requirements to support scoring or assessment decisions.

3.4.5. Institutions can obtain matrices, models, or additional information on risk assessments from industry groups and many auditing firms. Another resource for helping Board and auditors evaluate controls and risk assessments is the "Internal Control – Integrated Framework" report issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

3.4.6. Day-to-day management of the risk-based audit program rests with the internal auditor or internal audit manager who will monitor the audit scope and risk assessments to ensure that audit coverage remains adequate. The internal auditor or audit manager will also prepare reports showing the risk rating, planned scope, and audit cycle for each area. The audit manager should confirm the risk assessment system's reliability at least annually or whenever significant changes occur within a department or function. Line department managers and auditors should work together in evaluating the risk in all departments and functions. Line department managers should review risk assessments to determine whether they are reasonable. Auditors periodically review the results of internal control processes and analyze financial or operational data for any effect on a risk assessment or weighting. Accordingly, the institution's management should keep auditors current on all major changes in departments or functions, such as the introduction of a new product, implementation of a new system, or changes in organization or staff.

3.5. **Supervisory Approach to Assessing Audit Function**

3.5.1. Assessments of an institution's audit programs are fundamental to the NBRM overall supervisory process. Audit assessments help leverage NBRM resources, establish the scopes of supervisory activities, and contribute to an institution's supervisory strategy.

3.5.2. Effective NBRM audit supervision encompasses the following five principles:

- **Integration**. The supervisor integrates audit reviews, including validation, into the supervisory activities for each functional, specialty, and risk area as needed. Supervisory specialists are consulted about the audit functions for complex activities or assist in assessing those activities.
- **Analysis**. A supervisor reviews audit reports and management responses, auditing committee minutes and records, and supervisory findings to identify changes in the institution's risk profile, systemic control issues, or changing audit trends. This review also includes other information maintained by the internal auditor, such as organization charts, audit charter or mission statement, external auditor or outsourcing vendor engagement letters, audit manuals, operating instructions, job specifications and descriptions, directives to employees, flow charts, and internal control and risk assessments.
- **Communication**. NBRM staff maintain ongoing and clear communications with institutional personnel. Supervisors have periodic meetings with an institution's auditing committee and regular meetings with audit management/staff, other personnel closely associated with risk control functions (e.g., risk managers, control officers), and external auditors. Communication regarding audit supervision and audit findings occur throughout a supervisory cycle. Examination reports and other written communications to an institution include comments about the adequacy of the

institution's audit programs and summarize other appropriate findings and conclusions.

- **Linkage**. Supervisors link audit conclusions to assigned ratings, risk assessments, and supervisory strategies. In particular, management ratings, audit component ratings in specialty areas, and individual risk assessments are linked directly to the quality and reliability of an institution's audit functions.
- **Documentation**. Supervisors document working papers that leave a clear audit trail that supports findings and conclusions and allows for an understanding how conclusions were reached.

3.5.3. ***Supervisory Process and Validation.***

3.5.3.1.Supervisors will draw an overall conclusion and assess as *strong, satisfactory, or weak* the adequacy of the institution's internal and external audit programs during every supervisory cycle. The supervisory assessment of the audit program influences how much work supervisors will perform during supervisory activities. In developing the appropriate scope for audit activities, supervisors select procedures that fit the size, complexity, scope of activities, and risk profile of the institution being assessed.

3.5.3.2.Supervisors responsible for audit program reviews will determine how much reliance the NBRM can place on internal and external audit work by validating the audit program at each risk focused, CAMEL rating on-site examination. The objective of validating the auditors' work is to gain a better understanding of audit-related policies, procedures, practices, and findings, and to substantiate conclusions about the quality and reliability of internal and external audits. Validation encompasses observation, inquiry, and testing and generally consists of a combination of supervisor discussions with management and audit personnel, audit work paper reviews, and process reviews (e.g., reviews of policy adherence, risk assessments, follow-up activities, etc.).

3.5.3.3.In validating the adequacy of the institution's audit program, supervisors progress through three steps: work paper review, use of additional procedures, and direct verification.

3.5.4. ***Work paper review.***

3.5.4.1. During each supervisory cycle, supervisors will review an appropriate sample of internal audit program work papers, including those from outsourced internal audit work. The sample for internal audit work paper reviews should represent a cross-section of functions, activities, and assigned internal audit ratings, with a bias toward high-risk and rapid growth areas, technology audits, and activities that are new to the institution. The sample should provide a sufficient basis to validate the scope and quality of the audit programs. For small institutions with relatively low complexity and internal audit functions previously assessed as at least satisfactory, the extent of work paper reviews may be limited to confirming that the audit program has not changed substantially since the last risk focused CAMEL rating examination.

3.5.4.2.If examination findings reveal significant problems or issues with the external audit, or if supervisors become aware of information that raises questions about the adequacy of the external audit program, supervisors will review appropriate external audit work papers. Examples of situations that might trigger an external audit work paper review are:

- Reliance on external audit in lieu of an internal audit program.
- Unexpected or sudden changes in the external auditor.
- Significant changes in the external audit program.
- Significant safety and soundness concerns.
- Issues about independence, objectivity, or competence of the external auditor.

3.5.4.3.Supervisors initially request access to external audit work papers through the institution's management, but do not hesitate to communicate directly with the external auditor if management fails to provide access.

3.5.4.4.For institutions that have outsourced internal audit activities or external audit programs, engagement letters or written contracts should explicitly provide for supervisory access to audit work papers. External auditors may request that supervisors view external audit work papers at the auditor's offices. The external auditor may also require that their representative(s) be present during the reviews. Supervisors' request for work papers are specific to the areas of greatest interest and set forth the reason for the request. Because the external auditor or outsourced vendor may bill the institution for time spent by audit staff in conjunction with a supervisor's review of external audit or outsourced internal audit work papers, the review is focused and efficient.

3.5.5. ***Use of Additional Procedures.***

3.5.5.1. If the audit work paper review identifies significant discrepancies or weaknesses in the audit function, supervisors will expand the examination of the audit program. They also determine, with NBRM management, if the examination work in affected operational or functional business area(s) is to be expanded. For example, supervisors will expand audit program procedures if they encounter or identify:

- Issues of competency or independence relating to internal or external auditors.
- Unexplained or unexpected changes in external auditor or significant changes in the audit program.
- Inadequate scope of the audit program.
- Audit work papers that are deficient or do not support audit conclusions.
- High growth areas of the institution without adequate audit or internal controls.
- Inappropriate actions by insiders to influence the findings or scope of audits.

3.5.5.2.The scope of work will be sufficient to determine the extent of problems and their effect on the institution's operations.

3.5.6. ***Direct Verification.***

3.5.6.1. If after completion of expanded procedures, concerns remain about the adequacy of audit, internal controls, or the integrity of the institution's financial controls, supervisors will use verification procedures to substantiate the internal or external auditor's work. Verification includes, but is not limited to, direct confirmations with customers, service providers, and others as appropriate. Supervisors consult with NBRM management before conducting direct confirmations. Supervisors may perform verification even in situations in which the external auditor has issued an unqualified opinion if discrepancies or weaknesses call into question the accuracy of the opinion. Verification procedures must be used whenever:

- Account records are significantly out of balance.
- Management is uncooperative or poorly manages the institution.
- Management restricts access to the institution's records.
- Significant accounting, audit, or internal control deficiencies remain uncorrected from previous examinations or from one audit to the next.
- Institution's auditors are unaware of, or unable to sufficiently explain, significant deficiencies.
- Management engages in activities that raise questions about its integrity.
- Repeated violations of law affect audit, internal controls, or regulatory reports.
- Other situations exist that supervisors believe warrant further investigation.

3.5.7. For less problematic situations than those identified above, the supervisor may require the institution to expand its audit program to include the areas containing weaknesses or deficiencies. However, this alternative will only be used if management has demonstrated a capacity and willingness to address regulatory problems, if there are no concerns about management's integrity, and management has initiated timely corrective action in the past. If used, this alternative must resolve each identified supervisory problem in a timely manner. If supervisors use this alternative, supervisory follow-up will include a review of audit work papers in areas where the institution's audit was expanded.

4. Internal Audit Function

4.1. Overview

4.1.1. The primary role of the internal auditor is to independently and objectively review and evaluate the institution's activities to maintain or improve the efficiency and effectiveness of, internal controls, and corporate governance. Internal auditors must understand an institution's strategic direction, objectives, products, services, and processes; and communicate findings in a timely manner to the Board and/or its auditing committee and Directors.

4.1.2. The objectives of internal audit are to:

- Evaluate the reliability, adequacy, and effectiveness of accounting, operating, and administrative controls.
- Ensure that internal controls result in prompt and accurate recording of transactions and proper safeguarding of assets.

- Determine whether an institution complies with laws and regulations and adheres to established policies, and whether management is taking appropriate steps to address control deficiencies.

4.1.3. Internal auditors are increasingly responsible for providing constructive business advice on adding new products or services. They also help the institution formulate new policies, procedures, and practices and revise existing ones. Internal auditors often have a role in merger, acquisition, and transition activities. This role includes helping the Board and Directors evaluate safeguards and controls, including appropriate documentation and audit trails, during the institution's acquisition planning and implementation processes.

4.2. **Oversight and Structure**

4.2.1. Institutions should conduct their internal audit activities according to existing professional standards. The international Institute of Internal Auditor's (IIA) "Standards for the Professional Practice of Internal Auditing" establish standards for independence, professional proficiency, scope of work, performance of audit work, and management of internal auditing. (Those standards and other material about the practice of internal auditing can be found at the IIA website, www.theiia.org.) Internal auditors who are not certified or IIA members should be familiar with these or similar standards.

4.2.2. How an internal audit function is organized depends on the institution's size, complexity, scope of activities, and risk profile, as well as the audit function's Board-assigned responsibilities. The chief auditor is often a manager who fulfills his or her responsibilities with the help of an audit staff. The internal audit function also can be performed by holding company employees or by an outside vendor.

4.3. **Internal Audit Program**

4.3.1. An institution's internal audit program consists of the policies and procedures that govern its internal audit functions, including risk-based auditing programs and outsourced internal audit work, if applicable. While smaller institutions' audit programs may not be as formal as those found in larger, more complex institutions, all audit programs include the following:

4.3.2. **Mission statement** or audit charter that outlines the purpose, objectives, organization, authorities, and responsibilities of the internal auditor, audit department, audit staff, and the auditing committee.

4.3.3. **Risk assessments** that document the institution's significant business activities and their associated risks. Results of these risk assessments guide the development of an audit plan and audit cycle and the scope and objectives of individual audit programs.

4.3.4. **An audit plan** that details an internal auditor's budgeting and planning processes. The plan should describe audit goals, schedules, staffing, and reporting. Audit plans usually include overall and individual audit objectives, summary risk assessments for each audit area or business activity, the timing and frequency of planned internal audit work, and a resource budget (budgeted staff hours). The audit committee should formally approve the audit plan at least annually. The internal auditor should present any updated audit plan to the audit committee regularly (in accordance with established policy, although quarterly

is typical). Updated audit plans should compare actual with planned audits and audit hours and explain significant variances from the approved plan.

4.3.5. **An audit cycle** that identifies the frequency of audits. The frequency of audits is usually determined by risk assessments of business activities or areas to be audited and the staff and time available. It is often not practical to audit each area or business activity annually. Areas of high risk, such as funding, lending, or investment/treasury operations, normally warrant more frequent audits than low-risk areas such as premises. Additionally, auditors must consider regulatory and supervisory requirements and guidelines.

4.3.6. **Audit work programs** that set out, for each audit area, the scope and timing of audit procedures, the extent of testing (including criteria for selecting items to be tested), and the basis for conclusions. Work programs should be detailed, cover all areas of the institution's operation, and guide the auditor in gathering information, documenting procedures performed, arriving at conclusions, and issuing the audit reports. By completing the audit work programs, an internal auditor should be able to reach conclusions that satisfy internal audit objectives. Work programs normally include procedures for:

- Surprise audits as appropriate.
- Control over records selected for an audit.
- Review and evaluation of policies, procedures, and control systems.
- Risk assessments.
- Review of laws, regulations, and rulings.
- Sample selection methods and results.
- Verification of selected transactions or balances through:
  - Proof of subsidiary records/ledgers to related general ledger/control records.
  - Examination of supporting documentation.
  - Direct confirmation and appropriate follow-up for exceptions.
  - Physical inspection.

As part of audit work programs, auditors generally use **sampling methods and techniques** to select, verify, and test transactions, controls, and account balances for the period covered by the audit review. The audit work program should determine the objectives of testing, the procedures to meet the objectives, and how many items to review (i.e., all items in a group or a sample of items). When auditors choose to review a sample, they must decide whether to use statistical or non-statistical sampling methods. Auditors often use non-statistical sampling for small populations when internal controls are effective and it is not cost-effective to use statistical sampling. Auditors use statistical sampling methods when quantification is appropriate and they want to infer with a certain degree of reliability and precision that the sample's characteristics are indicative of the entire population. In either case, the auditor determines a representative sample size based on relevant factors, selects a representative sample, applies audit procedures, evaluates results, and documents conclusions. There are no hard and fast rules regarding the appropriate size of a "representative sample." Published tables provide statistical sample sizes based on desired precision and reliability levels. When assessing audit sampling processes, supervisors will review the auditor's documentation relating to sampling objectives, including procedures for establishing sampling objectives, defining

population and review characteristics, determining sample size, selecting sample methodology, and evaluating sample results/findings.

4.3.7. **Audit reports** that tell the Board and Directors whether a department, division, or activity adheres to policies and procedures; whether operating processes and internal controls are effective; and what corrective action has been taken or must be taken. The auditor must communicate findings and recommendations to appropriate parties and distribute audit reports as soon as practical after completing the related work. Audit work papers should adequately document and support these reports. Internal audit reports should be structured to fit the needs of an institution's internal audit function and the areas being audited. The reports usually contain the following information:

- A concise summary of key results and conclusions.
- The audit's scope and objectives.
- Audit results, including any summary rating.
- Recommendations, if any, including benefits to be derived.
- Management's commitments to correct material weaknesses.

After completing an audit, the internal auditor usually meets with the manager of the department to review the draft audit report, correct any inaccurate information, and reach agreement on management's commitments and actions. A final audit report is then distributed to Directors and officials who have the responsibility and authority to implement any suggested corrective actions.

4.3.8. **Follow-up activities** that allow internal auditors to determine the disposition of any agreed-upon actions and to focus future audit activities on new areas. The auditors should perform follow-up activities promptly and report the results to the Board or its auditing committee. Follow-up generally consists of first obtaining and reviewing Directors' response and then confirming that corrective action has been timely and effective.

4.3.9. **Professional development programs** for the institution's audit staff. Such programs should offer opportunities for continuing education and professional development through orientation programs, in-house training, and external training (e.g., formal or self-study courses offered by industry associations, professional societies, or other vendors).

4.3.10. **Quality assurance programs** which evaluate audit operations. In such programs, internal or external parties periodically assess the performance of the internal auditor or audit department. The auditor or audit department's performance is normally measured against established standards, the audit charter or mission statement, and any other criteria determined appropriate for the internal audit function.

4.4. **Independence**

4.4.1. Internal auditors must be independent of the activities they audit so that they can carry out their work freely and objectively. They must render impartial and unbiased judgments. The internal auditor or the manager of internal audit should report directly and regularly to the Board.

4.4.2. The Board is responsible for delegating the authority necessary to effectively allow internal auditors to perform their job. Auditors must have the power to act on their own initiative in all departments, divisions, and functions in the institution; to communicate directly with any personnel; and to gain access to all records, files, or data necessary for the proper conduct of the audit. Clear communication between the Board, the internal

auditors, and Directors is critical for timely identification and correction of weaknesses in internal controls and operating management. In some institutions, the head auditor reports to the Directors, rather than the Board, for day-to-day administrative issues. In such a case, the Board must take extra measures to ensure that the relationship does not impair or unduly influence the auditor's independence.

4.5. **Competence**

4.5.1. Internal audit staff should possess the necessary knowledge, skills, and disciplines to successfully implement the audit program in a proficient and professional manner. The evolving roles of internal auditors require that they expand their skills in analysis, technology, decision-making, and communication. At a minimum, members of the audit staff should:

- Have appropriate education and/or experience.
- Have organizational and technical skills commensurate with the responsibilities assigned.
- Be skilled in oral and written communication.
- Understand accounting and auditing standards, principles, and techniques.
- Recognize and evaluate the materiality and significance of deviations from sound business practices.
- Recognize existing or potential problems and expand procedures as applicable.

4.5.2. It is important for each member of the internal audit staff, including the audit manager, to commit to a program of continuing education and development. Courses and seminars offered by colleges, bank groups, or audit industry groups afford many opportunities for maintaining audit skills and proficiency. In-house training programs, work experience in various departments of an institution, and reviewing current literature on auditing and banking also are means to maintain and enhance auditing skills.

4.6. **Operations of Foreign Banking Organizations**

4.6.1. The internal audit function of a foreign banking organization (FBO) should cover its Macedonian operations in its risk assessments, audit plans, and audit programs. The internal audit of the Macedonian operations normally is performed by its Macedonian domiciled audit function, head-office internal audit staff, or some combination thereof. Internal audit findings (including internal control deficiencies) should be reported to the Directors of the Macedonian operations of the FBO and the audit department of the head office. Significant, adverse findings also should be reported to the head office's Directors and the Board or its auditing committee.

5. External Audit Function

5.1. **Overview**

5.1.1. A well-planned external audit complements the institution's internal audit function, strengthens internal controls, and contributes to safe and sound operations. An effective external audit function provides the Board and Directors with:

- Reasonable assurance about the effectiveness of internal controls over financial reporting, the accuracy and timeliness in recording transactions, and the accuracy and completeness of financial and regulatory reports.

- An independent and objective view of an institution's activities, including processes relative to financial reporting.
- Information useful to Board and Directors in maintaining an institution's risk management processes.

5.1.2. External auditors often provide services throughout the year, including in-depth reviews of the operations of specific departments, such as commercial loans or data processing. Such reviews often focus on operational procedures, personnel requirements, or other specific areas of interest. Institutions employ external auditors to help management in specialized fields such as taxes and management information systems. External auditors may, when requested, also help institutions prepare or review regulatory reports.

5.1.3. An institution's Board should require external auditors to submit engagement letters before commencing audit work. The letters usually reflect preliminary discussions between the institution's Board or Directors and the external auditor. Engagement letters stipulate, among other things, the audit's purpose, its scope, the period to be covered, and the reports the external auditor will develop. Schedules or appendixes may accompany the letter to provide more detail. The letter may briefly describe procedures to be used in specific areas. In addition, if the scope of the audit is limited in any way, the letter may specify procedures that the auditors will omit. Additionally, the letter should specify if the auditor is expected to render an opinion on the institution's financial statements.

5.1.4. After an audit has taken place, external auditors often make suggestions for improving the institution's internal control structure. They normally do so in a letter addressed to Directors and the audit committee (usually referred to as a "management letter") that is separate from the audit report.

5.1.5. The NBRM encourages communication and cooperation between Directors, external auditors, and the NBRM supervision team. Communication and cooperation can benefit all parties by helping to improve the quality of internal controls and supervision while promoting a better understanding of the NBRM's and the external auditor's policies and practices.

5.2. Types of External Auditing Programs

5.2.1. In addition to the required annual opinionated audit, there are two additional types of external audits available to the Board when analyzing an institution's external auditing needs. All three types are discussed below.

- **Financial statement audit by an independent auditing firm.** External auditing is traditionally associated with independent audits of an institution's financial statements. An independent audit of financial statements is designed to ensure that financial reports are prepared in accordance with generally accepted accounting principles. Independent financial statement audits are performed in accordance with generally accepted auditing standards and their scope is sufficient to enable an independent auditing firm to express an opinion on the institution's financial statements. All institutions are required to have an independent auditing firm audit their financial statements annually.

- **Reporting by an independent auditing firm on an institution's internal control structure governing financial reporting.** This type of audit examines and reports on management's assertion concerning the effectiveness of the institution's internal controls over financial reporting. The auditing firm's attestation may cover all internal controls relating to annual financial statement preparation or specified schedules of regulatory reports. Under this engagement, management documents its assessment of internal controls and prepares a written assertion specifying the criteria used and opining on control effectiveness. The auditing firm performs the attestation in accordance with generally accepted standards for attestation engagements.
- **Balance sheet audit performed by an independent auditing firm.** In this type of audit, an auditing firm examines and reports only on the institution's balance sheet. As with financial statement audits, the auditing firm audits in accordance with generally accepted auditing standards, but does not examine or report on whether statements of income, changes to equity capital, or cash flow are fairly presented.

5.3. **Audit Opinions**

5.3.1. An independent auditing firm's standard report consists of three paragraphs. The first paragraph identifies the financial statements and differentiates management's responsibilities from those of the auditor. The second, or scope, paragraph describes the nature of the audit and explicitly acknowledges that an audit provides reasonable assurance about whether the financial statements are free of material misstatement. The third paragraph expresses the auditing firm's opinion. There are four types of opinions: unqualified, qualified, adverse, and a disclaimer of opinion.

- An independent auditing firm issues an **unqualified opinion** when financial statements present fairly, in all material respects, the financial position, results of operations (i.e., earnings), and cash flows of the entity in conformity with generally accepted account practices. Certain circumstances, while not affecting the auditing firm's unqualified opinion on the financial statements, may require that the auditor add an explanatory paragraph to the report. These circumstances include, but are not limited to, (1) the auditor basing an opinion in part on the report of another auditor and (2) accounting principles changing materially between reporting periods.
- Independent auditing firms use a **qualified opinion** when the financial statements present fairly the condition of the institution except in the matters pertinent to the qualification. Independent auditing firms use such an opinion when (1) a lack of information or restrictions placed upon the audit prevent them from expressing an unqualified opinion or (2) the financial statements contain a material departure from generally accepted accounting practices.
- Independent auditing firms use an **adverse opinion** when the matter taken exception to is so substantive that the financial statements do not present fairly the financial condition of the institution. This opinion also covers financial statements that do not conform to generally accepted accounting practices.
- Independent auditing firms issue a **disclaimer of opinion** when the institution's management or circumstances restrict in a material way the scope of the auditors' examination.

5.3.2. When Independent auditing firms issue a qualified opinion, adverse opinion, or disclaimer of opinion, they should set forth in the report all material reasons for issuing that particular opinion.

5.4. **Special Situations**

5.4.1. *Institutions presenting supervisory concern.* Sometimes weaknesses in internal controls or management information systems adversely affect financial reporting or contribute to a material deterioration in an institution's safety and soundness. When this happens, the NBRM may require the institution to engage independent external auditors, at the institution's expense, and provide the NBRM copies of audit reports, including management letters, and to notify the NBRM prior to any meetings with external auditors.

5.4.2. *Holding company subsidiaries.* When an institution is owned by a holding company, it may be appropriate for the NBRM to address the scope of the institution's external auditing program in the context of the institution's relationship to the consolidated group. In some cases, however, a subsidiary bank may have activities involving significant risks that are not covered under the procedural scope of the holding company's consolidated audit. In such cases, the institution's Board should consider strengthening internal auditing procedures or implementing an appropriate alternative external auditing program to cover those activities. External auditing might pertain only to the consolidated financial statements of a holding company. In those circumstances, the NBRM may ask the external auditor to describe the audit procedures used to test transactions from subsidiary institutions' balance sheets and income statements. If the NBRM believes transaction testing may not have been sufficiently extensive, it will discuss the matter with the institution and its external auditor.

5.5. **Independence**

5.5.1. Independent auditing firms are subject to the professional standards adopted by their accounting societies or licensing agency. Traditionally, these standards have defined independence as the ability to act with integrity and objectivity. When an independent auditing firm expresses an opinion on financial statements, not only the fact, but also the appearance, of integrity and objectivity is of particular importance. For this reason, auditing firms are prohibited from expressing such an opinion when relationships exist which might pose such a threat to integrity and objectivity as to jeopardize its independence. These relationships fall into two general categories: (a) certain financial relationships with clients, and (b) relationships in which the auditing firm is virtually part of management or an employee under management's control.

5.5.2. The NBRM requires that all public auditing firms that audit licensed institutions be independent. Such firms can neither have, nor commit to acquire, a direct financial interest or any material indirect financial interest in the institution or related entities that they are auditing, nor can they be connected as an organizer, underwriter, voting trustee, director, officer, or employee with such an institution or related entities.

5.5.3. Auditors should disclose, in writing, all relationships with the institution and its related entities that could affect the auditor's objectivity and also confirm that it is independent.

5.6. **Competence**

5.6.1. Independent auditing firms are required to perform their audits in accordance with generally accepted auditing standards. There are three categories of standards: general standards, standards of fieldwork, and standards of reporting.

- **General standards** require that an auditor be proficient, having had adequate training in auditing and accounting. The auditor must also be independent in attitude in all matters relating to the assignment. Audits must be conducted using due professional care in the performance of the audit and the preparation of the report. Auditors must have basic education in accounting and auditing, and routinely participate in continuing education programs.
- **Fieldwork standards** require the auditor to adequately plan the audit and to properly supervise any assistants. The auditor must have sufficient understanding about the institution's internal control structure to plan the audit and to determine the nature, timing, and extent of testing to be performed. The scope of the audit must be sufficient to allow the auditor to obtain enough information through inspection, observation, inquiries, and confirmations to draw a reasonable opinion regarding the financial statements under audit.
- **Reporting standards** require the auditor to state whether the financial statements are presented according to generally accepted accounting practices and to identify circumstances in which generally accepted accounting practices have not consistently been followed. The auditor must ensure that the financial statements or the audit report provide adequate disclosures of material items. The report must express an opinion regarding the financial statements taken as a whole or to state that an opinion cannot be expressed. If an overall opinion cannot be expressed, the auditor must state the reasons. The report must give a clear indication of the auditor's work and the degree of responsibility the auditor is taking when his or her name is associated with the financial statements.

5.7. **Information System/Technology Audits**

5.7.1. There are no specific statutory requirements for information system (IS) or technology audits. However, institutions and their service providers are expected to conduct independent assessments of risk exposures and internal controls associated with the acquisition, implementation, and use of information technology. These assessments can be performed by the institution's own internal or external auditor, a service provider's internal auditor, a third party, or any combination of these. IS audits have two primary goals:

- Verify the adequacy of technology risk controls.
- Validate the accuracy of automated information.

5.7.2. IS audits should address the risk exposures in information technology throughout the institution and at its service provider(s). The audits should cover such areas as user and data center support and delivery, local and wide area networks, telecommunications, information security, electronic data interchange, development and acquisition, and contingency planning, as applicable.

5.7.3. The audit usually validates the accuracy of automated information during departmental audits. It involves such activities as transaction testing, reconciling input with output, and balancing subsidiary records to general ledger control totals. These validation procedures can be performed either "around the computer" using source documents and automated reports or "through the computer" by using independent audit software to independently test the production processing environment.

5.8. **Policy on Coordination and Communication Between External Auditors and Supervisors**

5.8.1. The NBRM desires to improve the coordination and communication between external auditors and supervisors. The discussion below provides guidelines regarding information that should be provided by institutions to their external auditors and meetings between external auditors and supervisors

5.8.2. ***Coordination of External Audits and Supervisors.*** In most cases, the NBRM provides institutions with advance notice of the starting date(s) of examinations. When notified, institutions are encouraged to promptly advise their external auditors of the date(s) and scope of supervisory examinations in order to facilitate the auditors' planning and scheduling of audit work. The external auditors may also advise the NBRM regarding the planned dates for the auditing work on the institution's premises in order to facilitate coordination with the supervisors.

5.8.2.1. Some institutions prefer that audit work be completed at different times from examination work in order to reduce demands upon their staff members and facilities. On the other hand, some institutions prefer to have audit work and examination work performed during similar periods in order to limit the effect of these efforts on the institutions' operations to certain times during the year. By knowing in advance when examinations are planned, institutions have the flexibility to work with their external auditors to schedule audit work concurrent with examinations or at separate times.

5.8.3. ***Other Information Provided By the Institution.*** Consistent with best practices, an institution should provide its external auditors with a copy of certain reports and supervisory documents, after receiving prior permission from the NBRM, including:

- The most recent regulatory reports;
- The most recent examination report and pertinent correspondence received from its regulator(s);
- Any supervisory memorandum of understanding with the institution that has been put into effect since the beginning of the period covered by the audit;
- Any written agreement between NBRM and the institution that has been put into effect since the beginning of the period covered by the audit; and
- A report of:
    - Any actions initiated or undertaken by the NBRM since the beginning of the period covered by the audit; and
    - Any money penalty assessed under any other provision of law with respect to the institution or any institution-affiliated party, since the beginning of the period covered by the audit.

5.8.4. ***External Auditor Attendance at Meetings between Directors and Supervisors.*** Generally, the NBRM encourage auditors to attend examination exit conferences upon completion of field work or other meetings between supervisors and an institution's Directors or Supervisory Board (or a committee thereof) at which examination findings are discussed that are relevant to the scope of the audit.

5.8.5. When other conferences between supervisors and Directors are scheduled (i.e., that do not involve examination findings that are relevant to the scope of the external auditor's work), the institution shall first obtain the approval of the NBRM in order for the auditor to attend the meeting. This policy does not preclude the NBRM from holding meetings with the Directors of institutions without auditor attendance or from requiring that the auditor attend only certain portions of the meetings. Institutions should ensure that their external auditors are informed in a timely manner of scheduled exit conferences and other relevant meetings with supervisors and of the NBRM policies regarding auditor attendance at such meetings.

5.8.6. ***Meetings and Discussions between External Auditors and Supervisors.*** An auditor may request a meeting with the NBRM after the completion of examinations in order to inquire about supervisory matters relevant to the institution under audit. External auditors should provide an agenda in advance to the NBRM. The NBRM will generally request that Directors of the institution under audit be represented at the meeting. In this regard, supervisors generally will only discuss with an auditor examination findings that have been presented to the institution's Directors.

5.8.7. In certain cases, external auditors may wish to discuss with the NBRM matters relevant to the institution under audit at meetings without the representation from the institution's Directors. External auditors may request such confidential meetings with the NBRM, and the NBRM may also request such meetings with the external auditor.

5.8.8. ***Confidentiality of Supervisory Information.*** While the policies of the NBRM permit external auditors to have access to the previously mentioned information on institutions under audit, institutions and their auditors are reminded that information contained in examination reports and supervisory discussions -- including any summaries or quotations -- is confidential supervisory information and must not be disclosed to any party without the written permission of the NBRM. Unauthorized disclosure of confidential supervisory information may subject the auditor to civil and criminal actions and fines and other penalties.