M-Aud

Comptroller of the Currency
Administrator of National Banks

# Internal and External Audits

## Comptroller's Handbook

April 2003

M

Management

# Internal and External Audits Table of Contents


**Introduction ..... 1**

**Board and Management Responsibilities ..... 4**

**Audit Programs ..... 7**

**Internal Audit Function ..... 12**
- Oversight and Structure ..... 13
- Risk Assessment and Risk-based Auditing ..... 14
- Internal Audit Program ..... 18
- Independence and Competence ..... 23
- Consulting Activities ..... 24

**Outsourcing of Internal Audit ..... 25**
- Oversight Responsibilities ..... 26
- Written Contracts ..... 26
- Guidelines ..... 28

**Directors' Examination ..... 31**

**External Audit Function ..... 32**
- Statutory Requirements ..... 33
- Independence ..... 35
- Competence ..... 37
- Types of External Auditing Programs ..... 38
- Audit Opinions ..... 40
- Other Communications Between the Bank and the External Auditor ..... 41
- Special Situations ..... 42

**OCC Assessment of Audit Functions ..... 44**
- Assessment Elements ..... 45
- Supervisory Reviews ..... 47
- Validation ..... 49
- Completing the Audit Function Review ..... 56

# Introduction

This booklet discusses the OCC's expectations for effective audit functions and will help examiners and bankers assess the quality and effectiveness of internal and external audit programs appropriate for a bank's size, complexity of activities, scope of operations, and risk profile. It describes the roles and responsibilities of the board of directors and management, identifies effective practices for internal and external audit programs, and details examination objectives and procedures that OCC examiners will use to assess the adequacy of a national bank's audit programs. This booklet's appendices provide additional guidance on internal and external audits. The examination procedures and other reference material in this booklet supplement the basic audit guidance in the "Community Bank Supervision" and "Large Bank Supervision" booklets of the *Comptroller's Handbook*.

**Underlying Principles**

Well-planned, properly structured auditing programs are essential to effective risk management and adequate internal control systems.[1] Effective internal and external audit programs are also a critical defense against fraud and provide vital information to the board of directors about the effectiveness of internal control systems.

The basic guidelines governing OCC expectations for a national bank's audit programs are:

- The board of directors and senior management cannot delegate their responsibilities for establishing, maintaining, and operating effective audit programs.

- For bank audit programs to be effective, they must be performed by independent and competent staff who are objective in evaluating the bank's control environment.

[1] For a detailed discussion of internal controls, please refer to the "Internal Control" booklet (dated January 2001) of the *Comptroller's Handbook*. The "Internal Control" booklet supplements the control core assessment standards in the "Large Bank Supervision" and "Community Bank Supervision" booklets of the *Comptroller's Handbook*. Further guidance on assessing controls can also be found in other *Comptroller's Handbook* booklets that address specific banking products and activities.

- Bankers and examiners must each validate the adequacy of a national bank's audit programs.

OCC examiners will assess and draw conclusions about the adequacy of a bank's overall audit function as part of every supervisory cycle. This will include some level of audit validation, including verification procedures as necessary. The conclusions could significantly influence the scope of other supervisory activities for the bank. The OCC will expand supervisory activities of applicable areas if significant issues or concerns about the quality or extent of auditing programs or the control environment are.

**Laws, Regulations, and Policy Guidance**

The following laws and regulations[2] establish minimum requirements for internal and external audit programs and are referenced throughout this booklet:

- 12 CFR 9, Fiduciary Activities of National Banks, establishes an annual audit requirement for national banks acting in a fiduciary capacity and defines requirements for a bank's fiduciary audit committee**.**

- 12 CFR 21.21, Bank Secrecy Act Compliance, establishes requirements for a board-approved ongoing Bank Secrecy Act (BSA) compliance program that includes, in part, provisions for independent testing by bank personnel or outside parties for compliance with BSA.

- 12 CFR 30, Safety and Soundness Standards, establishes operational and managerial standards for internal audit systems for insured national banks.

- 12 CFR 363, Annual Independent Audits and Reporting Requirements, applies to banks, thrifts, and holding companies having $500 million or more in total assets. Part 363 establishes requirements for independent financial statement audits; timing, contents, and types of management and auditor reporting; and the board of director's audit committee structure and responsibilities. Public accountants engaged by banks subject to Part 363 must adhere to AICPA and SEC independence rules.

[2] Appendix A contains a more detailed description of the requirements of these laws and regulations. For complete details, refer to the full text of published laws and regulations.

- 17 CFR 210, 228, 229, and 240 are U.S. Securities and Exchange Commission (SEC) regulations that apply to publicly held companies. The regulations establish requirements for independent financial statement audits; qualifications and independence of public accountants; and qualifications, responsibilities, and disclosures required of audit committees. National banks subject to the public and periodic filing and reporting requirements of 12 CFR 11 and 12 CFR 16.20[3] and bank holding companies that have their securities registered with the SEC are subject to these regulations.

- The Sarbanes-Oxley Act of 2002 specifically addresses auditor independence. It prohibits the independent public accountant who performs a company's financial statement audit from performing certain non-audit services, of which the company's internal audit is considered one. The OCC expects national banks whose securities are registered with the OCC and who file periodic reports under 12 CFR 11 and 12 CFR 16.20 to comply with the act and any SEC regulations issued pursuant to the act. National banks subject to 12 CFR 363 are expected to comply with the act's auditor independence provisions and any SEC regulations issued pursuant thereto.

The federal financial regulatory agencies have also issued three interagency policy statements on internal and external audit functions:

- "Interagency Policy Statement on the Internal Audit Function and Its Outsourcing," issued as OCC 2003-12.

- "Interagency Policy Statement on External Auditing Programs of Banks and Savings Associations," issued as OCC 99-37, and

- "Interagency Policy Statement on Coordination and Communication Between External Auditors and Examiners," issued as Banking Bulletin 92-42

[3] Part 11 banks have the same reporting obligations as those companies with a class of securities registered under the Securities Exchange Act of 1934 (filing of periodic reports such as Form 10K, Form 10Q, proxy materials, Form 8K etc.). 12 CFR Part 16.20 is a similar requirement of a bank offering securities under the Securities Act of 1933, subjecting them to reporting under Section 15(d) of the SEC Act (i.e., filing Form 10K, Form 10Q and Form 8K).

The policy statements discuss characteristics of effective internal and external audit programs, director and senior management responsibilities, and communication between external auditors and examiners.

## Board and Management Responsibilities

### Directors

The board of directors is responsible and accountable for establishing, overseeing, and maintaining audit functions that:

- Effectively test and monitor internal controls,
- Ensure the reliability of the bank's financial statements and reporting, and
- Satisfy statutory, regulatory, and supervisory requirements.

The directors must ensure that the 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**.**

Directors 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 internal auditors, other bank personnel, or external third parties. Board or audit committee minutes should reflect decisions regarding audits, such as external audit engagement terms (including any decision to forgo an external audit), the type of audits to be performed, or why an audit of a particular area is not necessary.

Directors should be aware of significant risk and control issues for the bank's operations, especially for new products, emerging technologies, information systems, electronic banking, and new or revised laws and regulations. Common 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 and accounting records, a lack of standards and controls for end-user systems, and

increased complexity of contingency plans and information system recovery plans.

**Audit Committee**

Establishing an independent audit committee to oversee and maintain audit functions is a good, and sometimes required, practice. 12 CFR 363 requires national banks with more than $500 million in assets to have an audit committee consisting entirely of outside directors that are independent of bank management. The OCC encourages all other national banks to have a similarly structured audit committee. In small banks where this may not be practical, outside directors should be at least a majority of the audit committee. The SEC and the Sarbanes-Oxley Act of 2002 also impose specific requirements on audit committees aimed at strengthening their independence, effectiveness, and accountability. Audit committees of national banks subject to 12 CFR 363 or the filing and reporting requirements of 12 CFR 11 and 12 CFR 16.20 should comply with SEC rulings and the Sarbanes-Oxley Act, as appropriate.

Audit committee[4] responsibilities should encompass:

- Reviewing and approving audit strategies, policies, programs, and organizational structure, including selection/termination of external auditors or outsourced internal audit vendors.

- Establishing schedules and agendas for regular meetings with internal and external auditors. The committee should meet at least four times a year.

- Supervising the audit function directly to ensure that internal and external auditors are independent and objective in their findings.

- Working with internal and external auditors to ensure that the bank has comprehensive audit coverage to meet the risks and demands posed by its current and planned activities.

- Significant input into hiring senior internal audit personnel, setting compensation, reviewing annual audit plans/schedules, and evaluating the internal audit manager's performance.[5]

[4] The board of directors may fulfill audit committee responsibilities if the bank is not statutorily required to have an audit committee.

- Retaining auditors who are fully qualified to audit the kinds of activities in which the bank is engaged.

- Meeting with bank examiners, at least once each supervisory cycle, to discuss findings of OCC reviews, including conclusions regarding audit.

- Monitoring, tracking, and, where necessary, providing discipline to ensure effective and timely response by management to correct control weaknesses and violations of law or regulation noted in internal or external audit reports or in examination reports.

For national banks with fiduciary activities, 12 CFR 9 outlines specific responsibilities and membership requirements for the board of directors' audit committee (or fiduciary audit committee).

A formal audit committee charter is a good means to set forth the objectives, authorities, responsibilities, and organization of the committee. A charter can serve to remind current committee members of their duties and responsibilities and to familiarize new committee members with them. The audit committee should review, update as warranted, and approve the charter on an annual basis. The charter should be approved by the board of directors and shared with internal auditors and external auditors.

The formality and extent of an institution's internal and external audit programs depend on the bank's size, complexity, scope of activities, and risk profile. The audit committee should assign responsibility for the internal audit function to someone (generally referred to as the manager of internal audit or internal audit manager) who understands the function, is independent of areas under review, and has no responsibility for operating the system of internal controls. Some small banks do not have either a formal internal or external audit program. Instead, internal audit responsibilities may lie with an officer or employee designated as a part-time auditor or with employees who may share the audit tasks. In other banks, the board, through its annual director's examination, performs the internal or external audit function.

[5] For example, the performance criteria could include the timeliness of each completed audit, comparison of overall performance to plan, and other measures.

**Audit Management**
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.

## Audit Programs

Effective audit programs should:

- Provide objective, independent reviews and evaluations of bank activities, internal controls, and management information systems (MIS).

- Help maintain or improve the effectiveness of bank 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.

Internal audit programs (including those that are outsourced or co-sourced to third-party vendors) are traditionally associated with:

- Independent and objective evaluation and testing of a bank's overall internal control system (i.e., operational and administrative controls beyond those associated with financial statement preparation),

- Ensuring the safeguarding and proper recording of a bank's assets, and

- Determining compliance with laws, regulations, and established bank policies and practices.[6]

[6] The Institute of Internal Auditors defines internal auditing as "an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes."

Internal audit programs are a bank's primary mechanism for assessing controls and operations and performing whatever work is necessary to allow the board and management to accurately attest to the adequacy of the bank's internal control system.

External audit programs typically focus on financial reporting and associated processes and matters that might result in material weaknesses, financial internal control weaknesses, or misstatements that compromise a bank's financial statements. Outsourced/co-sourced internal audit activities are not considered external audits.

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

National bank audit programs should include aspects of 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 bank 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. In small banks, individuals who have operational responsibilities may perform the internal audits in areas for which they have no responsibilities or involvement. 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.

***Operational audits*** generally include procedures to test the integrity of accounts, regulatory reports, management information systems, and other aspects of operations as part of the review of a specific department, division, or area of a bank. This type of audit includes a review of policies, procedures, and operational controls to determine whether risk management, internal controls, and internal processes are adequate and efficient. Because a bank significantly relies on information technology (IT) for transaction testing, record storage, and communications, IT audit coverage (more fully described below) is a significant component of operational audits. Operational audits may also include a review of the department's compliance with bank policies and procedures.

***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 public accountants (IPAs)[7] 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 (GAAP). An internal auditor may assist the external auditors during an annual financial statement audit or perform some financial auditing on his/her own throughout the year.

***Regulatory compliance audits*** determine whether the bank is complying with applicable laws and regulations. A consumer compliance audit is a typical example of this type of audit, but a compliance audit may also cover commercial laws and regulations such as those dealing with insiders and affiliates. The audit of consumer compliance, as part of a bank's compliance management system, enables the board of directors and senior management to monitor the effectiveness of a bank's compliance program. The compliance audit's formality and structure depends on a bank's size, the nature of its activities, and its risk profile, including compliance risk profile. In some large banks, for example, compliance audits are done on a systemic basis or on a business-by-business basis appropriate for the bank's structure. The function may be under the auspices of a bank's internal audit department, or it may be a direct responsibility of a bank's compliance division.

The audit tests compliance with all applicable consumer privacy and protection laws and regulations and BSA, anti-money laundering (AML), and Office of Foreign Assets Control (OFAC) regulatory requirements, as well as staff adherence to established policies and procedures. BSA audits should provide for independent testing by the internal audit staff or an outside party. The audit should address all bank products and services, all aspects of applicable operations, and all departments (such as trust and private banking), the bank's internet site, electronic banking, and branch locations. Someone qualified to conduct regulatory reviews should perform the audit. The audit

[7] Independent public accountants (IPAs) are accountants who are independent of the institutions they audit. They are registered or licensed by individual state boards of accountancy to practice public accounting, hold themselves out as public accountants, and are in good standing under the laws of the state or other political subdivision of the United States in which their home office is located.

should appropriately address compliance risk exposure, allowing for more frequent and intense reviews of high and moderate risk areas.

***Information technology (IT) audits*** assess the controls, accuracy, and integrity of an institution's electronic data processing and computer areas. National banks 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. The bank's internal auditor, external auditor, a service provider's internal auditor, a third party or any combination of these can perform these assessments. IT audit often includes both targeted audits of IT functions and integrated reviews of IT functions as part of other operational audits.

IT audits should address the risk exposures inherent in IT systems and applications throughout the institution and at its service providers. IT audits should cover, as applicable, such areas as:

- User and data center support and delivery,
- Local and wide area networks,
- Telecommunications,
- Information security,
- Electronic data interchange,
- Development and acquisition,
- Business continuity and contingency planning,
- Data integrity,
- Confidentiality and safeguarding of customer information, and
- Technology management.

IT audits might also include a review of computer and client/server systems, end-user reports, electronic funds transfer, and service provider activities.

The audit scope usually validates the accuracy and integrity 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, a critical aspect of operational audits, 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.

IT audits must cover the processing of transactions by servicing organizations. They usually do so in special audit reports produced in compliance with AICPA SAS 70, "Reports on the Processing of Transactions by Servicing Organizations." A SAS 70 report establishes whether policies and procedures are suitably designed to achieve control objectives, were in effect as of a specific date, and were working well enough to reasonably ensure that control objectives were achieved. Bankers and examiners should not rely solely on SAS 70 reports when assessing the adequacy of audit. The service provider and its existing control environment typically dictate the scope of an SAS 70 audit. Serviced banks should determine the adequacy of that scope based on the risk to their systems and information.

***Fiduciary audit*** requirements for national bank fiduciary activities are set forth in 12 CFR 9, Fiduciary Activities of National Banks. The regulation generally requires national banks with fiduciary powers to perform a suitable audit of all significant fiduciary activities during each calendar year. The board of directors' minutes must note the audit results, including significant actions the bank has taken as a result of the fiduciary audit.

The OCC and 12 CFR 9 do not define a "suitable audit" or establish minimum audit standards for fiduciary audits. The scope and coverage of fiduciary audits is the responsibility of the board of directors. The board should base those audit decisions on an appropriate assessment of fiduciary business risk and internal control systems.

In lieu of performing annual audits, 12 CFR 9.9(b) permits national banks to adopt a system of continuous audits. In a continuous audit system, internal or external auditors review each significant fiduciary activity discretely (activity by activity). The audit intervals should be commensurate with the nature and risk of fiduciary activities. Thus, certain fiduciary activities might receive audits at intervals of more or less than one year, as appropriate. At least once during each calendar year, the board of directors' minutes must note the results of all discrete audits performed since the last audit report, including significant actions taken as a result of the audits.

In addition to meeting the audit standards described above, the auditor may need to perform or participate in audits and issue audit reports relating to specific fiduciary activities. The auditors may also rely on audits of services performed by outside organizations for the subject bank. Activities that may require separate audit attention and reports include:

- Annual study and evaluation of internal accounting control reports of nonexempt registered transfer agents required by 17 CFR 240.17Ad-13.

- Annual audits of collective investment funds in accordance with 12 CFR 9.18(b)(6).

- Annual financial statements based on audits of proprietary mutual funds in compliance with applicable securities laws.

- Internal control audits covering the bank's performance of certain fiduciary services for other organizations.

- External control audits, using criteria in AICPA SAS 70, covering the fiduciary bank's functions that rely on the services of an outside organization.

## Internal Audit Function

The primary role of internal auditors is to independently and objectively review and evaluate bank activities to maintain or improve the efficiency and effectiveness of a bank's risk management, internal controls, and corporate governance. They do this by:

- Evaluating the reliability, adequacy, and effectiveness of accounting, operating, and administrative controls.

- Ensuring that bank internal controls result in prompt and accurate recording of transactions and proper safeguarding of assets.

- Determining whether a bank complies with laws and regulations and adheres to established bank policies.

- Determining whether management is taking appropriate steps to address current and prior control deficiencies and audit report recommendations.

Internal auditors must understand a bank's strategic direction, objectives, products, services, and processes to conduct these activities. The auditors then communicate findings to the board of directors or its audit committee and senior management.

In addition, internal auditors often have a role in merger, acquisition, and transition activities. This role may include such duties as helping the board and management evaluate safeguards and controls, including appropriate documentation and audit trails, during the bank's acquisition planning and implementation processes.

## Oversight and Structure

Institutions should conduct their internal audit activities according to existing professional standards and guidance. The IIA's "Standards for the Professional Practice of Internal Auditing" provides standards and guidance for independence, professional proficiency, scope of work, performance of audit work, management of internal auditing, and quality assurance reviews.[8] The Bank Administration Institute (BAI) has adopted the IIA's standards for certified bank auditors. The OCC expects internal auditors who are not certified or IIA members to be familiar with these or similar standards.

How the internal audit function is accomplished depends on the bank's size, complexity, scope of activities, and risk profile, as well as the responsibilities assigned to the internal auditor by the board of directors. In larger banks, a chief auditor and a full-time internal audit staff may accomplish the internal audit function. In other banks, the internal audit function may be accomplished by an employee of the bank or holding company or by an outside vendor. In many small banks, the officer or employee designated as a part-time auditor may have operational responsibilities. In any case, to maintain independence, the person responsible for accomplishing the internal audit function should be independent of whatever area is being audited and should report findings directly to the board or its audit committee.

The audit committee should position the internal audit function in the institution's organizational structure so that the function will perform its duties with impartiality and not be unduly influenced by managers of day-to-day operations. The ideal organizational arrangement is having the internal audit function report directly and solely to the audit committee regarding both

[8] Those standards and other material about the practice of internal auditing can be found at the IIA's Web site (www.theiia.org).

internal audit issues and administrative matters, e.g., resources, budget, and compensation.[9]

Some institutions might place the manager of internal audit under a dual reporting arrangement: functionally accountable to the audit committee for matters such as the design of audit plans and the review of audit scope and audit findings, while reporting to a senior executive on administrative matters. Such an arrangement potentially limits the internal audit manager's independence and objectivity when auditing the senior executive's lines of business. Thus, chief financial officer, controller, or other similar positions should generally be excluded from overseeing the internal audit activities even in a dual role. In structuring the reporting hierarchy, the audit committee should weigh this risk of diminished independence against the benefit of reduced administrative burden in adopting a dual reporting organizational structure.[10] Under a dual reporting arrangement, the internal audit function's objectivity and organizational stature is best served when the internal audit manager reports administratively to the chief executive officer.

Internal audit functions of foreign banking organizations (FBO) should cover the FBO's U.S. operations. Typically, the FBO's U.S.-domiciled internal audit function, its head office internal audit staff, or some combination of the two performs such audits. Audit findings should be reported to U.S. operations senior management and the head office audit department, with significant adverse findings reported to the head office board of directors or audit committee and senior management.

## Risk Assessment and Risk-based Auditing

The OCC, with the other federal banking regulators, encourages risk assessment and risk-based auditing for all banks. Risk assessment is a process by which an auditor identifies and evaluates the quantity of the bank's risks and the quality of its controls over those risks. 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.

---

[9] The IIA's *Practice Advisory 2060-2: Relationship with the Audit Committee* provides some good guidance regarding the roles and relationships between the audit committee and the internal audit manager.

[10] Additional guidance regarding functional and administrative reporting lines of the internal audit manager can be found in the IIA's *Practice Advisory 1110-2: Chief Audit Executive Reporting Lines*.

**An audit department cannot lose sight of or ignore areas that are rated low-risk. An effective risk-based auditing program will ensure adequate audit coverage for all of a bank's auditable activities. The frequency and depth of each area's audit should vary according to the auditor's risk assessment.**

### Program Design

Properly designed risk-based audit programs increase audit efficiency and effectiveness. The sophistication and formality of audit approaches will vary for individual banks depending on the bank's size, complexity, scope of activities, staff capabilities, 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 (i.e., the audit universe).

- Identify the activities and compliance issues within those businesses, product lines, services, and functions that the bank should audit (i.e., auditable entities).

- 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 board or audit committee approval of risk assessments or the aggregate result thereof and annual risk-based audit plans (that establish internal and external 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.

### Risk Matrix and Guidelines

An effective scoring system is critical to a successful risk-based audit program. In establishing a scoring system, directors and management 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., compliance with laws and regulations, 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
- Senior management oversight of the audit process.

Auditors or risk managers should develop written guidelines on the use of risk assessment tools and risk factors and review the guidelines with the audit or risk committee. The sophistication and formality of guidelines will vary for individual banks depending on their size, complexity, scope of activities, geographic diversity, and technology used. Auditors will use the guidelines to grade or assess major risk areas. These guidelines generally define the basis for assigning risk grades, risk weights, or risk scores (e.g., the basis could be normal industry practices or the bank'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 banks set audit cycles at 12 months or less for high-risk areas, 24 months or less for medium-risk areas, and 36 months or less for low-risk areas. However, individual judgment and circumstances at each institution will determine the length of its audit cycles.

- Guidelines for overriding risk assessments. The guidelines should specify who could override the assessments, the approval process for such overrides, and the reporting process for overrides. The override process should involve the board or its audit committee, perhaps through final approval authority or through timely notification procedures. Overrides of risk assessments should be more the exception than the rule.

- 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 bank or a bank product experiences excessive growth, if bank staff or activities change significantly, or changes to or new laws and regulations occur.

- Minimum documentation requirements to support scoring or assessment decisions.

Banks can obtain matrices, models, or additional information on risk assessments from industry groups such as the American Bankers Association, AICPA, Institute of Internal Auditors (IIA), Financial Managers Society, and many certified public accounting firms. Another resource for helping directors 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).

**Management Responsibilities**

Day-to-day management of the risk-based audit program rests with the internal auditor or internal audit manager, who monitors the audit scope and risk assessments to ensure that audit coverage remains adequate. The internal auditor or audit manager also prepares 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. Auditors and line department managers should discuss risk assessments to determine whether they are reasonable. However, the auditors, with concurrence of the board, audit committee or risk committee, should have ultimate responsibility for setting the final risk

assessment. Auditors should periodically review the results of internal control processes and analyze financial or operational data for any effect on a risk assessment or weighting. Accordingly, bank 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, changes in laws or regulations, or changes in organization or staff.

## Internal Audit Program

A national bank'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 banks' audit programs may not be as formal as those found in larger, more complex banks, all effective audit programs should include a mission statement or audit charter, risk assessments, an overall audit plan, audit cycles, audit work programs, sampling methods and techniques, audit reports, follow-up activities, professional development programs, and quality assurance programs.

**Mission Statement or Audit Charter**

The mission statement or audit charter should outline the purpose, objectives, organization, authorities, and responsibilities of the internal auditor manager, audit department, audit staff, and the audit committee. In particular, the charter should grant the audit department the initiative and authorization for direct access to any records, files, or data (including management information systems and board/committee minutes) needed to effectively examine any bank activity or entity. That authorization should also include access to and communication with any member of the bank's staff. The audit department should develop the charter and periodically review it for any needed changes. The audit committee should approve or confirm the audit charter, and the charter should be communicated throughout the bank.

**Risk Assessments**

Risk assessments should document the bank'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. The "Risk Assessment and Risk-based Auditing" section of this booklet provides further details on risk assessments.

**Overall Audit Plan**
The audit plan should detail the internal auditor's budgeting and planning processes and should describe audit goals, schedules, staffing, and reporting. Audit plans usually include:

- Overall and individual audit objectives,
- Summary risk assessments and compliance issues 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 overall 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 work performed with planned audits and audit hours and explain significant variances from the approved plan.

**Audit Cycles**
An audit cycle should identify 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 bank premises. Additionally, auditors must consider regulatory and supervisory requirements and guidelines.

**Audit Work Programs**
The audit work programs for each audit area should establish 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 bank'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 and control 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.

**Sampling Methods and Techniques**

Sampling methods and techniques are used 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 nonstatistical sampling methods. Auditors often use nonstatistical 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 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, examiners 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.[11]

**Audit Reports**

Audit reports should tell the board and management whether a department, division, or activity adheres to policies, procedures, and applicable laws or regulations, whether operating processes and internal controls are effective, and what corrective action the bank has taken or must take. 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. There are typically two types of audit reporting as described below.

*Individual internal audit reports* for audited activities should be structured to fit the needs of a bank's internal audit function and the areas being audited. The reports usually contain the following information:

- A concise summary of key results and conclusions, including identification of root causes of significant weaknesses.
- The audit's scope and objectives.
- Detailed audit results, including any overall assigned audit rating.
- Recommendations, if any, including benefits to be derived.
- Management's commitments to correct material weaknesses.

Generally, individual internal audit reports should discuss audit issues from the standpoint of:

- What the established criteria are,
- What problem currently exists,
- The root cause of any noted problem,
- What the effect of the problem is or could be, and
- Recommendations for correcting the problem.

After completing an audit, the internal auditor usually meets with the manager of the department to discuss 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 the management officials

[11] The "Sampling Methodologies" booklet of the *Comptroller's Handbook* more fully describes the concepts behind statistical sampling methods. In addition, the auditing industry (i.e., accounting firms, IIA, BAI, et al) also addresses audit sampling issues in audit manuals and other guidance.

who have the responsibility and authority to implement any suggested corrective actions.

*Board/Audit Committee reports* should be prepared as part of the internal audit manager's regular (OCC recommends at least quarterly) reporting to and discussions with the audit committee. Executive summary reports or audit information packages might include:

- Status of meeting annual audit plan;
- Activity reports for audits completed, in process, and deferred/cancelled,
- Staffing/training reports;
- Discussion of significant accounting issues and regulatory reports and findings;
- Summaries of IT and Consumer Compliance audits;
- Risk assessments or summaries thereof;
- Tracking reports for outstanding audit and control issues; and
- Other information the audit committee or internal auditor deem appropriate.

**Follow-up Activities**

Follow-up activities should 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 of directors or its audit committee. Follow-up generally consists of first obtaining and reviewing management's response and then confirming that corrective action has been timely and effective.

**Professional Development Programs**

Such programs should offer the bank's audit staff 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).

**Quality Assurance Programs**

In such programs, internal and external parties periodically assess the performance of the internal audit department to help improve audit operations and provide value to the bank.[12] The auditor's or audit department's

[12] IIA standards call for its members and certified internal auditors to have both internal and external quality assurance reviews (QAR). Information and guidance for such reviews can be found on the

performance is normally measured against bank-established standards, the audit charter or mission statement, and any other criteria determined appropriate for the internal audit function (i.e., IIA standards). Generally, quality assurance programs are more likely to be seen in large and mid-sized banks.

## Independence and Competence

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 (director) of internal audit should report directly and regularly to the board of directors. In some banks, the internal audit function may be part of a group that manages or controls the bank's overall risk-taking activities. This arrangement may be satisfactory as long as the audit function functionally reports directly to the board and retains its independence. If the internal audit manager reports to a senior executive on day-to-day administrative issues, the board must take extra measures to ensure that the relationship does not impair the auditor's independence or unduly influence the auditor's work.

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 bank; to communicate directly with any bank 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 management is critical to timely identification and correction of weaknesses in internal controls and operations.

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.

---

IIA's web site (www.theiia.org). Effective January 1, 2002, the IIA requires at least one mandatory external QAR be conducted every five years. If a bank's audit policy or charter requires adherence to IIA standards, that bank's internal audit department should follow IIA QAR guidance.

- 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.

It is important for each member of the internal audit staff, including the audit manager or director, 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. They also offer a means to become certified as bank auditors, internal auditors, or public accountants. In-house training programs, work experience in various departments of a bank, and reviewing current literature on auditing and banking are also means to maintain and enhance auditing skills.

In a small bank, internal auditing may be a one-person department. Nevertheless, the auditor should possess qualifications similar to those outlined above.

## Consulting Activities

Internal auditors are increasingly responsible for providing some degree of business advice or consultation for new products or services. They also may help the bank formulate new policies, procedures, and practices and revise existing ones. These consultative types of services may benefit the overall design of new policies and procedures and improve the controls inherent in them. However, in order to ensure that appropriate independence and objectivity is maintained, internal auditors should never approve, design, or implement any operating policies or procedures resulting from or related to their advisory or consulting activities. The internal auditor should not become involved in valuation activities or other management functions.

The audit committee should oversee any consulting service activities to be performed by the internal auditor staff to ensure that internal audit resources are appropriately balanced between core audit activities and advisory/consulting services. Management should make decisions to adopt or implement recommendations resulting from internal audit advisory or consulting services. The OCC encourages internal auditors to follow the Institute of Internal Auditors' (IIA) standards and guidance related to performing consulting services.[13]

## Outsourcing of Internal Audit

Banks are increasingly contracting with independent public accounting firms or other outside professionals to perform work traditionally conducted by internal auditors. These arrangements are frequently referred to as "internal audit outsourcing," "internal audit assistance," "audit integration," "audit cosourcing," or "extended audit services." Banks generally enter internal audit outsourcing arrangements to gain operational or financial efficiencies by engaging a vendor to:

- Assist internal audit staff when the bank's internal auditors lack the expertise required for an assignment. Such assignments are most often in specialized areas such as information technology, fiduciary, mortgage banking, consumer compliance, and capital markets activities. The vendor normally performs only certain agreed-upon procedures in specific areas and reports findings directly to the bank's internal audit manager.

- Perform all or part of internal audit. In these situations, banks should maintain a manager of internal audit and, as appropriate, an internal audit staff sufficient to oversee outsourced vendor activities. The vendor usually assists the board and audit manager in determining the critical risks to be reviewed during the engagement, recommends and performs audit procedures approved by the internal auditor, and, jointly with the internal auditor, reports significant findings to the board of directors or its audit committee.

[13] The IIA's Practice Advisory 1000.C1-1, "Principles Guiding the Performance of Consulting Activities of Internal Auditors," can be found on the IIA's Web site (www.theiia.org).

## Oversight Responsibilities

In any outsourced internal audit arrangement, the bank must maintain ownership of the internal audit function and provide active oversight of outsourced activities. The board of directors and management remain responsible for ensuring that the outsourced internal audit function is competently managed.

Larger institutions and more formally structured community banks should have internal audit departments or internal audit managers oversee the outsourced vendor. Small institutions should appoint a qualified and competent employee to act as a point of contact between the bank and the vendor and to oversee the outsourced vendor (this individual may or may not be a formally designated "audit manager"). Ideally, the individual should be operationally and managerially independent of the areas being audited. This person should report directly to the audit committee for purposes of communicating internal audit issues.

Entering into an internal audit outsourcing arrangement may increase operational risk. And because the arrangement involves reliance on external third parties or it could be suddenly terminated for some reason, the board should have a contingency plan in place to mitigate any significant disruption in audit coverage. This is particularly important for high-risk areas.

## Written Contracts

All national banks engaged in outsourcing internal audit activities must execute a written contract governing the terms of the outsourcing arrangement and specifying the roles and responsibilities of both the bank and the vendor. At a minimum, the contract should address the following items:

- Define the expectations and responsibilities for both parties under the contract.
- Set the scope, frequency, and cost of the vendor's work.
- Describe responsibilities for providing and receiving information, such as the type and frequency of the vendor's reporting to the bank's audit manager, senior management, and the board or audit committee.

- Describe the process for changing the terms of the engagement, including how audit services can be expanded when significant issues arise, as well as stipulations for default and termination of the contract.

- Stipulate that the internal audit reports are the property of the bank and specify ownership of associated work papers. If the vendor retains ownership of work papers, the contract should stipulate that the bank can get copies of the vendor's work papers it deems necessary, and employees authorized by the bank will have reasonable and timely access to vendor work papers.

- State where internal audit reports and related work papers will be stored and specify a period of time (generally five years) that vendors must maintain the work papers. For electronic work papers, consideration should be given to including vendor maintenance of proprietary software to allow review by the bank and examiners.

- Note that the vendor's internal audit outsourcing activities are subject to OCC review and that examiners will be given full and timely access to all outsourced audit reports, audit programs, audit work papers, and related memorandums and correspondence.

- Establish a process (arbitration, mediation, or other means) for resolving problems and for determining who bears the cost of consequential damages arising from errors, omissions, and negligence.

- State that the vendor will not perform management functions, make management decisions, or act or appear to act in a capacity equivalent to a member of bank management or as a bank employee.

- If applicable, state that the vendor will comply with AICPA, SEC, or regulatory independence guidance.[14]

[14] Public accountants for national banks with securities registered with the OCC and national banks subject to 12 CFR 363 must follow the SEC's independence rules regarding prohibited non-audit services (including internal audit outsourcing services).

## Guidelines

Examiners assess outsourced internal audit programs using the same standards applied to in-house internal audit programs. Outsourcing arrangements create a variety of safety and soundness issues that will vary with the size, complexity, scope of activities, and risk profile of the bank, as well as the nature of the outsourcing arrangement. Accordingly, outsourcing arrangements should meet the following guidelines:

- **The arrangement maintains or enhances the quality of a bank's internal audit function and internal controls.** The directors retain ownership of internal audit and control processes. They remain responsible and accountable for ensuring that any outsourcing arrangement does not detract from the scope or quality of a bank's internal audit work, overall internal control structure, or audit and control evaluations.

  The board or its audit committee must undertake means (e.g., a well-structured quality assurance program) to ensure that vendors perform outsourced internal audit activities in accordance with engagement terms. They must ensure that the work is consistent with board-approved audit policies and audit plans, as well as board and management expectations with regard to the scope and quality of audit work. The vendor should provide the bank timely written notice of changes in a key process, changes in staffing, or any other changes affecting contracted work.

- **Key bank employees and the vendor clearly understand the lines of communication and how the bank will address internal control or other problems noted by the vendor.** The engagement of a vendor should not diminish communication between the internal audit function and a bank's directors and senior management. Results of outsourced work must be well documented, discussed with appropriate bank audit and line management staff, and reported promptly to the board of directors or its audit committee by the internal auditor, the vendor, or both jointly.

  The concept of materiality, as used in connection with financial statement audits, may not be a good indicator of which control weaknesses to report. Even if a test of transactions were to reveal a single exception, if that exception represented a violation of law and regulation, such a finding would normally be included in the final report for the audited area. Decisions not to report vendor findings to the board, audit committee, or

senior management should be the mutual decision of the internal audit manager and the vendor.

- **The board and management perform sufficient due diligence to verify the vendor's competence and objectivity before entering into the outsourcing arrangement.** The board and management must satisfy themselves that the expertise and quality of the vendor's staff is sufficient to effectively meet contractual obligations. A bank's selection of a vendor should be an informed decision based on review of the vendor's:

  – Available services (including specialized areas) and work arrangements,
  – Staff qualifications and experience,
  – Costs and benefits of services to be provided, and
  – Ability and flexibility to perform services in a timely manner.

  The bank also should obtain names of other clients served by the vendor and check references. All parties should discuss independence, objectivity, integrity, and conflict of interest standards applicable to the engagement, i.e., AICPA, IIA, and SEC.

- **The bank has an adequate process for periodically reviewing the vendor's performance and ensuring that the outside vendor maintains sufficient expertise to perform effectively throughout the life of the arrangement.** The board (directly or through its audit committee or internal audit manager) must satisfy itself that a vendor is satisfactorily completing outsourced work. They should hold the outside provider to the same standards as they would their own internal audit management and staff.

  The bank should subject the vendor to objective performance criteria, such as whether an audit is completed on time and whether overall performance meets the objectives of the audit plan, to determine the adequacy of the vendor's work and compliance with contractual and coverage requirements. The audit committee or designated bank staff responsible for vendor oversight should periodically perform an assessment and present findings to the board or audit committee, as appropriate, for review and approval.

- **The arrangement does not compromise the role or independence of a vendor who also serves as the bank's external auditor.** When one firm or vendor performs both financial statement audit services and outsourced

internal audit services for a bank, the firm or vendor risks compromising its independence by being placed in a position of appearing to audit, or actually auditing, its own work. ***Therefore, from a safety and soundness perspective and in keeping with regulatory requirements, the OCC prohibits registered national banks[15] and national banks subject to 12 CFR 363[16] (regardless of whether they are registered or not) from outsourcing internal audit work to the same external audit firm that performs a bank's financial statement audit and other attestation services.[17]***

The OCC encourages all other national banks that have financial statement audits performed by independent public accountants to follow the internal audit outsourcing prohibitions mentioned above. However, where a small national bank determines that hiring separate firms to perform internal and external audit work is not cost effective, the bank and the external auditor must pay particular attention to preserving the independence of both the internal and external audit functions. Furthermore, the board or its audit committee should document its considerations of independence issues associated with the outsourcing arrangement. They may also want to discuss the independence issues with its supervisory office before entering such an outsourcing arrangement.

The OCC will not consider the outsourcing relationship to be independent unless all parties adhere to the guidance in this section of the handbook. In addition, the bank's board or audit committee must retain ownership and accountability for the internal audit function and actively oversee the outsourced internal audit relationship. Refer to the "Interagency Policy Statement on Internal Audit and Its Outsourcing," for more details.

---

[15] National banks whose securities are registered with the OCC and that file periodic reports under 12 CFR 11 and 12 CFR 16.20. Title II, section 201(a), of the Sarbanes-Oxley Act of 2002 prohibits a registered public accountant who performs a financial statement audit for a publicly registered company from also performing specified non-audit services for that company. Internal audit outsourcing services is one of those prohibited services.

[16] National banks with total assets of $500 million or more. 12 CFR 363 guidelines (Appendix A – Guidelines and Interpretations, Paragraph 14, Independence) state that independent public accountants engaged by such a bank should meet the independence requirements and interpretations of the SEC and its staff.

[17] Until the effective date – May 6, 2004 – of the SEC's revised independence regulations (issued pursuant to the Sarbanes-Oxley Act of 2002) on non-audit services, publicly registered national banks and national banks subject to Part 363 must comply with the SEC's current independence regulation issued in November 2000 regarding non-audit services (including internal audit outsourcing services).

## Directors' Examinations

The bylaws of many national banks require that the directors have independent parties periodically examine the bank's affairs. In these cases, the board is responsible for determining that agreed-upon procedures adequately meet the bank's internal or external auditing needs. The board considers such issues as the bank's size, complexity, scope of activities, and risk profile. Agreed-upon procedures normally focus on the bank's high-risk areas and consist of more than just confirmations of loans and deposits. After reviewing the findings of this type of review, the board or audit committee draws its own conclusions about the quality of financial reporting and adequacy of internal controls.

The report of examination findings, also commonly known as a directors' examination, usually states whether the bank is in sound condition, whether internal controls are adequate, and whether the board of directors should take action to address noted issues or problems. The bank's bylaws may also require that directors or a directors' committee participate in the directors' examination at least to appraise the bank's policies and procedures and to review the directors' examination report with the auditors.

Effective directors' examinations normally focus on major risk areas and internal controls and ensure that all areas are adequately covered on a regular or rotational basis. Directors' examinations should include a review of major bank acquisitions and new products and services. They should substantially test financial integrity and internal controls and normally include:

- Account reconcilement;
- Asset verification;
- Completion of internal control questionnaires;
- Quality assessment of loans and investments;
- Verification of some or all call report data;
- Review of management information systems; and
- Checks for compliance with laws, regulations, and internal policies.

These reviews will help ensure that management is following acceptable bank policies and procedures and has instituted sound internal controls.

Independent parties selected by the board to perform directors' examinations should have sufficient knowledge and understanding of banking and the

bank's business lines. They also should know how to apply accounting and auditing principles and be familiar with the bank's information systems and technology.

## External Audit Function

An external audit program encompasses engaging an independent auditor to perform a full-scope financial statement audit, a balance-sheet-only audit, an attestation of internal controls over financial reporting, or other agreed-upon external audit procedures. Outsourced or co-sourced internal audit activities are not considered part of an external audit program.

An effective external audit function often provides the board of directors and management 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 a bank's activities, including processes relative to financial reporting.
- Information useful to directors and management in maintaining a bank's risk management processes.

**Non-audit services**
At the request of a bank's board of directors (usually through its audit committee), external auditors often provide non-audit (i.e., management advisory) 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. Banks may also engage external auditors to help management in specialized fields such as taxes and management information systems. However, if the bank is registered with the OCC or subject to 12 CFR 363, there are specific non-audit services that the external financial statement auditor cannot perform for the bank. See this booklet's section on "Independence" below.

**Engagement Letters**
The audit committee should require external auditors to submit engagement letters before commencing audit work. The letters usually reflect preliminary discussions between the bank's audit committee, senior management, and the external auditor. Engagement letters should stipulate the audit's purpose, its scope, the period to be covered, the reports the external auditor will develop, and the fees charged by the auditor for services to be performed. 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 whether the auditor is expected to render an opinion on the bank's financial statements.

**Communication**
The OCC encourages communication and cooperation between bank management, external auditors, and the OCC examination team. For specific guidelines on such communication, refer to Banking Bulletin 92-42, "Interagency Policy Statement on Coordination and Communication between External Auditors and Examiners," and the AICPA's *Audit and Accounting Guide, Banks and Savings Institutions*. Communication and cooperation can benefit all parties by helping to improve the quality of internal controls and bank supervision while promoting a better understanding of the OCC's and the external auditor's policies and practices.

## Statutory Requirements

12 CFR 363[18] and its appendix impose the following auditing, reporting, and audit committee requirements on national banks with $500 million or more in total assets:

- An independent public accountant (IPA) must audit financial statements.
- Banks must file an annual report and certain other reports with the FDIC and the appropriate OCC supervisory office.
- Banks must have an independent audit committee composed entirely of outside directors.

[18] More detailed information relating to 12 CFR 363 requirements is provided in appendix A.

- The audit committees of national banks with total assets of $3 billion or more must meet criteria that are more stringent.

- IPAs are subject to reporting, attestation, and examination requirements regarding a bank's internal control structure relating to its financial reporting procedures.

- IPAs must be enrolled in a peer review program and must file a copy of the accounting firm's peer review report with the FDIC.

- IPAs must make their audit work papers, policies, and procedures available to OCC examiners for review upon request.

While 12 CFR 363 requires national banks having $500 million or more in total assets to establish and maintain an external audit program, the OCC strongly encourages all other national banks to do so. A well-planned external audit complements the bank's internal audit function and can help strengthen financial reporting internal controls and contribute to safe and sound operations. Many of the principles of independence and competence discussed below are highlights of broader requirements set forth in the Sarbanes-Oxley Act of 2002, SEC independence rules, and the AICPA's *Professional Standards* and *Audit and Accounting Guide, Banks and Savings Institutions*. The OCC encourages examiners and bankers to consult these source documents for more detail on specific standards and for guidance concerning the role of independent accountants.

The Sarbanes-Oxley Act of 2002 contains provisions specifically directed to independent public accountants performing services for publicly registered companies (including national banks whose securities are registered with the OCC). The SEC is responsible for developing and issuing new or revised regulations to implement the act's provisions. Affected public accountants must:

- Register with the Public Company Accounting Oversight Board (PCAOB).

- Adhere to any auditing, quality control, and independence standards and rules adopted by the PCAOB.

- Refrain from performing specified non-audit services.

- Obtain pre-approval from a company's audit committee for any audit or non-audit services to be performed.

- Rotate the lead and concurring audit partner every five years.[19]

- Report to the audit committee, in a timely manner:
  - All critical accounting policies and practices to be used in the audit,
  - All alternative treatments of financial information within generally accepted accounting principles (GAAP) discussed with company management, the ramifications of such alternative disclosures or treatments, and the treatment preferred by the accountant, and
  - Other material written communications between the firm and company management.

- Refrain from performing audit services for a company if the company's senior management (chief executive officer, controller, chief financial officer, chief accounting officer, or equivalent position) was employed by the firm and participated in the audit of the company within the last 12 months.

- Attest to, and report on, management's assessment of financial reporting internal controls and procedures.

## Independence

IPAs are subject to the professional standards[20] of the national or state accounting societies or the state agency issuing their licenses. In addition, FFIEC banking/thrift agencies and the SEC require that all accounting firms that perform audit work for banks or thrifts be independent.[21] These standards and

[19] SEC rules provide that audit firms with fewer than five audit clients and fewer than ten partners can qualify for an exemption to the rotation requirement provided covered engagements are subject to and pass special reviews by the Public Company Accounting Oversight Board (PCAOB) every three years.

[20] AICPA's *Code of Professional Conduct* Rule 101 and its interpretations (refer to the AICPA's web site – www.aicpa.org – for details regarding this rule) and the AICPA's *Professional Standards* and *Audit and Accounting Guide, Banks and Savings Institutions*.

[21] *Interagency Policy Statement on Internal Audit and its Outsourcing, Interagency Policy Statement on External Auditing Programs of Banks and Savings Associations,* national banks subject to 12 CFR 363 or the filing and reporting requirements of 12 CFR 11 and 12 CFR 16.20, and

requirements focus on relationships and services (financial, employment, business, non-audit services) that pose threats, real or perceived, to an IPA's ability to act with integrity and objectivity when performing and reporting on audit or attestation work.

Banks and their external auditors should discuss and consider whether the relationship or services do or could:

- Create a conflict of interest between the bank and its accountant;

- Place the accountant in the position of auditing their own work; or

- Result in the accountant acting in the capacity of bank management or a bank employee or being in a position acting as an advocate for the bank.

A good practice is for accountants to disclose, in writing, all relationships with the bank and its related entities that could affect the accountant's objectivity, and to discuss their independence with the bank's audit committee. Relationships the IPA should discuss include those pertaining to:

- Direct or material indirect financial relationships with the bank, such as:
  - Investments in the bank or bank investment in the accounting firm,
  - Bank underwriting securities issued by an accounting firm,
  - Loans to or from the bank,
  - Savings and checking accounts in amounts exceeding FDIC insurance coverage,
  - Broker/dealer accounts,
  - Futures commission merchant accounts,
  - Credit card accounts greater than $10,000,
  - Insurance products issued by the bank, or
  - Interests in an investment company that includes the bank.

- Employment relationships between the bank and the accountant, such as:
  - The accountant being employed by the bank or serving on the bank's board or in a similar management capacity,
  - Employment of the accountant's close family members or a former employee of the audit firm at the bank in an accounting or financial reporting oversight role, or

17 CFR 210.2-01 and subsequent revisions for publicly registered companies.

  - Former bank officer, director, or employee becoming an employee of the accountant.

- Direct or material indirect business relationships with the bank or persons associated with the bank in decision-making capacities, such as an officer, director, or substantial stockholder.

- Providing non-audit services to the bank,[22] such as:
  - Bookkeeping or other services related to the bank's accounting records or financial statements,
  - Financial information system design and implementation,
  - Appraisal or valuation services, fairness opinions, or contribution-in-kind reports,
  - Actuarial services,
  - Internal audit outsourcing services,
  - Management functions, such as acting as a bank director, officer, or employee or performing decision-making, supervisory, or ongoing monitoring functions,
  - Human resources,
  - Broker/dealer, investment advisor, or investment banking services, or
  - Legal services and expert services not related to the audit.

- Providing, during an audit period for the bank, any services or products to the bank for a contingent fee or a commission or receiving from the bank any contingent fees or commissions.

## Competence

IPAs are required to perform their audits in accordance with generally accepted auditing standards (GAAS). There are three categories of GAAS standards: general standards, standards of fieldwork, and standards of reporting.[23]

---

[22] If the bank is registered with the OCC or subject to 12 CFR 363, the OCC prohibits it from using the same firm to perform both its financial statement audit and the above non-audit services. See footnote 16.

[23] Refer to SAS 1, "Codification of Auditing Standards and Procedures" of the AICPA *Professional Standards* for specific details.

**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. Certified public accountants (CPAs) must have basic education in accounting and auditing that is a prerequisite to taking the uniform CPA examination. Most states have made continuing education a requirement for renewing a CPA license. The AICPA also has continuing education requirements for its members.

**Fieldwork standards** require the auditor to adequately plan the audit and to properly supervise any assistants. The auditor must have sufficient understanding about the bank'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 GAAP and to identify circumstances in which GAAP has not consistently been followed. The auditor must ensure that the financial statements or the audit report provides adequate disclosures of material items. The report must express an opinion regarding the financial statements as a whole or must 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, if the auditor is associating his or her name with the financial statements, how much responsibility the auditor is taking for the statements.

## Types of External Auditing Programs

When the board of directors analyzes a bank's external auditing needs, it should decide which of the following types of external audits best fits the bank's needs:

- **Financial statement audit by an IPA.** External auditing is traditionally associated with independent audits of a bank's financial statements. An independent audit of financial statements is designed to ensure that financial reports are prepared in accordance with GAAP. Independent financial statement audits are performed in accordance with GAAS. Their

scope is sufficient to enable an IPA to express an opinion on the bank's (or parent holding company's consolidated) financial statements. National banks with total assets of $500 million or more are required by 12 CFR 363 to have an IPA audit their financial statements.[24] The OCC encourages all other national banks to voluntarily engage the services of an IPA to conduct audits of the bank's financial statements.

- **Reporting by an IPA on a bank's internal control structure governing financial reporting.** This type of audit examines and reports on management's assertion concerning the effectiveness of the bank's internal controls over financial reporting. The IPA's attestation may cover all internal controls relating to annual financial statement preparation or specified schedules of call reports. Under this engagement, bank management documents its assessment of internal controls and prepares a written assertion specifying the criteria used and opining on control effectiveness. The IPA performs the attestation in accordance with generally accepted standards for attestation engagements (GASAE).

- **Balance sheet audit performed by an IPA.** In this type of audit, an IPA examines and reports only on the bank's balance sheet. As with financial statement audits, the IPA audits in accordance with GAAS, but does not examine or report on whether statements of income, changes to equity capital, or cash flow are fairly presented.

- **Agreed-upon procedures.** This type of audit, carried out by bank directors or other independent parties, entails specified or agreed-upon procedural reviews of the adequacy of internal controls and the accuracy of financial information. Such an audit is commonly referred to as a directors' examination (see the "Director's Examination" section above). The independent parties can be public accountants, certified internal auditors, certified bank auditors, certified information systems auditors, bank management firms, bank consulting firms, or other parties knowledgeable about banking.

[24] A bank that is a subsidiary of a holding company can satisfy 12 CFR 363.2(a) if it relies on the audited consolidated financial statements of its holding company.

## Audit Opinions

After an audit has taken place, external auditors issue reports, audit opinions, and other communications/correspondence relative to audit findings.

An IPA's standard report generally 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 IPA's opinion.

There are four types of opinions: unqualified, qualified, adverse, and a disclaimer of opinion.[25] An IPA 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 GAAP. Certain circumstances, while not affecting the IPA'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.

IPAs use a **qualified opinion** when the financial statements present fairly the condition of the bank except in the matters pertinent to the qualification. IPAs 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 GAAP.

IPAs 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 bank. This opinion also covers financial statements that do not conform to GAAP.

[25] For specific standards governing how an IPA derives an audit opinion, examiners and bankers should refer to SAS 58, "Reports on Audited Financial Statements," in the AICPA *Professional Standards*. The AICPA's *Audit and Accounting Guide, Banks and Savings Institutions* provides additional information on audit opinions.

IPAs issue a **disclaimer of opinion** when bank management or circumstances restrict in a material way the scope of the auditors' examination.

***When IPAs 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. Examiners should assess the seriousness of issues raised, corrective actions by the board or management, and how much, if any, validation/testing they should perform. If the IPA's opinion is anything other than an unqualified opinion, examiners should meet with the IPA to determine the facts and circumstances that led to the opinion. Examiners should also promptly advise the OCC supervisory office of any adverse or disclaimer of opinion encountered.***

## Other Communications between the Bank and the External Auditor

In addition to the audit reports and opinions, external auditors typically issue or communicate other information to a bank's board or audit committee. The extent of communication varies depending on audit findings and statutory requirements. Some or all of the following information may be communicated (external auditors may issue this information in a number of communications or together in a single "management letter"):

- **Communication of internal control-related matters noted in the audit.** This is commonly referred to as the "material weakness" letter. If, during an audit, the auditor notes reportable conditions identified as material weaknesses in financial reporting internal control, the auditor may make suggestions for improving the bank's internal control structure. Statement on Auditing Standards (SAS) 60, "Communication of Internal Control Structure Related Matters Noted in an Audit," requires the auditor to communicate such matters to management, preferably in writing, and provides appropriate guidance. In some cases, an auditor may issue a "no material weakness" letter if no material weaknesses were noted involving internal control.

  If the auditor's communication is not in writing, the examiner should discuss the matter with the board of directors or its audit committee. It would be unusual that the board would not require such communications from its external auditor to be in writing. In addition to material weaknesses, the auditor may report on other conditions as noted below.

- **Communication with audit committees.** If a bank has an audit committee (or similar group formally designated to oversee financial reporting) or is subject to filing and reporting requirements under 12 CFR 11 and 12 CFR 16.20, SAS 61 requires that the auditor communicate certain information regarding the scope and results of the audit. This communication can be oral or written, but must address:
  - Auditor responsibilities under GAAS,
  - Significant accounting policies,
  - Management judgments and accounting estimates,
  - Audit adjustments and a summary of unadjusted audit differences,
  - Auditor judgments about the quality of the bank's accounting principles,
  - Other information in documents containing audited financial statements,
  - Disagreements with management,
  - Consultation with other accountants,
  - Major issues discussed with management prior to retention, and
  - Difficulties encountered in performing the audit.

  If this communication is not in writing, examiners should determine why the board or audit committee did not request a written report.

- **Confirmation of audit independence.** For banks subject to 12 CFR 11 and 16 reporting requirements, auditors are required to disclose, in writing, all relationships with the bank and its related entities that could affect the auditor's objectivity. The auditor must also confirm that they are independent in accordance with SEC requirements, and discuss their independence with the bank's audit committee.

## Special Situations

**New national banks.** As a condition of preliminary approval of a newly chartered national bank, the OCC and the FDIC normally require banks to have an annual independent external audit for a period of three years after they open. The first audit should occur no later than 12 months after the bank opens for business. The audit must be of sufficient scope to enable the auditor to render an opinion on the financial statements of the bank or consolidated holding company.

The OCC may grant exemptions from this external audit requirement to a new bank subsidiary of a bank holding company (BHC) when:

- The new bank's financial statements are included in the audited consolidated financial statements of the parent BHC;

- The sponsoring BHC is an existing holding company that has operated for three years or more under Federal Reserve Bank supervision and does not have any institutions subject to special supervisory concerns; and

- Adequate internal audit coverage will be maintained at the bank level. At a minimum, the internal audit program must evaluate the quality of internal controls, including the reliability of financial information, safeguarding of assets, and the detection of errors and irregularities.

The OCC and the FDIC will coordinate determinations about external audit exemptions consistent with the "Interagency Policy Statement on External Auditing Programs of Banks and Savings Associations," which focuses on banks holding less than $500 million in total assets. If an exemption is granted, the OCC will include that determination in its preliminary conditional approval letter. If any of the requirements listed above are not met during the first three years of the bank's operation, the OCC may withdraw the exemption at its discretion.

The OCC may also waive the external audit requirements for a new bank sponsored by an independent organizing group that is experienced in banking. A group is experienced in banking if a majority of its members have three or more years of recent and significant involvement in policy-making as directors or executive officers in federally insured institutions that the OCC finds have performed satisfactorily (the time since such experience should not exceed six months). This category may include "chain banking groups." The group must be able to demonstrate that internal expertise or other outside sources can substantially provide the benefits generally associated with an external audit. In most cases, a bank owned by a non-bank holding company does not qualify for an external audit exemption. For more information, bank directors and management should contact the OCC's licensing division staff in the appropriate district office.

**Institutions presenting supervisory concern.** Sometimes weaknesses in internal controls or management information systems adversely affect financial

reporting or contribute to a material deterioration in a bank's safety and soundness. When this happens, the OCC may require the bank to engage independent external auditors and provide the supervisory office copies of audit reports, including management letters, and to notify the bank's supervisory office prior to any meetings with external auditors.

**Holding company subsidiaries.** When a national bank is owned by a holding company, it may be appropriate for the OCC to address the scope of the bank's external auditing program in the context of the bank's relationship to the consolidated group. If the group's consolidated financial statements are audited, the OCC generally will not require the subsidiary bank to undergo separate financial statement audits.

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 bank's directors should consider strengthening internal auditing procedures or implementing an appropriate alternative external auditing program to cover those activities.

External auditing performed for banks not subject to 12 CFR 363 might pertain only to the consolidated financial statements of a holding company. In those circumstances, the examiner should ask the external auditor to describe the audit procedures used to test transactions from subsidiary banks' balance sheets and income statements. If the examiner believes transaction testing may not have been sufficiently extensive, he or she should discuss the matter with the bank and its external auditor.

## OCC Assessment of Audit Functions

Assessment of a national bank's audit functions is fundamental to the OCC's overall supervisory process and forms the basis for our control assessments. Effective bank audit functions may help:

- Leverage OCC resources,
- Establish the scopes of current supervisory activities, and
- Contribute to supervisory strategies for future supervisory activities.

The bank's examiner-in-charge (EIC) will tailor the audit review to fit examination objectives. When doing so, he or she should consider the bank's size, complexity, scope of activities, and risk profile.

Examiners responsible for audit reviews, through coordination with functional and specialty area examiners, will determine how much reliance the OCC can place on audit work. OCC examiners will assess the bank's overall audit function during each supervisory cycle (e.g., 12 or 18 months) by:

- Drawing an overall conclusion about the adequacy and effectiveness of the overall audit program and the board of directors' oversight of the audit program.

- Assigning a rating of strong, satisfactory, or weak to the overall audit program.

## Assessment Elements

Effective OCC audit assessment encompasses integration, analysis, communication, linkage, documentation, and interagency coordination. This section discusses each of these elements of an effective assessment.

**Integration**. Examiners are responsible for planning, coordinating, and integrating audit reviews, including validation, into the supervisory activities for each functional, specialty, and risk area as needed. OCC specialists should be consulted about the audit functions for complex activities and they should assist in assessing the audit of those activities. Examiners should use core assessment standards and other tools in assessing and documenting conclusions about individual areas and combining conclusions into an overall audit assessment.[26]

**Analysis**. Examiners should review audit reports and management responses, audit committee minutes and audit information packages, and supervisory findings to identify changes in the bank's risk profile, systemic control issues, or changes in audit trends, stature, or structure. This review should also include 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,

[26] Appendices E through J provide worksheets and other guidance that can assist examiners in making an overall internal audit assessment. Individual booklets of the "Comptroller's Handbook for Compliance" contain worksheets to assist examiners in determining the adequacy of consumer compliance audits.

job specifications and descriptions, directives to employees, flow charts, and internal control and risk assessments.

**Communication**. Examiners will maintain ongoing and clear communications with audit-related personnel throughout an examination or supervisory cycle. They should periodically meet with a bank's audit committee, audit management/staff (including outsourced internal audit vendors), and other bank personnel closely associated with risk control functions (e.g., risk managers, control officers). It is also vitally important that examiners establish communication lines and periodically meet with a bank's external auditors to discuss and, if warranted, review work papers associated with audit planning methodologies, risk assessment, and any required internal control attestations (Part 363 or SEC).

Examiner meetings with audit committees and internal and external audit personnel should occur as frequently as appropriate depending on the bank's size, complexity, scope of activities, and risk profile. Examination reports and other written communications to a bank will include comments about the adequacy of the bank's audit functions and summarize other appropriate findings and conclusions about audit.

**Linkage**. Examiners must link audit conclusions to assigned bank ratings, risk assessments, and supervisory strategies. In particular, examiners should link management ratings, audit component ratings in the specialty areas, and individual risk assessments directly to the quality and reliability of a bank's audit functions.

**Documentation**. Examiners should document working papers in accordance with OCC working paper guidelines (PPM 5400-8, "Examination Working Papers"). Working papers need not be voluminous, but they should leave a clear audit trail that supports findings and conclusions and allows the EIC or another reviewer to understand how conclusions were reached. Examiners will also update OCC databases and supervisory strategies to reflect supervisory assessments and follow-up.

**Interagency coordination**. Audit supervision may involve working with Federal Reserve examiners in bank holding company situations, Federal Deposit Insurance Corporation (FDIC) examiners in problem bank situations, or other functional supervisory agencies such as the SEC. In such cases, the EIC should coordinate the timing of audit reviews and share information with

the appropriate supervisory agencies. Examiners participating in joint holding company examinations should, after consultation with the Federal Reserve, communicate audit conclusions to affiliate national bank EICs.

## Supervisory Reviews

In developing the appropriate scope for audit reviews, community bank examiners will begin with the core assessment audit objectives and procedures from the "Community Bank Supervision" booklet. Large bank examiners will begin with the minimum audit standards from the "Large Bank Supervision" booklet and tailor their review of audit to fit their objectives and needs. As part of the audit reviews, examiners may need to perform additional procedures from this audit booklet to assess the audit function.

**Internal Audit Reviews**
Review of a banks' audit function should focus first on the internal audit program. Examiners should determine the program's adequacy and effectiveness in assessing controls and following up on management's actions to correct any noted control weaknesses.

These reviews should, for both in-house and outsourced or co-sourced internal audit activities, encompass internal audit's:

- Policies and processes,
- Staffing resources and qualifications,
- Risk and control assessments,
- Annual audit plans/schedules/budgets,
- Frequency of audits/audit cycles,
- Individual audit work programs and audit reports,
- Follow-up activities, and
- Reports submitted to the audit committee.

Results of these reviews form the basis for the OCC's control assessments and determine how much validation the external audit program requires.

**External Audit Reviews**
Reviews of external audit are essential to the OCC's evaluation of a bank's overall audit program. However, our review is not an "audit of the auditors," nor is it designed to determine whether the audit conforms to AICPA professional standards. Reviews of external audit determine whether the

board of directors or its audit committee effectively oversees a bank's external audit program and whether the program complies with statutory and regulatory requirements, as applicable.

Reviews should focus on:

- The type of external audit activity performed;
- The external auditor's conclusions, findings, and communications to the board or its audit committee; and
- Management's response to those findings.

The examiner should use information readily obtainable from bank management or, if management cannot furnish it, from external auditors. Examples of such information include:

- Engagement letter.
- Opinion letter.
- Management letters (e.g., confirmation of auditor independence, communications with audit committee, no material weaknesses).
- Management representation letter.
- Attorney letters.
- Attestation report on management's control assertion.
- List of unadjusted audit differences/adjusting journal entries.

If these communications are not in writing, examiners should ask bank management their reasons for not obtaining written communications.

As part of the supervisory process, examiners should periodically contact or meet with external auditors, especially if there are questions or issues regarding the external audit. Through this communication, examiners can learn the scope, results, and ongoing plans for external audits.

Topics of discussion should include:

- External auditor's reliance on the work done by internal auditors.
- Extent of the external auditor's assessment and testing of financial reporting controls.
- Results and conclusions of risk assessments, including fraud risk assessment.

- External auditor reliance on financial reporting controls when auditing financial reports.
- Examination and audit results or major findings.
- Upcoming audit and examination activities.
- Assessment of internal controls.
- Reports, management letters, or documents.
- Other appropriate audit or supervisory topics.

## Validation

The objective of the OCC's validation work is to gain or maintain an understanding of audit-related policies, procedures, practices, and findings. Examiners use that understanding to substantiate conclusions about the quality and reliability of a bank's overall audit program, and to determine the scope of supervisory activities required to assess the quality of risk management in other examination areas.

Validation encompasses observation, inquiry, and testing using a combination of:

- Discussions with bank management and audit personnel,
- Audit work paper reviews, and
- Process reviews (e.g., reviews of policy adherence, risk assessments, follow-up activities).

To validate the adequacy of the bank's audit program, OCC examiners will progress, as needed, through three successive steps: **work paper review**, **use of supplementary procedures**, and **verification**.

**Work Paper Review — Internal Audit**
The OCC considers internal audit a fundamental building block of sound internal controls. Therefore, during each supervisory cycle, examiners must review an appropriate sample of **internal** audit program work papers. This includes work papers for outsourced internal audit work performed by independent third parties and those for directors' examinations.[27] Internal

[27] When the director's examination consists of both internal and external audit work (i.e., serves as a bank's sole audit program with an independent external party using agreed-upon procedures), examiners should review a sample of the work papers dealing with traditional internal audit activities (operational and internal control reviews, transaction testing).

audit work paper reviews may not be waived during any supervisory cycle. However, the EIC can limit the scope of the work paper reviews (i.e., the number of internal audit programs or work papers to review) based on his or her familiarity with the bank's internal audit function and findings from previous reviews of internal audit. If the EIC plans to perform a limited review of internal audit work papers, he or she should contact the bank's internal auditor or senior management, as appropriate, before the examination begins. The purpose of this contact is to determine whether there have been any significant changes in the internal audit function or severity of findings since the prior examination.

The purpose of work paper reviews is to find out if internal audit's coverage and scope adequately test and assess the internal control environment in the audited business line or activity. Examiners responsible for functional or line-of-business supervisory activities should review audit work papers for those areas during target reviews. The selected sample should:

- Represent a cross-section of bank functions, activities, and bank-assigned internal audit ratings,

- Preferably be taken from high-risk, problem or rapid growth/decline areas, technology audits, and products, services, or activities new to the bank, and

- Provide a sufficient basis to:
  - Validate the scope and quality of the audit program, and
  - Determine how much reliance, if any, can be placed on the audit program and internal control system.

Work paper documentation should support the internal audit program's conclusions. In reviewing work papers, examiners should not perform the bank's internal audit program procedures. Examiners "re-perform" audit procedures only when they find it necessary to perform verification procedures.

*Outsourced Vendor Work Papers*

When internal audit is outsourced from a third-party vendor and work papers are stored in that vendor's office in another city, examiners can be flexible in their approach to work paper reviews. Work papers from an outsourced internal audit program do not have to be reviewed during an on-site

examination; examiners can review them anytime during the bank's supervisory cycle (i.e., as part of planning activities, quarterly reviews, periodic monitoring, or targeted reviews). Examiners should weigh the pros and cons of traveling to the vendor's office or having the bank ask the vendor to send copies of designated work papers to the bank.

When a vendor performs internal audit program work for multiple national banks, the work papers may be located at the vendor's office in another city. For these situations, examiners should consider the feasibility of centralized work paper reviews. The goals of centralized work paper reviews are efficiencies gained by reducing burdens on examiners, bankers, and third-party vendors, and application of a consistent supervisory approach to such work paper reviews. Examiners may want to coordinate centralized vendor reviews with other OCC field offices when a vendor or firm performs outsourced internal audit work for multiple banks in a geographical area.

**Work Paper Review – External Audit**

Except for director's examinations, examiners are not required to review external audit work papers during a supervisory cycle.[28] However, external audit work papers may be subject to OCC review under certain circumstances. Examiners should consider reviewing external audit work papers in the following circumstances:

- If the review of internal audit discloses significant problems or issues (e.g., insufficient internal audit coverage), or

- If questions are raised about matters that are normally within the scope of an external audit program.

Examples of situations that might trigger an external audit work paper review are:

- Unexpected or sudden changes in the bank's external auditor. Examiners might want to have discussions with the previous and current external auditor before embarking on a work paper review. If the discussions raise unanswered questions that might be addressed in the work papers, then a work paper review may be warranted.

[28] See footnote 27.

- Significant changes in the bank's external audit program. Examiners should contact the external auditor to discuss these changes and determine whether a review of work papers is warranted.

- Significant and unexpected changes in accounting or operating results.

- Issues that affect the bank's safety and soundness. There may be instances when the external auditor raises safety and soundness concerns, or when examiners or internal auditors surface safety and soundness concerns in areas normally within the scope of an external audit program. In such cases, examiners should obtain information from the bank, discuss the issues with bank management and the external auditor, and consider reviewing work papers related to those matters or findings.

- Issues with respect to the independence, objectivity, or competence of the bank's external auditor.

- Recalcitrant external audit firm or staff.

*Access to External Audit Work Papers*
IPAs for banks subject to 12 CFR 363 are required to provide the OCC access to audit-related work papers, policies, and procedures upon request. For banks not subject to 12 CFR 363, engagement letters or written contracts should explicitly provide for examiner access to external audit work papers in accordance with interagency policy statements.

If the examiner determines that the external audit program's work papers warrant review, they should discuss the request with bank management and the external auditor. This discussion may make the work paper review unnecessary or it may help examiners focus their review on the most relevant work papers.

Rather than a blanket request to review all external audit work papers, examiners should make their requests specific to areas of greatest interest and give the reasons for the request. In this way, the external auditor may be able to suggest additional work papers or audit areas for examiner review. Examiners should also consider requesting that the auditor make available, for the specific areas under review, related planning documents and other information pertinent to the area's audit plan (including the sample selection process).

When examiners request access to work papers, an audit firm might ask examiners to sign an acknowledgement letter (SAS 41, "Providing Access to or Photocopies of Working Papers to a Regulator"). If presented with such a letter, examiners should not sign it. Instead, they should complete the OCC acknowledgement letter template in appendix D and return it to the auditor with the auditor's original letter attached. If examiners have questions about the auditor's letter or an external auditor denies or prevents timely access to their work papers, they should contact their District Accountant and District Counsel.

The external auditor may need to offer assistance to examiners for the review of electronic or other work papers. The external auditor should arrange a process to answer examiner questions about the format and organization of work papers. When the audit work papers support holding company financial statement audits or attestation reports, examiners should coordinate reviews with appropriate OCC supervisory offices and other regulators.

Examiners should also be aware that the external auditors might charge the bank for the time they spend responding to an examiner's review of the external audit program's work papers. An external auditor may request that examiners view the audit work papers at the auditor's office. The auditor may also require that their representative(s) be present during the reviews and may not allow photocopying. EICs of community banks and mid-size banks should consult with their ADCs and District Accountants before beginning to review any external audit program work papers. Likewise, large bank EICs should consult with their Large Bank Supervision deputy comptroller and the Chief Accountant's office before beginning such a review.

**Use of Supplemental Procedures**

Minimum or standard core assessment community and large bank audit procedures may identify significant audit or control discrepancies or weaknesses or may raise questions about the audit function's effectiveness. In those situations, examiners will consider expanding the audit program review by selecting supplemental procedural steps from this booklet. Examiners should determine, in consultation with the EIC, whether to expand audit examination work in affected operational or functional business area(s).

For example, examiners will consider expanding audit program procedures if they encounter or identify:

- Issues of competency or independence relating to internal or external auditors.

- Unexplained or unexpected changes in internal or external auditors or significant changes in the audit program.

- Inadequate scope of the overall audit program, or in key risk areas.

- Audit work papers in key risk areas that are deficient or do not support audit conclusions.

- High growth areas of the institution without adequate audit or internal control.

- Inappropriate actions by insiders to influence the findings or scope of audits.

The scope of expanded work must be sufficient to determine the extent of problems and their effect on bank operations. Examiners should include appropriate internal control questionnaires (ICQs) in the expanded procedures.

**Verification**

When reviewing the audit function, significant concerns may remain about the adequacy of an audit or internal controls, or about the integrity of a bank's financial or risk management controls. If so, examiners should consider further expanding the audit review to include verification procedures.[29] Verification procedures should be considered even when the external auditor issues an unqualified opinion but discrepancies or weaknesses call into question the accuracy of the opinion.

*Required Use*

Examiners will use verification procedures whenever they identify the following issues:

- Key account records are significantly or chronically out of balance.

[29] Verification procedures for all examination areas can be found on the "Examiner Library" and "efiles" CDs issued by the OCC.

- Management is uncooperative or poorly manages the bank.
- Management attempts to restrict access to bank records.
- Significant accounting, audit, or internal control deficiencies remain uncorrected from previous examinations or from one audit to the next.
- Bank auditors are unaware of, or unable or unwilling 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.

There may be other situations where examiners believe audit or controls warrant further investigation. In those cases, examiners should consider the risk posed by any noted audit or control weaknesses and use judgment in deciding whether to perform verification procedures.

*Performing Verification Procedures*
When considering use of verification procedures, the following options are available in lieu of examiners performing the procedures:

- Have the bank expand its own audit function to address the weaknesses or deficiencies. Use this alternative only if:
  - Management demonstrates a capacity and willingness to address regulatory problems,
  - There are no concerns about management's integrity, and
  - Management has initiated timely corrective action in the past.
- Have the bank contract with third parties, such as its external auditor or other independent party, to perform the verification. Use this alternative when management's capabilities and commitments are inadequate or where substantive problems exist with having the bank or its audit function perform the procedures.

If examiners choose to use either of the above alternatives, the actions taken must resolve each identified supervisory problem in a timely manner. Supervisory follow-up will include a review of audit work papers in areas where the bank audit was expanded. Examiners should review associated auditor or vendor engagement letters to ensure that the auditor/vendor agreed to provide OCC examiners appropriate access to work papers and reports.

The supervisory office, on a case-by-case basis, will decide whether to pursue verification and, if so, will determine the extent of verification and who will perform it. Verification procedures are generally performed only in rare cases where significant concerns exist. Examiners should consult with the bank's external auditors to determine whether the auditors completed applicable verification procedures. If so, consider whether to use those results to supplement or replace OCC verification. Direct confirmation with bank customers must have prior approval of the ADC and district deputy comptroller or appropriate large bank supervisors. The Enforcement and Compliance Division, the District Counsel, and the District Accountant should also be notified when direct confirmation is being considered.

## Completing the Audit Function Review

The previous sections of this booklet discuss characteristics and practices of effective internal and external audit programs, as well as the principles and processes behind examiner review of a bank's audit function. Examiners will evaluate the extent to which the bank uses these practices, taking into consideration the bank's size, complexity, scope of activities, and risk profile. Examiners evaluate compliance, information technology, and fiduciary audits using the same criteria they use for any other type of audit. Appendixes E through H provide worksheets that can help examiners evaluate a bank's audit function. Individual booklets of the "Comptroller's Handbook for Compliance" also contain worksheets to assist examiners in determining the adequacy of consumer compliance audits.

**Audit Program**

During each bank's supervisory cycle, examiners will evaluate the quality and scope of the bank's overall audit program considering whether:

- The board of directors or its audit committee reviews and approves audit programs and policies at least annually.

- The board of directors or its audit committee monitors the implementation of the audit program and associated audit schedules.

- The internal and/or 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 of directors or its audit committee and appropriate bank management.

- The board and management properly follow up on the results of audits and appropriately monitor any significant issues.

- Internal and/or external auditors maintain an appropriate level of professional standards and training/development.

**Board/ Audit Committee**

Examiners should determine whether a bank's board or audit committee understands its audit oversight responsibilities and whether the board or audit committee members are sufficiently experienced to execute these responsibilities. Examiners make these determinations by reviewing board or audit committee minutes and by discussing the audit program with the board or audit committee. Examiners should focus attention on the quality of the board's or audit committee's communication with the internal and external auditors. When appropriate, examiners should recommend ways to enhance the board's or audit committee's oversight. For community banks, especially smaller ones, examiners must be cognizant of the bank's size, complexity, and risk profile; they should bear those circumstances in mind when making recommendations. Where applicable, examiners should review a bank's compliance with statutory requirements governing audit committee disclosures and member qualifications. These requirements apply to OCC-registered national banks and national banks with total assets of $500 million or more.

Examiners will use judgment and discretion when evaluating a board's decision to forgo an external audit. OCC examiners will not criticize a small bank or include adverse comments in the Report of Examination simply because it does not have an external audit program. Examiners' considerations should include a bank's size; the nature, scope, and complexity of its activities; its risk profile; the extent of its internal audit program; compensating internal controls; the significance of any identified audit or internal control weaknesses, and board/management actions to address those weaknesses.

**Corrective Action**

Significant concerns with the work, independence, objectivity, or competence of internal, external, or outsourcing auditors should first be discussed with the auditor to resolve the issues. If significant concerns remain unresolved, examiners will discuss the situation with the board of directors/audit committee, senior management, and relevant parties and contact OCC district management, the Chief Accountant's Office, or the Chief Counsel's Office, as appropriate, before finalizing the report of examination.

When warranted by the circumstances, the OCC may refer an external auditor to the state board of accountancy, AICPA, or other regulatory bodies for possible ethics or independence violations. Moreover, the OCC may conclude that the bank's external audit program is inadequate and does not comply with auditing and reporting requirements. If necessary, the OCC may also bar an external auditor from engagements with OCC-supervised institutions. Examiners should direct questions about such referrals to the supervisory office, the Chief Accountant's office, or the Chief Counsel's Office.

If examiners identify supervisory issues concerning a bank's external audit program, they should not look to the external auditors to fix the problems, although the auditor may be part of the solution. Rather, examiners should look to the bank's board of directors, usually to its audit committee, to take corrective action on noted issues. The board is responsible for maintaining an effective audit program and, at many banks, the external audit is a prominent part of that program.

If examiners identify significant audit weaknesses, the EIC will recommend to the appropriate supervisory office what formal or informal action is needed to ensure timely corrective measures. Consideration should be given to whether

the bank meets the internal audit safety and soundness operational and managerial standards of 12 CFR 30, Appendix A. Possible options examiners will consider include having bank management develop a compliance plan consistent with 12 CFR 30 to address the weaknesses, or making the bank subject to other types of enforcement actions. In making a decision, the supervisory office will consider the significance of the weaknesses, overall audit rating, audit-related Matters Requiring Attention, management's ability and commitment to effect corrective action, and the risks posed to the bank.

**Communication of Audit Review Conclusions**

At the conclusion of the audit review, the EIC or designee will discuss findings, significant audit weaknesses, and audit-related recommendations with the bank's board of directors or its audit committee and senior management. Examiners will summarize the discussions in examination working papers and assign a rating of strong, satisfactory, or weak to the overall audit function. Appendixes I and J provide guidance for assigning an overall audit rating for community banks and large/mid-size banks. Regardless of the overall audit rating assigned, the report of examination will contain comments summarizing the adequacy of the bank's audit program and any significant audit issues or concerns.

The Uniform Interagency Consumer Compliance Rating System takes into consideration a bank's compliance audit functions. When assigning a consumer compliance rating, examiners must consider the adequacy of operating systems, including internal procedures, controls, and audit activities that the bank uses to ensure compliance with applicable consumer laws, rules, and regulations.

Under the Uniform Rating System for Information Technology (URSIT), part of the evaluation of a bank's information technology system includes an assessment of the IT audit program. Examiners and bankers should refer to OCC Bulletin 99-3, "Uniform Rating System for Information Technology" for additional information on assigning a rating for IT audits.[30]

Under the Uniform Interagency Trust Rating System (UITRS), the fiduciary activities of national banks are assigned a composite rating for five areas. One of those areas is operations, controls, and audits. For this area to be

[30] For more information on IT audits, examiners and bankers can refer to the FFIEC's "Information Systems Examination Handbook." It has examination procedures specifically for IT audits.

considered adequate, audit coverage must ensure the integrity of the financial records, the sufficiency of internal controls, and the adequacy of the compliance process.[31]

[31] OCC Bulletin 98-46, "Uniform Interagency Trust Rating System," provides further information on assigning trust ratings.

**Supplemental Examination Procedures ..... 61**
Planning the Audit Review ..... 61
Board and Committee Oversight ..... 64
Internal Audit ..... 69
External Audit ..... 93
Overall Conclusions ..... 105

# Supplemental Examination Procedures

**These examination procedures supplement the core assessment audit objectives in the "Community Bank Supervision" booklet and the minimum audit review standards in the "Large Bank Supervision" booklet. Examiners should begin their audit review with those core assessment or minimum objectives and steps. The examiners' assessment of risk, the supervisory strategy objectives, and any examination scope memorandum should determine which of this booklet's procedural and validation steps to perform to meet examination objectives. Seldom will every objective/step of this booklet's procedures be required to satisfy examination objectives.**

These procedures are intended to help examiners determine the quality and reliability of the bank's policies, procedures, personnel, and controls with respect to its overall audit functions. The procedures are not meant to be performed strictly in the order presented, but should be fit to the bank's or examination's particular circumstances. The review of audit functions should be closely coordinated with the reviews of examiners responsible for other areas of the bank (e.g., credit, capital markets, compliance, fiduciary, and information systems). Such coordination can reduce burden on the bank, prevent duplication of examination efforts, and be an effective crosscheck of compliance and process integrity.

## Planning the Audit Review

Objective 1: Determine the scope and objectives of the examination of the internal and external audit functions.

1. Determine whether the bank has internal and external audit functions.

2. If a community bank does not have an external auditing function, discuss the circumstances with the board and management. Focus on:

   - Why the board decided not to have an external audit.
   - The benefits of an external auditing function.
   - Whether such benefits are being provided by an alternative means such as internal expertise or other outside sources.

3. Obtain and review the following documents to identify any issues or concerns that require follow-up:

   - ☐ Previous Report of Examination and key supervisory information (e.g., strategy, analyses, other significant events) in OCC databases.
   - ☐ EIC's scope memorandum, if applicable.
   - ☐ OCC audit summary memos and working papers from the previous examination.
   - ☐ Centralized vendor review memorandums, if applicable.
   - ☐ Internal audit reports, including audit reports that the auditors may have participated in or relied on to any extent, such as AICPA SAS 70 reports ("Reports on the Processing of Transactions by Servicing Organizations").
   - ☐ External audit reports and other correspondence/communication between the bank and the external auditor, e.g., opinion letter and financial statement report, FDICIA attestation report, list of audit differences or adjusting journal entries, and letters/correspondence pertaining to SAS 61, confirmation of independence, material control weaknesses.
   - ☐ Audit policies and manuals, including those applicable to sampling plans, risk-based auditing, or outsourcing of internal audit functions.
   - ☐ Minutes of the audit committee(s), including the fiduciary audit committee, if applicable, and applicable board of directors' minutes since the last examination.
   - ☐ Audit packages and information submitted to the board or its audit committee.
   - ☐ Listing of members of the audit committee(s), including those on the fiduciary audit committee, if applicable, and the date of each member's appointment to committee.
   - ☐ Audit plans and scopes, including any external audit or internal audit outsourcing engagement letters.
   - ☐ The institution's annual reports.
   - ☐ Correspondence memorandum.

4. Identify, through discussion with management and review of the most recent internal and external audit reports:

   - How management supervises audit activities.

- Any significant changes in business strategy or activities that could affect the audit function.

- Any material changes in the audit program, scope, schedule, or staffing related to internal and external audit activities.

- Any other internal or external factors that could affect the audit function.

5. Obtain a list of outstanding audit items and compare the list with audit reports to ascertain completeness. Determine whether all significant deficiencies noted in the audit reports have been corrected and, if not, determine why corrective action has not been initiated. Make those determinations by:

   - Distributing to each examiner responsible for an examination area a copy of the area's audit report or a list of significant audit deficiencies for that area.

   - Requesting that the examiner prepare and return a memorandum stating whether the board or management has addressed the audit deficiencies and whether their actions were adequate.

6. Identify internal audit work programs, including those from any outsourced internal audit activities and directors' examination, from which to select a reasonable sample of internal audit work papers for validation purposes. Coordinate work paper review efforts with the examiners reviewing functional or specialty areas (e.g., credit, capital markets, compliance, information systems, and fiduciary) and:

   - Provide the examiner(s) with the audit program(s) and audit report(s) for the specific area(s) to be tested.

   - Request that the examiner(s) review applicable internal audit work papers.

**Note:** A sample of internal audit work papers will be reviewed during every supervisory cycle. The sample should provide a sufficient basis to validate the scope and quality of the internal audit program and determine how much examiners can rely on the internal audit function and internal control system.

The sample should represent a cross-section of bank activities, functions, and bank- assigned audit ratings, and should preferably be taken from high-risk, problem, and rapid growth/decline areas, technology audits, and products/services/activities new to the bank.

**Note:** When the director's examination consists of both internal and external audit work (i.e., serves as a bank's sole audit program with an independent external party using agreed-upon procedures), examiners should review a sample of the work papers dealing with traditional internal audit activities (e.g., operational reviews, internal control reviews, transaction testing).

## Board and Committee Oversight

Conclusion: The board of directors or its audit committee (does, does not) effectively oversee appropriate audit functions for the bank.

**Note:** Examiners may want to use appendix H, "Board/Audit Committee Oversight Worksheet," as an aid in completing this portion of the examination procedures.

Objective 2: Determine the overall quality of board and committee oversight of the bank's audit functions.

1. By discussing audit activity with bank management, reviewing board or audit committee minutes and audit information packages, and performing appropriate examination procedures, determine whether the bank's board of directors or its audit committee:

   - Reviews and approves audit strategies, policies, programs (including the BSA compliance program), and organizational structure, including selection/termination and compensation of external auditors or outsourced internal audit vendors.

   - Establishes schedules and agendas for regular meetings with internal and external auditors. The audit committee should meet at least four times a year.

   - Supervises the audit functions directly to ensure that internal and external auditors are independent and objective in their findings.

- Works with internal and external auditors to ensure that the bank has comprehensive audit coverage to meet the risks and demands posed by its current and planned activities.

- Has significant input into hiring senior internal audit personnel, setting their compensation, and evaluating the internal audit manager's performance.

- Reviews and approves annual audit plans and schedules (and any changes thereto) for both internal and external audits.

- Retains auditors who are fully qualified to audit the kinds of activities in which the bank is engaged.

- Meets with bank examiners, at least once each supervisory cycle, to discuss findings of OCC reviews of the bank's audit functions.

- Monitors, tracks, and, when necessary, provides discipline to ensure effective and timely response by management to correct control weaknesses and violations of laws/regulations noted in internal or external audit reports or in examination reports.

2. Has the board of directors established an audit committee? If so, are committee members:

   - Independent of bank management?
   - All outside directors or at least a majority of outside directors?

Objective 3: If the bank had total assets of $500 million or more at the beginning of its current fiscal year, determine compliance with the following provisions of 12 CFR 363.

**Note:** The following requirements can be satisfied by the parent holding company of a bank subsidiary on two conditions: (1) if the services and functions comparable to those required of the bank are provided at the holding company level, and (2) if, as of the beginning of its fiscal year, the bank had total assets of less than $5 billion or total assets of $5 billion or more and a composite CAMELS rating of 1 or 2 (12 CFR 363.1(b)(2)). The OCC or FDIC may revoke the exception in 12 CFR 363.1(b)(2) if the bank has total

assets of $9 billion or more and the agency determines that exempting the bank would place the deposit insurance fund at significant risk (12 CFR 363.1(b)(3)).

1. Obtain the board of directors' most recent annual determination that its audit committee is structured in accordance with 12 CFR 363.5(a). Review the determination to see whether the board concluded that:

   - The committee is made up entirely of outside directors of the bank.

   - Each committee member is independent of bank management by considering whether he or she:
     - Is, or has been within the preceding year, an officer or employee of the institution or its affiliates.
     - Serves or served as the institution's or its affiliates' consultant, advisor, promoter, underwriter, legal counsel, or trustee.
     - Is a relative of an institution's or its affiliates' officers or employees.
     - Holds or controls, or held or controlled within the preceding year, either directly or indirectly, a financial interest of 10 percent or more in the institution or its affiliates.
     - Has outstanding extensions of credit from the institution or its affiliates.

   - The committee's duties include:
     - Performing all duties assigned by the institution's board of directors.
     - Reviewing with management and the IPA:
       - The basis of reports required by 12 CFR 363.2(a), (b) and 363.3(a) and (b).
       - The scope of services required by the audit, significant accounting policies, and audit conclusions regarding significant accounting estimates.
       - Their assessments of internal control adequacy and resolution of identified material internal control weaknesses and reportable conditions.
       - The institution's compliance with laws and regulations.
     - Discussing with management the selection and termination of the IPA and any significant disagreements between the IPA and management.

- Overseeing the internal audit function.
- Maintaining minutes and other relevant records of their meetings and decisions.

2. If the bank had assets of more than $3 billion at the beginning of its fiscal year, review the board's determination to see if it also concluded that the audit committee complies with 12 CFR 363.5(b) by having:

   - At least two members with the following banking or related financial management expertise:
     - Significant executive, professional, educational, or regulatory experience in financial, auditing, accounting, or banking matters as determined by the board of directors, or
     - Significant experience as an officer or member of the board of directors or audit committee of a financial services company.

   - Access to its own counsel at its discretion and without prior approval of the board or management.

   - No member who is a large customer of the bank.

   **Note:** If a large bank is a subsidiary of a holding company and relies on the audit committee of the holding company to comply with this requirement, the holding company's audit committee shall not include any members who are large customers of the subsidiary bank.

3. Review the institution's most recent fiscal year-end management report (12 CFR 363.2(b)) and determine whether the report:

   - Is signed by its chief executive officer and chief accounting or chief financial officer.

   - Contains a statement of management's responsibilities for:
     - Preparing the institution's annual financial statements.
     - Establishing and maintaining adequate internal control structures and procedures for financial reporting.
     - Complying with laws and regulations relating to safety and soundness that are designated by the OCC (12 CFR 363.2(b)(1)).

   - Contains management's assessments of:

  - The effectiveness of internal control structures and procedures as of the end of its fiscal year.
  - The institution's compliance with laws and regulations during the fiscal year (12 CFR 363.2(b)(2)).

4. Review documentation pertaining to management's assessment of financial reporting controls and its own investigation and review of compliance with designated laws and regulations regarding insider loans and dividend restrictions (appendix A to 12 CFR 363, table 1).

   - Has management maintained records of its review?
   - Were the results of the review discussed with the audit committee?
   - Is management's assessment of financial reporting controls and compliance with designated laws consistent with findings of the bank's internal and external auditors, as well as supervisory examination findings?

5. Review the institution's determination that it met the filing and notice requirements of 12 CFR 363.4. Does the determination indicate that:

   - Within 90 days after its fiscal year end, the institution filed with the OCC and FDIC two copies of an annual report containing (12 CFR 363.4(a)):
     - Audited financial statements.
     - Independent public accountant's report on the financial statements.
     - Management's statements and assessments.
     - Independent public accountant's attestation report concerning the institution's internal control structure and procedures for financial reporting.

   - The institution's annual report in 363.4(a) is available for public inspection (12 CFR 363.4(b)).

6. Note any exceptions to 12 CFR 363 reporting or audit committee requirements or activities and discuss corrective measures with the board of directors or audit committee.

Objective 4: If the national bank is subject to the periodic filing and reporting requirements of 12 CFR 11 or 12 CFR 16.20 (i.e., they have registered their

securities with the OCC), determine compliance with certain SEC requirements.

**Note:** The OCC's Security and Corporate Practices (SCP) division is responsible for reviewing filings and reports submitted by national banks under 12 CFR 11 and 12 CFR 16.20. Examiners should not check for compliance themselves, but they may want to contact SCP if they have any questions regarding the filings or reports.

1. Review correspondence or other communications issued by SCP resulting from their review of the bank's proxy material and annual reports.

2. Determine whether the bank has adequately addressed issues requiring attention resulting from SCP's review.

## Internal Audit

Conclusion: The board of directors (has, has not) implemented and (does, does not) effectively oversee an internal audit function appropriate for the bank's activities and risk profile that complies with 12 CFR 30 operational and managerial standards.

Objective 5: Determine the adequacy of board and management oversight of the bank's internal audit function.

1. Determine whether the board, commensurate with the bank's activities and risk profile, has established an internal audit program, in accordance with 12 CFR 30, that:

   - Adequately monitors internal control systems.
   - Is independent and objective.
   - Is staffed by qualified persons.
   - Adequately tests and reviews information systems.
   - Adequately documents tests, findings, and corrective actions.
   - Verifies and reviews management actions addressing material weaknesses.
   - Requires the board of directors or audit committee to review the internal audit systems' effectiveness.

**Note:** Examiners should consider citing a violation of 12 CFR 30 if the internal audit program does not effectively or fully meet the above requirements. Consider whether overall audit is rated "Weak" because of significant deficiencies in the internal audit function or its oversight, whether MRAs pertaining to internal audit are being put in the report, or whether recommended enforcement actions will include internal audit-related articles.

2. Determine whether the bank's internal audit program possesses:

   - An audit charter or mission statement that sets forth the audit department's purpose, objectives, organization, authority, and responsibilities.

   - An audit plan that addresses goals, schedules, staffing budget, reporting, and, if applicable, financial budgets.

   - A policies and procedures manual for audit work programs and, if applicable, risk-based auditing/risk assessments and outsourcing of internal audit work.

   - A program for professional development and training of audit staff, including orientation and in-house and external training opportunities.

   - A quality assurance program performed by internal or external parties to evaluate the operations of the internal audit department.

3. Review board or audit committee minutes, or summaries thereof, and audit information packages submitted to the board or audit committee. Determine whether:

   - The board of directors or its audit committee has formally approved the internal audit program and annual audit plan and schedule.

   - Internal audit reports and other audit-related information submitted regularly to the board or audit committee are sufficient for effective monitoring of internal audit's performance and progress toward meeting approved audit plans and schedules. Consider:

  - Status reports of annual audit plan and schedules.
  - Activity reports for audits completed, in process, and deferred/cancelled.
  - Staffing/training reports.
  - Tracking reports for significant outstanding audit and control issues.
  - Discussion of significant regulatory or accounting issues.
  - Compliance and IT review summaries.
  - Risk assessments/evaluations or summaries thereof.
  - Results of regulatory examinations.
  - Other information the audit committee or internal auditor deem appropriate

- The internal audit program and annual plan/schedule are periodically reviewed and updated by the internal audit department, with changes reported to the board or audit committee.

- Progress has been made toward completing the audit program or schedule and the board or audit committee has approved significant audit program/schedule changes.

- Reasonable consideration is given to staffing, compensation, and training requirements.

- Management does not unduly participate in or dominate the directors' or audit committee's supervision of the internal audit function.

4. Review management's records supporting any assertions concerning the effectiveness of internal controls over financial reporting and compliance with designated insider loan and dividend restriction laws and regulations (required for any bank subject to 12 CFR 363).

   - Determine whether management's standards for measuring the adequacy and effectiveness of internal controls over financial reporting are appropriate. Consider:
     - Sources of established standards (e.g., AICPA, OCC, and Committee of Sponsoring Organizations of the Treadway Commission [COSO]).
     - Risk analyses or assessments.

- Control assessments.
- Audit report findings.

- Determine whether management's assessment of financial reporting controls and compliance with designated laws is consistent with findings of the bank's internal and external auditors, as well as with supervisory examination findings.

5. Determine whether the internal auditor reports directly to the board or to an appropriate audit committee.

6. Determine whether management takes appropriate and timely action on internal audit findings and recommendations and whether it reports the action to the board of directors or its audit committee.

7. Determine whether the activities of the internal audit function are consistent with the long-range goals of the institution and are responsive to its internal control needs.

8. For banks that have a quality assurance program, evaluate the adequacy and effectiveness of the program by determining whether:

   - Standards and criteria have been established for evaluating the performance of the internal audit function.

   - Quality assurance is conducted in the following manner:

     - Continuous supervision by the internal audit manager,
     - Periodic internal reviews by a team or individual from the internal audit staff, or
     - External reviews by qualified persons independent of the bank.

     **Note:** The Institute of Internal Auditors' (IIA) standards call for its members and Certified Internal Auditors to have both internal and external quality assurance reviews (QAR). Effective January 1, 2002, the IIA requires at least one mandatory external QAR to be conducted every five years. If a bank's audit policy or charter requires adherence to IIA standards, examiners should remind the bank's internal audit department to follow IIA QAR guidance.

- Any type of formal report, written or oral, is generated and to whom the report is directed (i.e., internal audit manager, senior management, or board of directors or its audit committee).

- Quality assurance reviews are conducted regularly.

9. Review policies and manuals pertaining to the bank's internal audit function, including, as applicable, those related to risk-based audits, outsourcing of internal audit activities, and directors' examinations. Consider whether written policies:

   - Are adequately reviewed and approved by the board of directors or its audit committee annually.

   - Properly reflect authorities and responsibilities established by the audit charter or mission statement.

   - Establish proper scope and frequency for internal audits. Consider:
     – Statutory requirements and regulatory guidelines.
     – Purpose and objectives of audits.
     – Control and risk assessments.
     – Audit cycles.
     – Reporting relationships and requirements.

     **Note:** Banks using traditional auditing typically will have audit cycles of 12 to 18 months. However, banks using risk-based auditing or internal risk assessments generally have audit cycles of varying lengths based on the level of risk in an activity. See risk-based auditing objective for details.

   - Establish adequate guidelines for human resources involved in the audit function. Consider:
     – Organization and independence of the audit department.
     – Responsibilities of audit staff.
     – Job standards and qualifications.
     – Training and development.
     – Performance evaluations.

Objective 6: Evaluate the independence and competence of those who manage and perform internal audit functions, whether or not they are bank employees.

1. Obtain the following:

   - ☐ Resumes of the internal auditor/manager, new internal audit staff, or those recently promoted to senior levels.
   - ☐ Job descriptions for various audit positions.
   - ☐ As deemed appropriate, performance evaluations of the audit manager and selected audit staff.

2. Assess the educational and professional experience of the internal auditor and staff by reviewing resumes and noting:

   - The level of education attained.
   - Significant work experience, especially in the bank auditing arena, including specialized areas such as capital markets, information systems, fiduciary activities, and subsidiary activities.
   - Any certification as a certified bank auditor, certified internal auditor, certified information systems auditor, or certified public accountant.
   - Membership in professional associations.

3. Review job descriptions and discuss with the audit manager:

   - Educational and experience requirements for various audit positions, including those for specialized areas.
   - Programs of continuing education and professional development, including in banking and auditing technology and specialized areas.
   - Supervision of the auditors.

4. If deemed appropriate, review performance evaluations of the audit manager and audit staff. Determine how identified strengths and weaknesses in supervisory, technical, or interpersonal skills or abilities affect the quality of the internal audit function.

5. Assess audit personnel turnover and vacancies, focusing on the reasons for turnover/vacancies and their effect on the internal auditing function.

6. Evaluate the ability of the audit manager and staff to communicate and interact with other institution personnel.

7. Determine whether there are any reporting lines or operational duties assigned to the auditor that are incompatible with the internal audit function. Consider:

   - Reporting to a senior management official, i.e., CFO, controller, or similar officer.

   - Dual reporting, functionally to audit committee on audit issues and to senior management for administrative matters (i.e., performance appraisal, salary, department budget).

   - Responsibilities for operating a system of internal controls or actually performing operational duties or activities.

   If any of the above situations exist, determine whether independence is compromised or whether the situation is appropriately controlled and monitored. Consider the bank's size, underlying risks, and activities.

8. Ascertain whether there is any auditor relationship, such as family ties with other bank employees, which is incompatible with the internal audit function.

9. Determine whether there are any restrictions placed on the internal audit program, including scheduling or budgetary restraints imposed by management.

Objective 7: Determine the adequacy and the reliability of work performed by the internal auditors.

1. If not previously provided, obtain copies of or access to:

- ☐ Internal audit reports.
- ☐ Internal audit work papers.

2. Using internal audit work programs previously identified in "Planning the Audit Review," obtain or request access to internal audit work papers to complete this objective and its steps. Consider having examiners responsible for other areas of the bank (e.g., credit, capital markets, compliance, information systems, fiduciary) review internal audit work programs and work papers associated with those activities.

   **Note:** In most situations, reviewing the **work papers** that document the procedures and testing performed by the internal auditor should be sufficient to substantiate conclusions about the quality and reliability of the internal auditing function. Examiners should use appendix E, "Internal Audit Review Sheet," and appendix F, "Audit Function Questionnaire," to help them review internal audit work papers. They also may want to use worksheets found in individual booklets of the "Comptroller's Handbook for Compliance Activities." Findings from the work paper reviews will help determine whether further verification or testing is warranted.

3. Review the bank's internal audit program for completeness and compliance with prior board or audit committee approval.

4. Analyze the internal auditor's evaluation of departmental internal controls, and compare it with the control evaluations done by OCC examiners.

5. Review internal audit reports to determine whether they are adequate and prepared in accordance with established audit policy. Consider the reports':

   - Distribution
     - To division heads/senior management responsible for taking action.
     - To internal audit staff, as appropriate.
     - To board of directors or its audit committee.

   - Time frames

  - Audit findings discussed with appropriate parties (i.e., division personnel or senior management) after completion of audit work.
  - Responses obtained from appropriate parties after discussion of audit findings.
  - Final report issued after discussion of audit findings and receipt of responses.

- Content
  - Executive summary or opening paragraph.
  - Statements on the audit's purpose, objectives, and scope.
  - Findings, recommendations, root causes of deficiencies, and other comments.
  - Management commitments.
  - Opinion or grading summary.

- Follow-up
  - Written responses from audited parties to division or senior management and the internal auditor.
  - Auditor's review and discussion of corrective action efforts or results with appropriate parties.
  - A re-audit, if performed.

6. Review the most recent audit plan and determine whether adequate coverage and internal risk assessment is provided for all areas of bank operations (for example, cash, loan controls, conflicts of interest, off-balance-sheet activities, negotiable instruments, interoffice clearing accounts, due from banks, employee accounts, overdrafts, and payments against uncollected funds.)

7. If the bank uses sampling in control testing, asset verification, transactional testing, administrative audits, etc., determine whether the audit work program addresses:

   - Objectives of testing.
   - Procedures to meet objectives.
   - Populations subject to sampling.
   - Method of sampling (i.e., statistical or judgmental).
   - Selecting and justifying a representative sample sufficient to support conclusions.
   - Evaluation of results and documentation of conclusions.

**Note:** Examiners can refer to the "Sampling Methodologies" booklet or other industry material for detailed guidance about statistical and judgmental sampling.

8. Evaluate the scope of the internal auditor's work as it relates to the bank's size, the nature and extent of banking activities, and the bank's risk profile.

   - Do the work papers disclose that specific program steps, calculations, or other evidence supports the procedures and conclusions set forth in the reports? Consider:

     – Verification of account balances (reconciliation, confirmation, and physical count).
     – Review/test of income and expense accounts, accruals, gains/losses, including computations.
     – Transaction testing and testing the value or pricing of assets (i.e., investments, collateral).
     – Physical inspection of legal and supporting documentation, including validation of authorities granted (i.e., making/approving loans, signing official bank documents, etc.).
     – Review of information system data controls.
     – Review and evaluation of policies, procedures, and internal controls.
     – Checks of compliance with laws/regulations.
     – Checks of adherence to bank policy.

   - Is the scope of the internal audit procedures adequate and properly documented? Consider:

     – Audit planning memoranda.
     – Checklists.
     – Internal control questionnaires.
     – Control and risk assessments.
     – Previous audit reports, responses, and follow-up.
     – Procedures performed (general and specific).
     – Testing conducted.

9. Consider expanding the audit review to include verification procedures, including completing internal control questionnaires, if

   - Significant concerns remain about the adequacy of internal audit, the soundness of internal controls, or the integrity of financial or risk management controls for an audited area, or

   - Any of the following issues exist:

     – Key account records are significantly or chronically out of balance.
     – Management is uncooperative or poorly manages the bank.
     – Management attempts to restrict access to bank records.
     – Significant accounting, audit, or internal control deficiencies remain uncorrected from previous examinations or from one audit to the next.
     – Bank auditors are unaware of, or unable or unwilling 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.

   **Note:** Verification procedures are required in certain situations. See the "Supervisory Process and Validation" section of this booklet for specific details. Consult with the EIC and ADC, on a case-by-case basis, to decide whether to pursue verification and, if so, determine how thorough the procedures will be and who will perform them. Verification procedures are performed rarely, and only in cases where significant concerns exist. Examiners should consult with the bank's external auditors to determine whether they completed applicable verification procedures and, if so, whether to use those results to supplement or replace OCC verification. Direct confirmation with bank customers must have prior approval of the ADC and district deputy comptroller. The Enforcement and Compliance Division, the District Counsel, and the District Accountant should also be notified when direct confirmation is being considered.

   In lieu of directing examiners to perform verification procedures, the EIC may consider calling on the bank:

- To expand its own audit function to address the weaknesses or deficiencies. Examiners should use this alternative only if management has demonstrated a capacity and willingness to address regulatory problems, if there are no concerns about management's integrity, and if management has initiated timely corrective action in the past.

- To contract with third parties, such as its external auditor or other independent party, to perform the verification. Examiners should use this alternative when they believe management's capabilities and commitments are inadequate or when there are substantive problems in having the bank or its audit function perform the procedures.

If examiners choose to use either of the above alternatives, the actions must resolve each identified supervisory problem in a timely manner. And supervisory follow-up will include a review of audit work papers in areas where the bank audit was expanded.

Objective 8: If the internal audit function, or any portion of it, is outsourced from outside vendors, determine how effective and reliable the outsourced internal auditing work is.

**Note:** *Centralized Vendor Reviews* – When a third-party vendor performs outsourced internal audit work for two or more national banks in a geographical area, examiners may, at their discretion, choose to perform a centralized review of the vendor's work. Examiners can coordinate this review with examiners from one field office or with examiners from other field offices. A centralized vendor review may result in examination efficiencies by reducing the supervisory burden on the bank and the third-party vendor, as well as examiners, and eliminating duplication of examination efforts. It also may result in a more consistent examination approach for reviewing outsourced vendor work. Examiners can use the centralized vendor review process to determine the effectiveness and reliability of outsourced internal audit work and can use review results to leverage the scope of individual examinations and OCC audit reviews at affected banks.

**Ideally, centralized vendor reviews should be part of the audit review planning process and should take place before the start of any onsite**

**examinations at affected banks. A team of experienced examiners who are familiar with audit processes should perform the reviews.** Review-team examiners should consult with the ADC/EIC/portfolio manager of each affected bank to help determine which work papers to review at the centralized vendor review. The initial centralized vendor review should be comprehensive. Subsequent centralized vendor reviews could consist of a limited review of work papers and discussions with the third-party vendor to determine whether there have been significant changes in the process, system, scope or findings since the previous review. A more complete centralized vendor review of internal audit work papers should be done every second supervisory cycle.

**Examiners must understand that the focus of centralized vendor reviews is on the quality and reliability of internal audit work for each individual bank, rather than a blanket endorsement of the vendor. The reviews are not a substitute for or waiver of other work examiners must do as part of their overall audit assessment during onsite examinations or other supervisory activities at the individual banks. Examiners are encouraged and have the flexibility, if so desired or warranted, to undertake additional testing at the bank level or to review additional internal audit work papers during onsite and other supervisory activities during a supervisory cycle. Examiners should base that decision on events that have occurred since the most recent centralized vendor review and any other matters that come to their attention during supervisory activities (e.g., high risk areas and new products and services).**

1. Obtain and review the following documents:

   - Outsourced internal audit arrangement contracts or engagement letters.
   - Outsourced internal audit reports.
   - Outsourced audit policies, if any.

   If performing a centralized vendor review, examiners should contact affected ADCs/EICs/portfolio managers and discuss the scope of the review. In addition to the above information, also obtain and review the supervisory strategy, EIC scope memorandum (if applicable), and previous report of examination and OCC database summary comments for each of the banks included in the centralized review.

2. Review the outsourcing arrangement contract/engagement letter between the vendor and bank and determine whether the contract/letter adequately:

   - Defines the expectations and responsibilities under the contract for both parties.

   - Sets the scope, frequency, and fees to be paid for work to be performed by the outside vendor.

   - Describes responsibilities for providing and receiving information, such as the type and frequency of vendor reporting to the bank's audit manager, senior management, and audit committee or board of directors about the results and status of work.

   - Establishes protocol for changing the terms of the engagement, especially for expansion of audit work if significant issues arise, as well as stipulations for default and termination of the contract.

   - States that internal audit reports are the property of the bank and specifies ownership of internal audit work papers. If the vendor retains ownership of the work papers, the contract should stipulate that the bank will be provided copies of related work papers it deems necessary, and that bank-authorized employees will have reasonable and timely access to vendor work papers.

   - Notes that the vendor's internal audit activities are subject to OCC review and that examiners will be granted full and timely access to all related outsourced internal audit reports, audit programs, audit work papers, and memorandums and correspondence prepared by the outsourced vendor.

   - Specifies the locations of and how long (generally five years) the vendor will retain outsourced internal audit reports and related work papers. If the work papers are in electronic format, the agreement should also address vendor maintenance of proprietary software to facilitate bank or examiner reviews of work papers.

   - Establishes processes (arbitration, mediation, or other means) for resolving disputes, as well as indemnification provisions for

determining who bears the cost of consequential damages arising from errors, omissions, and negligence.

- States that the vendor will not perform management functions, make management decisions, or act or appear to act in a capacity equivalent to a member of bank management or a bank employee.

- As applicable, states the vendor will comply with AICPA, SEC, Public Company Accounting Oversight Board (PCAOB), or other regulatory independence guidance.

3. Determine, through discussions with bank management or review of applicable documentation, whether the board of directors or audit committee performed sufficient due diligence to satisfy themselves of the vendor's competence and objectivity prior to entering the outsourcing arrangement. Consider whether due diligence addressed the following:

   - Available vendor services (including specialized areas) and work arrangements.

   - Costs and benefits of vendor services to be provided.

   - Ability and flexibility of vendor to perform the services in a timely manner and maintain the confidentiality of bank data.

   - Experience level, technical expertise, and credentials of vendor staff (including specialized areas such as information technology, international, trust, and capital markets).

   - Notifications of any changes in vendor processes, staffing, or other changes affecting assigned staff.

   - Vendor's approach for conducting outsourced internal audits (e.g., risk-based or traditional, use of audit tools and audit technology).

   - Reference checks.

   - Vendor's internal quality control processes (peer review and quality assurance).

- Discussions of vendor independence, objectivity, integrity, and conflict of interest standards applicable to the engagement, e.g., AICPA, IIA, PCAOB, and SEC.

4. Arrange a meeting with the vendor and discuss the vendor's outsourced internal audit program. Consider:

   - Vendor's understanding of the bank's risk profile and business.
   - Vendor's sampling techniques for testing internal controls.
   - Vendor's training program for its audit staff.
   - Communication with and reporting to the bank's board of directors, audit committee, and management.
   - Whether the vendor's audit procedures are customized for each bank client or are generic.
   - Vendor's method for reviewing internal controls.
   - Methods used to structure vendor contracts.
   - How the vendor ensures independence/coordination with external audit activities.
   - Work paper documentation standards.

5. Determine how the bank and vendor address internal control weaknesses or other matters noted by the outsourced vendor during internal audits. Consider whether:

   - The vendor reports results of outsourced internal audit work to the bank's audit manager or internal auditor in a timely manner.
   - The internal auditor or audit manager and the vendor mutually decide whether to report findings to the board or its audit committee and senior management.

**Note:** Examiners must review an appropriate sample of outsourced internal audit work papers during every supervisory cycle. The sample should provide a sufficient basis to validate the scope and quality of outsourced internal audit activities and determine how much examiners can rely, if at all, on the bank's internal audit program and internal control system. During centralized reviews of vendor work papers from individual banks, when deciding which areas' work papers will be reviewed, coordinate the selection with affected ADCs/EICs/portfolio managers.

6. Review outsourced internal audit reports issued and a sample of outsourced internal audit work papers to determine their adequacy and preparation in accordance with the audit program and the outsourcing agreement for the bank. If performing a centralized vendor review, review reports issued and a sample of outsourced internal audit work papers for each individual bank for which the vendor performs outsourced internal audit work. Examiners may want to use the "Internal Audit Review Worksheet" in appendix E to evaluate the quality of outsourced internal audit work programs. Determine whether:

   - Work program steps, calculations, or other evidence support the audit scope's objectives, procedures and conclusions set forth in the outsourced internal audit reports. Consider:

     – Procedures performed.
     – Testing/sampling methods used.
     – Adequacy of sampling techniques utilized.
     – Risk and control assessments.
     – Approval of the internal audit manager.
     – Independence from external audit activities.

   - The scope of the outsourced internal audit procedures and work is adequate in light of risk and control assessments for the area audited.

   - The work program and audit reports adequately document material findings, including root causes of significant weaknesses, and whether follow-up on noted weaknesses and promised corrective action is adequate.

- Examiners should, as a result of centralized vendor reviews, perform additional testing or validation of the internal audit program at the individual bank level.

7. Determine whether the outsourcing arrangement maintains or improves the quality of the internal audit function and the institution's internal controls. Consider:

   - Scope and quality of internal audit work.
   - Overall internal control structure.
   - Audit and control evaluations.
   - Adherence with engagement terms
   - Consistency with audit policies, audit plans, and board and management expectations.
   - Vendor notification of any process, staffing, or other changes affecting contracted work

8. Determine whether the scope of outsourced audit work is revised appropriately when the bank's environment, activities, risk exposures, or systems change significantly.

9. If performing a centralized vendor review, discuss findings from above steps with the vendor and:

   - Draft a memorandum summarizing the results of the centralized vendor review. The memorandum should address the following as they pertain to each individual bank:
     - Adequacy of the vendor's work paper documentation.
     - The reliance of the audit work performed by the vendor.
     - Evaluation of the vendor's work, including the scope and timing of procedures, extent of testing, and basis of conclusions.
     - Recommendations to enhance the vendor's audit program.
     - Follow-up needed on any deficiencies noted and corrective action promised.
     - Recommended updates to OCC audit review strategies or scopes for individual banks.

   - Distribute the memorandum, customized as warranted, to each EIC of banks for which the vendor performs outsourced internal audit work.

- Bank EICs or portfolio managers should:
  - Use the memorandum to set the scope of and gain efficiencies in their bank examination.
  - Discuss centralized vendor review findings with the bank's board or audit committee and management.
  - Validate board of director and management oversight of the bank's internal audit program during the onsite examination, using appropriate objectives and steps from the internal audit examination procedures in this booklet.
  - Undertake additional testing or review of internal audit work papers, if desired or warranted, at the bank level during onsite examinations or other supervisory activities during a supervisory cycle. Examiners should base that decision on events occurring since the vendor review was performed and any other matters that come to their attention during supervisory activities (e.g., high-risk areas and new products and services).

10. Determine, by discussion with bank management and the vendor, whether the bank and its vendor have discussed and determined that applicable independence standards are being met. Examiners may want to provide bankers a copy of appendix G, "Auditor Independence Worksheet," to help them assess vendor independence. Consider the following:

    - If the vendor is a CPA who does not also perform the bank's financial statement audit, have any potential conflicts of interest been properly addressed?

    - If the vendor is a CPA who also performs the bank's financial statement audit and the bank is subject to 12 CFR 363, cite a violation of 12 CFR 363.3(a).

    - If the vendor is a registered public accountant who also performs the bank's financial statement audit and the bank's securities are registered with the OCC, cite a violation of 15 USC 78j-1(g)/17 CFR 210.2-01(c)(4).

11. Until May 6, 2004, determine whether publicly registered national banks and national banks subject to Part 363 comply with the SEC's

independence regulation issued in November 2000 regarding internal audit outsourcing services by considering whether:

- The public accountant:
  - Does not act or appear to act in a capacity equivalent to a member of bank management or as a bank employee.

  - Does not provide more than 40 percent of the total hours spent (by the bank, the accountant, and anyone else) on internal audit matters related to internal accounting controls, financial systems, financial statements, and matters affecting financial statements. Covered national banks with total assets less than $200 million are exempt from the 40 percent limit.

- The bank:
  - Acknowledges, preferably in writing to the vendor and the bank's audit committee or board, its responsibility to establish and maintain an effective system of internal accounting controls.

  - Designates a competent bank employee or employees, preferably within senior management, to be responsible for the internal audit function.

  - Determines the scope, risk, and frequency of internal audit activities, including those to be performed by the vendor.

  - Evaluates the findings and results arising from internal audit activities, including those performed by the vendor.

  - Evaluates the adequacy of the audit procedures performed and the findings resulting from performance of those procedures by, among other things, obtaining reports from the vendor.

  - Does not rely on the vendor's work as the primary basis for determining the adequacy of the bank's internal controls.

12. If there is sufficient reason to question the independence, objectivity, or competence of the vendor, discuss the situation with the ADC/EIC, the bank's board or audit committee, and the vendor to clarify or resolve the issues in the following manner:

- If appropriate, request through the bank that additional work papers be made available or meet with the vendor to discuss the concerns.

- If significant concerns remain unresolved, contact your OCC District Accountant or District Counsel, the Chief Accountant's office, or the Chief Counsel's office and discuss measures to be taken.

13. If the OCC determines that it cannot rely on the vendor's work, discuss that assessment with the board, bank management, and the affected party before finalizing the report of examination.

Objective 9: Determine the adequacy, effectiveness, and quality of the bank's directors' examination.

**Note:** When the director's examination consists of both internal and external audit work (i.e., serves as a bank's sole audit program with an independent external party using agreed-upon procedures), examiners should review a sample of the work papers dealing with traditional internal audit activities (e.g., internal control and operational reviews, transaction testing).

1. Determine whether the bank's bylaws require the board of directors to have independent parties periodically examine and report on the bank's affairs (i.e., require a directors' examination).

2. Determine whether directors, or a committee of directors, participate in the directors' examination at least to appraise the bank's policies and procedures and to review the directors' examination report with the auditors.

3. Determine whether the directors' examination focuses on major risk areas and internal controls and whether the independent parties:

   - Substantively test financial integrity.
   - Reconcile accounts.
   - Verify assets.
   - Complete internal control questionnaires and assess control risk.
   - Assess the quality of loans and investments.
   - Verify some or all call report data.
   - Review management information systems.

- Confirm the bank's compliance with laws, regulations, and internal policies.
- Review acquisition and/or merger activities.
- Review new products and services.

4. Review the directors' examination report findings and determine whether it addresses:

   - The bank's soundness.
   - The adequacy of internal controls.
   - The actions the board should take to address noted issues or problems.

5. Determine whether the board ensured that independent parties selected to perform the directors' examination possessed:

   - Sufficient knowledge and understanding of banking.
   - Knowledge and understanding of the bank's operations and activities.
   - Ability to apply accounting and auditing principles.
   - Familiarity with the bank's information systems and technology.

Objective 10: Determine whether the internal risk analysis processes are adequate for the bank's size, the nature and extent of its banking activities, and its risk profile.

1. Determine whether the bank has appropriate standards and processes for risk-based auditing and internal risk assessments. Such standards and processes should:

   - Identify businesses, product lines, services, or functions and the activities and compliance issues within those areas that should be audited.

   - Develop risk profiles that identify and define the risk and control factors to assess and the risk management and control structures for each business, product line, service, or function.

- Establish the process for grading or assessing risk factors for business units, departments, products, or functions, including time frames.

- Describe how the process is used to set audit plans, resource allocations, scopes of audits, and audit cycle frequency.

- Implement audit plans through planning, execution, reporting, and follow-up.

- Establish minimum documentation requirements to support scoring or assessment decisions and draw conclusions.

- Define when overrides of risk-based scores or assessments are acceptable or necessary, including which level of authority approves overrides.

- Provide for confirming the system regularly, i.e., annually or whenever significant changes occur within a department or function.

2. Select a sample of the bank's auditable entities (i.e., business lines, product lines, services, or functions) and determine the reasonableness of the internal risk analysis decision, including application of any risk models used.

3. Determine whether audit frequencies are reasonable and are being met.

   **Note:** In a risk-based audit system, banks set audit cycles based on risk scores/assessments. Customarily, banks may set audit cycles at 12 months or less for high-risk areas, 24 months or less for moderate-risk areas, and more than 24 months for low-risk areas. Individual circumstances at each bank will determine how it establishes audit cycle lengths.

4. If audit management has overridden risk-based audit schedules, discuss justifications with the audit manager.

5. If applicable, determine the quality and effectiveness of internal audit's ongoing monitoring of the bank's business operations.

## Objective 11: Determine whether the bank's fiduciary audit program complies with 12 CFR 9, Fiduciary Activities of National Banks

**Note:** Examiners should perform the following steps if they are not being performed as part of an asset management examination or review.

1. Determine whether the OCC has granted the institution the power to act in a fiduciary capacity (12 CFR 9.3).

   If so, proceed with steps 2 through 4 by reviewing previously requested materials.

2. Verify whether a suitable audit of the bank's significant fiduciary activities, including any audit reports that the internal auditors may have participated in or relied on to any extent, such as AICPA SAS 70, "Reports on the Processing of Transactions by Servicing Organizations," is conducted:

   - At least once during a calendar year (12 CFR 9.9(a)), or under a continuous audit system in conformance with 12 CFR 9.9(b).

   - Under the direction of the bank's fiduciary audit committee (12 CFR 9.9(a) and (b)).

   - With the results of the audit, including significant actions taken as a result of the audit, noted in the minutes of the board of directors (12 CFR 9.9(a)). Alternatively, under a continuous fiduciary audit program, results and actions of all discrete audits completed should be noted in board minutes at least once during each calendar year (12 CFR 9.9(b)).

3. Determine whether the institution has a fiduciary audit committee structured along the following lines (to comply with applicable provisions of 12 CFR 9.9(c)):

   - Members of the audit committee do not include officers who participate significantly in the administration of the bank's fiduciary activities (12 CFR 9.9(c)(1)).

- A majority of committee members are not also members of other committees delegated power to manage and control the bank's fiduciary activities (12 CFR 9.9(c)(2)).

4. If the bank has established collective investment funds, obtain the most recent audit of each fund and give it to the examiner responsible for reviewing that activity (12 CFR 9.18(b)(6)(l)).

## External Audit

Conclusion: The board of directors (has, has not) implemented and (does, does not) effectively oversees an external auditing function that is appropriate for the bank and that (complies/does not comply) with established statutory requirements and regulatory guidance.

Objective 12: Determine the adequacy of board oversight of the bank's external audit function.

1. Review board or audit committee minutes, or summaries thereof, as well as audit information packages submitted to the board or audit committee, and determine whether the following is noted:

   - Formal approval of the external audit program and schedule, or reasons supporting any decision to forgo an external audit program.

   - The monitoring of external audit reports to determine whether the approved external audit program and schedule is being followed.

   - The results of any vote taken regarding external audit.

   - Confirmation that the audit committee reviews external audit reports with management and the external auditors in a timely manner.

   - Discussion of the external auditor's independence.

2. Trace the distribution of the external audit reports to determine whether the external auditor reports to the board or audit committee.

3. Determine whether bank management responds appropriately and in a timely manner to external audit findings and recommendations.

4. Determine whether the activities of the external audit function are consistent with the institution's long-range goals and are responsive to its internal control and financial reporting needs.

5. Determine whether the board or its audit committee, at least annually, identifies the major risk areas in the institution's activities and assesses the extent of external auditing needed for each area.

6. Determine how the institution ensures that it files with the OCC and FDIC copies of audit reports and any management letters, qualifications, or other reports (including attestation reports) from the bank's independent public accountant within 15 days of receipt (12 CFR 363.4(c)).

**Note:** Which of the following steps to perform depends considerably on whether the auditor is a CPA or not. Other factors to consider are the examiner's familiarity with the external auditor's professional reputation, the extent of any previous validation/testing of the auditor's work, and whether problems or issues arise regarding the auditor's independence, objectivity, and competence.

Objective 13: Determine the extent of and reliability of work performed by the external auditors.

1. Determine whom the bank engages to perform the bank's external audit, i.e., CPA, certified information system auditor (CISA), or other independent parties.

2. If the bank is subject to 12 CFR 363, determine whether it has engaged an independent public accountant (IPA) to audit and report on its financial statements in accordance with generally accepted auditing standards (GAAS) (12 CFR 363.3(a)).

3. If the bank's securities are registered with the OCC, determine whether it has engaged an independent public accountant registered with the Public Company Accounting Oversight Board (Sarbanes-Oxley Act of 2002, Section 102(a)).

4. Determine whether, since the previous examination, the bank's external auditor terminated its services or the bank selected, changed, or terminated its external auditor. If so, and the bank is subject to 12 CFR 363, verify that the IPA and the bank properly notified the OCC and FDIC (12 CFR 363.3(c)) by submitting notification:

   - In writing.
   - Within 15 days of the event.
   - Giving reasons for the event.

5. Determine the type of external audit performed:

   - Financial statement audit.
   - Attestation on management's assertion of financial reporting internal control.
   - Balance sheet audit.
   - Agreed-upon procedures (e.g., director's examination, specialized audits such as IT, Fiduciary, or Compliance).

6. Obtain copies of:

   - ☐ Engagement letters.
   - ☐ Annual reports or other audit reports issued to the bank by the external auditor.
   - ☐ Other external audit reports, including audit reports that the internal auditors may have participated in or relied on to any extent, such as AICPA SAS 70 ("Reports on the Processing of Transactions by Servicing Organizations") audits.
   - ☐ Letters, communications, and other correspondence pertaining to external audits issued to or by bank management.

7. Arrange through the bank to meet with the external auditor. Examiners should communicate directly with external auditors early in the examination process (e.g., planning phase) and, as appropriate, throughout the supervisory cycle. Discuss the following topics:

   - Audit planning methodologies, risk assessments, sampling techniques, and (if applicable) 12 CFR 363 control attestation.

- How much the external auditors rely on the work of internal auditors.

- The extent of the external auditor's assessment and testing of financial reporting controls and how much the external auditor relies on those controls when auditing financial reports.

- Current examination and external audit results or significant findings.

- Upcoming external audit and examination activities.

- Reports, management letters, and other communications issued by the external auditors to the bank.

- Assigned audit staff experience and familiarity with banking and bank auditing, particularly in specialized areas.

- Any other pertinent information.

8. Read engagement letters covering audit activities or management advisory services (i.e., non-audit or consulting) performed by external auditors for the bank. Determine whether the letter addresses the following:

   - Purpose, scope, and fees of the audit or consulting services.
   - Period to be covered by the audit or consulting services.
   - Reports expected to be rendered.
   - Any limits on the scope of the audit or consulting services.
   - Examiner access to audit work papers.

9. Determine the type of opinion (unqualified, qualified, adverse, or disclaimer) rendered by an IPA or CPA from an audit of the institution's financial statements. If other than an unqualified opinion has been issued, discuss with the external auditor and determine the facts and circumstances that led to the opinion.

10. Review any SAS 70 report rendered, if applicable. Determine how reliable the report is in assessing overall audit effectiveness. An SAS 70

report should not be the sole factor in assessing overall audit effectiveness. Consider the scope of the audit, i.e., whether the auditor:

- Tested user controls at the institution or controls at the service organization, or
- Obtained and reviewed the service organization's report on controls placed in operation and tests of operating effectiveness.

11. Obtain copies of and review the following documents, as applicable, to determine whether there are any significant issues that should be followed up on with bank management or the external auditor:

    - *Communication of matters related to internal control structure* noted in the audit (commonly referred to as the SAS 60, material weakness, or no material weakness letter). This letter is issued when the auditor notes reportable conditions identified as material weaknesses in financial-reporting internal control and makes suggestions for improving the bank's control structure. If no material weaknesses are noted, the audit may, in some cases, issue a "no material weakness" letter.

    - *Communication with the audit committee* (commonly referred to as the SAS 61 letter). This communication, either orally or in written form, is required if the bank is subject to filing and reporting requirements of 12 CFR 11 and 16 (or publicly registered holding companies subject to SEC rules) and must cover:

        – Auditor responsibilities under GAAS,
        – Significant accounting policies,
        – Management judgments and accounting estimates,
        – Audit adjustments,(recorded and waived)
        – Auditor judgments about the quality of the bank's accounting principles,
        – Other information in documents containing audited financial statements,
        – Disagreements with management,
        – Consultation with other accountants,
        – Major issues discussed with management prior to retention, and
        – Difficulties encountered in performing the audit.

Prior to filing of annual reports issued after May 6, 2003, registered public accountants must also report to the audit committee:
  – All critical accounting policies and practices;
  – All alternative treatments of financial information within GAAP that have been discussed with bank management, including ramifications of the use of such alternate disclosures and treatments, and the treatment preferred by the firm; and
  – Other material written communications between the firm and bank management, such as management letters or schedules of unadjusted differences. (17 CFR 210.2-07(a))

- *Confirmation of audit independence* (required for banks subject to filing and reporting requirements of 12 CFR 11 and 16, and publicly registered holding companies subject to SEC rules). For affected banks, auditors must disclose, in writing, all relationships with the bank and its related entities that could affect the auditor's objectivity. They must also confirm they are independent in accordance with SEC requirements and discuss their independence with the bank's audit committee.

- Review any other communication (e.g., management letter) between the bank and the external auditor.

12. If any of the above communications are not in writing, discuss with the board of directors, its audit committee, and external auditor to determine why written communications were not requested or provided.

13. Obtain and review the list of audit differences or adjusting journal entries made and any list of waived adjustments. Determine whether such differences or entries indicate inadequate accounting records or controls.

14. If applicable, determine whether the IPA, in accordance with generally accepted standards for attestation engagements (GASAE), has examined, attested to, and reported separately on management's assertions concerning internal control structure and procedures for financial reporting (12 CFR 363.3(b)).

**Note:** Examiners are not required to review external audit work papers during a supervisory cycle. However, external audit work papers may be subject to OCC review if the examiner's review of internal audit discloses significant problems or issues (e.g., insufficient internal audit coverage), or if questions are otherwise raised about matters that are normally within the scope of an external audit program. IPAs are required to agree to provide examiners access to and copies of any work papers, policies, and procedures related to work performed under 12 CFR 363. When considering whether a review of external audit program work papers is warranted, examiners should discuss the request with bank management and the external auditor. Examiners should refer to the July 1994 AICPA interpretation of Statement on Auditing Standard (SAS) 41, *Working Papers*, entitled "Providing Access to or Photocopies of Working Papers to a Regulator" in the AICPA's *Professional Standards*. They should also consult with their ADC and District Accountant (EIC and Chief Accountant's Office for large bank examiners). These discussions may make the work paper review unnecessary or it may help examiners focus their review on the most relevant work papers.

When examiners request access to work papers, an audit firm might ask examiners to sign an acknowledgement letter (SAS 41, "Providing Access to or Photocopies of Working Papers to a Regulator"). If presented with such a letter, examiners should not sign it. Instead, they should complete the OCC acknowledgement letter template in appendix D and return it to the auditor with the auditor's original letter attached. If examiners have questions about the auditor's letter or an external auditor denies or prevents timely access to their work papers, they should contact their District Accountant and their District Counsel.

Examiners should not make a blanket request to review all external audit work papers; examiners should make their requests specific to areas of greatest interest and give the reasons for the request. Examiners should also consider requesting that the auditor make available, for the specific areas under review, related planning documents and other information pertinent to the area's audit plan (including the sample selection process). When the audit work papers support holding company financial statement audits or attestation reports, examiners should coordinate reviews with appropriate OCC supervisory offices and other regulators.

**If reviewing external audit work papers, perform steps 15 and 16. If not, skip to step 17.**

15. Consider asking to review appropriate external audit work papers if the following circumstance exist:

    - Unexpected or sudden changes in the bank's external auditor. Examiners should have discussions with the previous and current external auditor before embarking on a work paper review. If the discussions raise unanswered questions that might be addressed in the work papers, then a work paper review may be warranted

    - Significant changes in the bank's external audit program. Examiners should contact the external auditor to discuss these changes and determine whether a review of work papers is warranted.

    - Significant and unexpected changes in accounting or operating results. Examiners should discuss such changes with the external auditor and determine whether a review of work papers is warranted.

    - Issues that affect the bank's safety and soundness. There may be instances when the external auditor raises safety and soundness concerns, or when examiners or internal auditors surface safety and soundness concerns in areas normally within the scope of an external audit program. In such cases, examiners should obtain information from the bank, discuss the issues with bank management and the external auditor, and consider reviewing work papers related to those matters or findings.

    - Issues about the independence, objectivity, or competence of the external auditor.

    - Recalcitrant external audit firm or staff.

16. Determine (and discuss with the external auditor as warranted) whether selected work papers contain information documenting whether:

    - A written audit program (including appropriate audit procedures) was in place for the area audited.

    - Work was adequately planned and supervised.

- Sufficient understanding of internal control was obtained to plan the audit and determine the nature, timing, and extent of tests to perform.

- Audit procedures obtained sufficient competent evidential material to provide a reasonable basis for the audit opinion or conclusion about:
  - Sampling and testing bases and results.
  - Risk assessments.
  - Whether accounting records agree/reconcile with financial statements or other information reported on.
  - Supporting documentation of audit findings or issues that in the auditor's judgment are significant, actions taken to address the issues, and the basis for the conclusions reached.

17. If, after performing the preceding steps, significant concerns remain about the adequacy of external audit, internal controls, financial control integrity, or the accuracy of the audit opinion rendered, consider whether to perform **verification procedures** or complete **internal control questionnaires** for the applicable areas of concern. Verification procedures are required in certain situations. See "Supervisory Process and Validation" section of this booklet for specific details.

    In lieu of performing verification procedures themselves, examiners may request that for areas containing weaknesses or deficiencies:

    - The bank perform verification procedures, or
    - The bank ask its external auditor or other independent third party to perform verification procedures.

    If one of the latter two alternatives is chosen, follow-up with a review of applicable work papers to ensure that identified supervisory issues are resolved in a timely manner.

Objective 14: Review the independence and objectivity of those who provide the external audit function.

**Note:** Examiners may want to use, or provide to bankers, appendix G, "Auditor Independence Worksheet," to help them assess auditor independence.

1. Determine whether the board of directors (or its audit committee) and the external auditor have discussed any financial, employment, business, or non-audit service relationships that compromise or appear to compromise the external auditor's independence:

   - If the bank is subject to Part 363 or has its securities registered with the OCC, has the audit committee pre-approved all audit, review, and attest engagements, including any non-prohibited non-audit services? (17 CFR 210.2-01(c)(7))

   - Has any partner, principal or shareholder of the audit firm that was a member of the audit engagement team, at any point during the audit engagement period, earned or received compensation based on the performance of, or procuring of, engagements with the bank to provide any products or services other than audit, review, or attest services? (17 CFR 210.2-01(c)(8))

2. Review available documentation (e.g., board or audit committee meeting minutes, written communications between the bank and the external auditor) or arrange a meeting with knowledgeable bank officials and the external auditor to determine whether they discussed:

   - Employment relationships between the bank and the accountant, such as:
     – The accountant being employed by the bank or serving as a bank director or in a similar management role.
     – An accountant's close family members or a former accountant being employed by the bank in an accounting or financial reporting oversight role.
     – A former bank officer, director or employees becoming an employee of the accountant.

     **Note:** Effective May 6, 2003, if a bank is subject to Part 363 or if its securities are registered with the OCC, a registered independent public accounting firm is prohibited from auditing the bank's financial statements if the bank's chief executive officer, controller,

chief financial officer, chief accounting officer, or person serving in a similar position was employed by the accounting firm and participated in any capacity in an audit of the bank that took place within 12 months of the start of the current audit of the bank. (17 CFR 210.2-01(c)(2)(iii)(B))

- Direct or material indirect financial interests between the accountant and the bank, such as:
  - Investments in the bank or bank investment in the accounting firm.
  - The bank underwriting securities issued by an accounting firm.
  - Loans to or from the bank.
  - Savings and checking accounts in amounts exceeding FDIC insurance coverage.
  - Broker/dealer accounts.
  - A futures commission merchant account.
  - Credit card accounts greater than $10,000.
  - Insurance products issued by the bank.
  - Investment company associated with the bank.

- Direct or material indirect business relationships of the accountant with the bank or persons associated with the bank in decision-making capacities, such as an officer, director, or substantial stockholder.

- The accountant providing non-audit services to the bank, such as:
  - Bookkeeping or other services related to the bank's accounting records or financial statements.
  - Financial information system design and implementation.
  - Appraisal or valuation services, fairness opinions, or contribution-kind reports.
  - Actuarial services.
  - Acting as a bank director, officer or employee or performing decision-making, supervisory, or ongoing monitoring functions.
  - Human resources.
  - Broker/dealer, investment advisor, or investment banking services.
  - Legal and expert services not related to the audit.

**Note:** Effective May 6, 2004 (for services under contract prior to May 6, 2003), the external auditor **cannot** perform the above non-audit services for the bank if the bank is subject to 12 CFR 363 or if it is publicly registered and the external auditor is a registered public accountant who performs the bank's financial statement audit. (17 CFR 210.2-01(c)(4))

- The accountant providing, during an audit period for the bank, any service or product to the bank for a contingent fee or a commission or receiving from the bank any contingent fee or commission.

- The external auditor also performing any of the bank's outsourced internal audit work. If so, perform steps 10 through 12 under objective 8 to determine that the auditor's independence is not compromised and is maintained in accordance with established rulings and guidelines.

- The professional reputation of the auditors.

3. Determine whether the bank has recently changed external auditors and discuss with appropriate bank management the reasons for such change. Particular attention should be given to disagreements between the external auditor and management about the appropriate accounting principles applicable to specific transactions or matters.

   **Note:** Effective May 6, 2003, lead and concurring partners of the audit engagement team will have to rotate out of the bank's audit engagement team after participating for five consecutive years and remain out of the audit engagement team for five years. In addition, significant audit partners will have to rotate out after seven years and remain out of the audit for two years. (17 CFR 210.2-01(c)(6))

4. Arrange through the bank to meet with non-CPA external auditors, if applicable, to discuss relevant education and experience. Consider the following:

   - Level of education attained, including any training in specialized areas such as capital markets, information systems, fiduciary activities, and subsidiary activities.

- Significant banking industry audit experience, including specialized areas.

- Certification as a chartered bank auditor, certified internal auditor, etc.

- Their commitment to a program of continuing education and professional development.

5. If, in performing the preceding steps, there is sufficient reason to question the external auditor's work, independence, objectivity, or competence:

   - Meet with the external auditor to discuss the situation and, if appropriate, request additional work papers be made available.

   - If significant concerns are unresolved, discuss the issues with the board of directors, bank management, and the affected party.

   - Contact OCC staff (district accountant, chief accountant's office, or chief counsel's office as appropriate) before finalizing the report of examination.

## Overall Conclusions

Conclusion: The quality of the bank's audit function is (strong, satisfactory, weak)

Objective 15: Determine the overall conclusions for the bank's audit function.

1. Prepare written conclusion summaries, discuss findings with the EIC, and communicate findings to management. Areas to be covered should include:

   - The ability and effectiveness of the bank's audit processes to assess and detect risk in bank operations.

   - The adequacy of audit policies, procedures, programs, and the board's or audit committee's oversight.

- Whether internal and external auditors and outsourced vendors operate in conformance with established policies, standards, rules, and regulations.

- The adequacy and availability of information about, or generated by, the audit function and provided to management and the board of directors or its audit committee.

- Significant areas of weaknesses identified by internal or external audits and management's progress in correcting those weaknesses.

- Internal or external audit report findings not acted upon by management as well as any other concerns or recommendations resulting from the review of audit functions.

- Recommended corrective actions, if applicable, and management's commitments.

- Assignment of an overall audit rating of strong, satisfactory, or weak.

2. Determine how the quality of the audit function affects the aggregate level and direction of OCC risk assessments. Examiners should refer to guidance provided under the OCC's risk assessment programs for large banks and community banks.

3. Determine, in consultation with the EIC, whether identified issues or concerns are significant enough to merit bringing them to the board's attention in the report of examination.

   If so, prepare comments for inclusion under the heading "Matters Requiring Attention" (MRA). MRA comments should address practices that (1) deviate from sound fundamental principles and are likely to result in financial deterioration if not addressed or (2) result in substantive noncompliance with laws or internal policies or processes. The examiner should provide details regarding:

   - The problem's causes.
   - Consequences of inaction.
   - Management's commitment to corrective action.

- The time frame for any corrective action and who is responsible for the action.

4. Prepare a comment on audits for inclusion in the report of examination taking into consideration the requirements of 12 CFR 30. The comment should address:

   - The adequacy of audit policies, processes, personnel, control systems, overall audit programs, and board/audit committee oversight.

   - Significant problems discerned by the auditors that have not been corrected.

   - Any deficiencies or concerns reviewed with management, any corrective actions recommended by examiners, and management's commitment(s) to corrective actions.

5. **Give serious consideration to citing a violation of 12 CFR 30 if audit is rated "Weak" because of significant deficiencies in the internal audit function or its oversight, if MRAs pertaining to internal audit are being put in the report, or if enforcement actions being recommended include internal audit-related articles.**

6. Prepare a memorandum to update OCC audit work programs with any information that will facilitate future examinations. Make recommendations about the scope of the next audit review and recommend whether audit findings should change the scopes of other supervisory activity reviews.

7. Update the OCC databases. For fiduciary, information system/technology, and compliance examinations, update the applicable audit component rating and communicate audit findings/rating to the appropriate EIC for incorporation into the UITRS, URSIT, or compliance rating systems.

8. Organize and reference working papers in accordance with PPM 5400-8, "Bank Supervision: Supervision of Work Papers."

**Appendixes ..... 108**
A: Statutory and Regulatory Requirements ..... 108
B: Part 363 Annual Report Worksheet ..... 119
C: Part 363 Periodic Report Worksheet ..... 122
D: OCC Acknowledgement of CPA Work Paper Request Letter ..... 123
E: Internal Audit Review Worksheet ..... 124
F: Audit Function Questionnaire ..... 131
G: Auditor Independence Worksheet ..... 148
H: Board/Audit Committee Oversight Worksheet ..... 162
I: Audit Rating Guidance-Community Banks ..... 171
J: Audit Rating Guidance-Large/Mid-size Banks ..... 176

**References ..... 182**

# Appendix A: Statutory and Regulatory Requirements

By law, national banks must adhere to certain requirements regarding internal and external auditing functions. These requirements ensure that banks operate in a safe and sound manner, accurately prepare their financial statements, and comply with other banking laws and regulations.

## Operational and Managerial Standards

In July 1995, the OCC issued 12 CFR 30, Safety and Soundness Standards, establishing operational and managerial standards for all national banks. Some of these standards are for internal audit systems. According to appendix A to 12 CFR 30, a national bank should have an internal audit system that is appropriate to the size of the bank and the nature and scope of its activities. The appendix states that the audit system should provide for:

- Adequate monitoring of the system of internal controls through an internal auditing function. For a bank whose size, complexity or scope of operations does not warrant a full-scale internal auditing function, a system of independent reviews of key internal controls may be used.
- Independence and objectivity.
- Qualified persons.
- Adequate testing and review of information systems.
- Adequate documentation of tests and findings and any corrective actions.
- Verification and review of management actions to address material weaknesses.
- Review by the bank's audit committee or board of directors of the effectiveness of the internal auditing systems.

## Compliance Activities

All banks are required by 12 CFR 21.21 to have a board approved BSA compliance program that provides:

- An internal control system that assures ongoing compliance.
- Independent testing for compliance conducted by bank personnel or outside parties.
- Designation of bank personnel responsible for coordinating and monitoring day-to-day compliance.
- Training for appropriate personnel.

**Federal Securities Laws**

National banks that register their securities with the OCC are subject to the public and periodic filing and reporting requirements of 12 CFR 11 and 12 CFR 16.20[32] and are subject to the SEC's regulations on financial statement form, content, and other requirements. Bank holding companies that register their securities with the Securities and Exchange Commission (SEC) are also subject to the SEC's regulations on financial statement form, content, and other requirements.

17 CFR 210.2-01, Qualifications of Accountants, addresses the qualifications and independence of independent public accountants (IPAs) engaged to perform services for companies with a class of securities registered pursuant to the Securities Exchange Act of 1934.

17 CFR 210.10-01, Interim Financial Statements, requires that IPAs must review interim financial statements included in a company's quarterly 10-Q reports using procedures in SAS 71, "Interim Financial Information."

17 CFR 229.306, Audit Committee Report, requires disclosures relating to the functioning of corporate audit committees. As part of proxy and information statements for meetings at which directors are to be elected, an audit committee report must be made which states whether the audit committee:

[32] Part 11 banks have the same reporting obligations as those companies with a class of securities registered under the Securities Exchange Act of 1934 (filing of periodic reports such as Form 10K, Form 10Q, proxy materials, Form 8K etc.). 12 CFR Part 16.20 is a similar requirement of a bank offering securities under the Securities Act of 1933, subjecting them to reporting under Section 15(d) of the SEC Act. (filing Form 10K, Form 10Q and Form 8K).

- Reviewed and discussed audited financial statements with management.

- Discussed with the company's IPA the matters required to be discussed by SAS 61, "Communication with Audit Committees."

- Received the written disclosures and the letter from the IPA (as required by Independence Standards Board Standard No. 1, "Independence Discussions with Audit Committees"), and discussed the IPA's independence with the IPA.

- After taking the preceding actions, recommended to the board of directors that the audited financial statements be included in the company's annual report.

Section 306 also requires that the name of each member of the company's audit committee appear below the above disclosures. In the absence of an audit committee, the names of the board committee performing the equivalent functions or the entire board must appear.

17 CFR 240, Section 14a-101, Items 7 and 9, includes the following requirements if a registrant has an audit committee:

- Provide the information required by 17 CFR 229.306.
- State whether the board of directors has adopted a written charter for the audit committee.
- Include a copy of the written charter, if any, as an appendix to the proxy statement at least once every three years.
- Disclose audit committee financial expertise, or why there are no financial experts on the committee.
- Disclose fees paid to the external auditor.
- Disclose the audit committee's pre-approval policies and procedures.

**Annual Independent Audit and Reporting Requirements**

Following are the specific requirements of 12 CFR 363 (Part 363) on auditing, reporting, and audit committees. The requirements are applicable to all national banks with total assets of $500 million or more.

**Reports to Regulators.** National banks with $500 million or more in total assets must send the following reports to the FDIC and the appropriate OCC supervisory office:

- An annual report, due within 90 days after the fiscal year-end, consisting of:
  - Financial statements that include:
    - Comparative consolidated financial statements for each of the two most recent fiscal years prepared in accordance with generally accepted accounting principles and audited in accordance with generally accepted auditing standards by an independent public accountant; and
    - An audit report.
  - A management report that contains:
    - A statement of management's responsibilities for financial statements, establishing and maintaining an internal control structure 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 bank's internal control structure and procedures for financial reporting as of the end of the fiscal year (internal controls that safeguard assets, such as loan underwriting and documentation standards, must be considered) and the bank's compliance with designated laws and regulations during the most recent fiscal year.
  - A report by the independent public accountant attesting to management's assertions regarding internal control structure and procedures for financial reporting. The attestation is to be made in accordance with generally accepted standards for attestation engagements.

- Management letters and certain reports prepared for the bank, due 15 days after they are received, that include:

  – Audit reports and any qualification to the audit reports;
  – Any management letter; and
  – Any other reports, including attestation reports, from the independent public accountant.
  – A notification of the selection, change, or termination of the bank's independent public accountant, due within 15 days after the event. The report must include a statement of the reasons in sufficient detail for the examiner to evaluate the decision.

Independent public accountants for covered banks must file a report of termination of services, due within 15 days of the event. The report must be filed with the FDIC and the appropriate OCC supervisory office.

**Filing Reports.** Covered national banks, including covered branches of foreign banks, are required to file **two** copies of each required report at each of **two** locations – the appropriate OCC supervisory office and the appropriate FDIC regional office. Of the OCC's copies, one will be maintained at the supervisory office, and the other will be forwarded to the bank's portfolio manager. The exception to this rule is the independent accountant's peer review report, which is required to be filed only with the FDIC.

**Disclosing Reports.** Annual reports required by Part 363 are available to anyone, from the bank, upon request. However, the OCC may designate certain information as privileged and confidential; such information may not be available to the public.

The peer review report is also publicly available. The list of clients subject to Part 363, however, is exempt from public disclosure.

**Reports to Independent Accountants.** Every covered national bank also must provide its independent public accountant with copies of the following reports:

- Its most recent OCC examination report and related correspondence;

- Its most recent Reports of Condition and Income or Report of Assets and Liabilities of U.S. Branches and Agencies of Foreign Banks; and

- Any supervisory memoranda of understanding, written agreements, requests for corrective action, notice of intent to commence an action, record of enforcement action taken, or notice of change in the bank's prompt corrective action capital category during the audit period.

**Reports to the FDIC Only.** Independent public accountants for covered national banks must file the following reports with the Washington office of the FDIC:

- A peer review report for each covered bank or, if no peer review has been performed, a statement of the accountant's enrollment in a peer review program. This report is due within 15 days of receipt, or prior to commencing any services under Part 363; and

- A list of clients subject to Part 363, due at the accountant's option as a substitute for the peer review report or statement for each client.

**Special Reporting Situations.** *Consolidated Reporting by Holding Company Subsidiaries* -- A chart at the end of this appendix summarizes the responsibilities of holding company member banks. To simplify, any national bank that is a subsidiary of a holding company may, regardless of its size, file the audited consolidated financial statements of the holding company in place of separate financial statements.

All other report and notice requirements of the rule may be satisfied at the holding company level if:

- The bank has assets of less than $5 billion **or** of $5 billion or more with a composite CAMELS rating of 1 or 2, and

- The holding company provides the bank with comparable services and functions for other required reports and notices by:

  – Preparing reports used by subsidiary national banks to meet Part 363 requirements,

  – Having an audit committee that meets Part 363 requirements appropriate to its largest subsidiary bank, and

– Preparing and submitting reports on internal control and compliance with designated laws based on the activities and operations of all subsidiary banks.

*Reporting by Insured U.S. Branches of Foreign Banks* -- Under the guidelines, insured branches of foreign banks may satisfy the financial statement requirement by filing:

- Audited balance sheets that also disclose information about financial instruments with off-balance-sheet risk;

- Audited call report schedules RAL and L of form FFIEC 002 (the Report of Assets and Liabilities of U.S. Branches and Agencies of Foreign Banks); **or**

- Consolidated financial statements of the parent company, if approved in writing by the OCC's appropriate supervisory office. Since consolidated financial statements do not necessarily provide relevant information about the branch, requests should be considered only in rare and unusual circumstances and any approvals should cover only a specified time period.

*Reporting by Merged or Consolidated Institutions* -- Insured national banks that had more than $500 million in total assets at the beginning of their fiscal year, but that no longer exist as a separate entity at the end of their fiscal year, have no responsibility under this rule to file reports due after the date they cease to exist.

A covered bank that merged into another institution after the end of the fiscal year but before its annual report and other reports must be filed under this rule should still submit reports to the FDIC and the appropriate OCC supervisory office.

National banks should consult with its OCC supervisory office concerning the statements and reports that would be required under such circumstances.

**Audit Committee Requirements.** National banks with total assets of $500 million or more must have independent audit committees that meet the following standards:

- The committee must be made up entirely of outside directors of the bank.

- The members must be independent of the management of the bank. The guidelines accompanying the Part 363 rule outline factors that should be considered in determining independence.

  NOTE: Exceptions to the independent audit committee membership requirements may be granted in certain circumstances. Some insider directors may be allowed to serve on the audit committee if the OCC determines that the bank has encountered a hardship in retaining and recruiting competent outside directors. However, in no circumstances may the audit committee be made up of less than a majority of outside directors. Exceptions to the independent membership requirement should be rare and should be approved by the OCC's Office of the Chief Accountant.

- The committee's duties must include reviewing the basis of the reports required under Part 363, with management and the independent public accountant.

For banks with total assets of more than $3 billion, the audit committee also must:

- Include at least two members with banking and related financial management expertise.

- Not include any "large customers" of the banks.

  Any individual or entity (including a controlling person of a company) whose relationship with the bank (credit or otherwise, direct or indirect) is so significant that termination of the relationship would materially and adversely affect the bank's financial condition or results of operations should be considered a "large customer."

- Have access to the committee's own outside counsel.

**Special Audit Committee Situations**. *Bank Holding Company Subsidiary Banks* – For banks that are subsidiaries of a holding company, the audit committee requirement may be satisfied at the holding company level if:

- The bank has assets of less than $5 billion **or** of $5 billion or more with a CAMELS composite rating of 1 or 2, and

- The holding company provides the bank with comparable services and functions for required other reports and notices by:

  – Preparing reports used by subsidiary banks to meet Part 363 requirements,

  – Having an audit committee that meets Part 363 requirements appropriate to its largest subsidiary bank, and

  – Preparing and submitting reports on internal control and compliance with designated laws based on the activities and operations of all subsidiary banks.

A holding company subsidiary bank must have its own audit committee if the bank has total assets of $5 billion or more and a CAMELS composite rating of 3 or worse.

A holding company subsidiary bank's audit committee may be composed of the same persons as the holding company's audit committee **only** if such persons are:

- Outside directors of the holding company and the bank subsidiary, and
- Independent of management of the holding company and the bank.

Even in such situations, each audit committee must meet and maintain separate minutes of its meetings.

*Branches of Foreign Banks* – Because branches of foreign banks do not have separate boards of directors, the audit committee requirements do not apply. However, insured branches of foreign banks are encouraged to make a good faith effort to see that duties similar to those described for the audit committee are performed by persons whose experience is generally consistent with the requirements.

**Implementation.** Every covered national bank was required to have established an audit committee by November 2, 1993. If the bank's audit committee did not meet the independence or other applicable criteria at that

time, the bank had until the next annual stockholders' meeting or July 2, 1994, whichever was earlier, to structure the committee to comply.

Insured national banks that subsequently become subject to Part 363 requirements must form an independent audit committee within four months of the beginning of the first fiscal year in which they are covered. An insured national bank that becomes covered by the large bank requirements by growing to have total assets of more than $3 billion must ensure that its audit committee meets the additional requirements by the next annual meeting of stockholders, or within six months of the beginning of its fiscal year, whichever is earlier.

**Independent Accountant Eligibility Requirements.** The independent public accountant must satisfy certain requirements to perform an audit or attestation for a covered bank. Specifically, the accountant must:

- Be enrolled in an acceptable peer review program, and

- File the peer review report (or a statement certifying enrollment in a peer review program if no peer review has yet been completed) with the Registration and Disclosure Section of the FDIC Washington office.

The report or statement must be filed within 15 days after the accountant receives notice that the peer review has been accepted by the appropriate practice section or other governing group, or before commencing the audit, whichever is earlier.

The following table illustrates applicability of Part 363 requirements for subsidiary banks of holding companies:

# Part 363 Applied to Subsidiary Banks

| Insured Depository Institutions–Subsidiaries of Holding Companies with Assets of: | Audit Committee Requirements* | Reporting Requirements |
|---|---|---|
| Less than $500 million | None** | None** |
| $500 million to $3 billion | Committee must consist entirely of independent outside directors and may be satisfied at the holding company level. | Annual report, including:<br>• Audited financial statements,<br>• Audit report,<br>• Management report, and<br>• Independent public accountant's report on the internal controls over financial reporting.<br><br>Requirement may be satisfied at the holding company level. |
| $3 billion to $5 billion<br><br>and<br><br>$5 billion or more and CAMELS composite rating of 1 or 2. | Committee must:<br>• Consist entirely of independent outside directors,<br>• Include members with banking and related financial management expertise,<br>• Have access to its own outside counsel, and<br>• Not include large customers of the bank.<br><br>Requirements may be satisfied at the holding company level. | |
| $5 billion or more and CAMELS composite rating of 3 or worse. | Committee requirements same as above, but must be satisfied at the bank level. | Banks may submit holding company financial statements and audit reports, but all other reports listed above must be at the bank level. |

* Exceptions to the independent outside member requirement may be made when the OCC determines the bank has encountered a hardship in retaining or recruiting a sufficient number of competent outside directors. However, the audit committee may not be made up of less than a majority of outside directors.

** However, the banking agencies continue to encourage all institutions, regardless of size, to have annual audits and to establish audit committees made up entirely of outside directors.

NOTE: The appropriate federal banking agency may require a bank with total assets of $9 billion or more to comply with requirements of Part 363 at the bank level if the agency determines that exemptions as noted above, if applied to the bank, would create a significant risk to the deposit insurance fund.

# Appendix B: Part 363 Annual Report Worksheet*

| Name of Reporting Institution or Holding Company | Charter No. |
|---|---|
| City and State | Date Received |
| Name and Address (City, State) of Independent Accountant | Year End |
| If Holding Company, Names and Addresses of Subsidiary Institution(s) subject to Part 363 (attach list if needed) | Date of Last Peer Review |
| | Reviewer |

ANNUAL REPORT (Check attachments)

☐ Financial Statements and Notes ☐ Audit Report ☐ Management Report

☐ Independent Public Accountant's Attestation on Internal Controls

REVIEWER Complete all sections and the following questions:

Describe any item in the report that may adversely influence the institution's safety and soundness (reference should be made to the discussion in following sections I and II.)

| AS A RESULT OF THIS REVIEW, IS ANY FOLLOW-UP ACTION REQUIRED OR CHANGE IN SUPERVISORY STRATEGY WARRANTED? | YES ☐ | NO ☐ |
|---|---|---|

If yes, attach a memorandum outlining your recommendations.

* A new copy of this worksheet should be prepared each year upon receipt of either the annual report or the Laws and Regulations Attestation Report. Review of any other reports received periodically should be recorded on the "Part 363 Periodic Reports Worksheet".

I. ANNUAL REPORT

AUDIT REPORT

Do the report and financial statements cover a holding company or an individual institution? HC ☐ INST ☐

Has the report been signed and dated? YES ☐ NO ☐

Does it have any explanatory paragraphs in addition to the three paragraphs of the standard auditor's report? YES ☐ NO ☐

If yes, briefly describe the matter(s) covered in these paragraphs.

FINANCIAL STATEMENTS AND NOTES

Compare the information presented in the audited financial statements and the most recent available financial information from call report or examination report. Describe and discuss any differences or changes material to the institution between significant items on the statements and the call or examination report.

Briefly describe any unusual transactions or valuation methods described in the financial statements and accompanying notes that may influence the institution's safety and soundness including, but not limited to, those in the following areas:

| | |
|---|---|
| Securities | Loans and Leases |
| Derivatives | Servicing Rights |
| Other Real Estate | Allowance for Loan and Lease Losses |
| Related Party Transactions | Taxes |
| Pensions or Deferred Compensation Plans | Off-Balance-Sheet Activities |
| Business Combinations/Pushdown Accounting | Nontraditional Activities |

MANAGEMENT REPORT

| | | |
|---|---|---|
| Does the report cover a holding company or an individual institution? | HC ☐ | INST ☐ |
| Has the report been signed by both the CEO and the CFO/Chief accounting officer? | YES ☐ | NO ☐ |
| Does it state management's responsibilities for: | | |
| Preparing financial statements? | YES ☐ | NO ☐ |
| Establishing and maintaining an adequate internal control structure and procedures for financial reporting? | YES ☐ | NO ☐ |
| Complying with designated laws and regulations? | YES ☐ | NO ☐ |
| Does it assess the: | | |
| Effectiveness of the aforementioned internal controls at the end of the most recent year? | YES ☐ | NO ☐ |
| Compliance with the designated laws and regulations during the year? | YES ☐ | NO ☐ |

Briefly describe any instances of ineffectiveness or noncompliance reported by management or apparent deficiencies in reporting.

INDEPENDENT PUBLIC ACCOUNTANT'S ATTESTATION ON INTERNAL CONTROLS

| | | |
|---|---|---|
| Has the report been signed and dated? | YES ☐ | NO ☐ |
| Does it indicate material weaknesses in the internal control structure and procedures for financial reporting? | YES ☐ | NO ☐ |

If so, briefly describe:

# Appendix C: Part 363 Periodic Report Worksheet*

| | |
|---|---|
| Name of Reporting Institution or Holding Company | Charter No. |
| City and State | Date Received |
| Name and Address (City, State) of Independent Accountant | Year End |
| If Holding Company, Names and Addresses of Subsidiary Institution(s) subject to Part 363 (attach list if needed) | Date of Last Peer Review |
| | Reviewer |
| REPORT FILED<br>☐ Change of Accountant Report ☐ Termination of Services Report<br>☐ Management Letter ☐ Other Report (Describe) | |
| REVIEWER -- Complete the following sections: | |
| Describe briefly any item in the report that may adversely influence the institution's safety and soundness. | |
| AS A RESULT OF THIS REVIEW, IS ANY FOLLOW-UP ACTION REQUIRED OR CHANGE IN SUPERVISORY STRATEGY WARRANTED? YES ☐ NO ☐<br>If yes, attach a memorandum outlining your recommendations. | |

* A separate copy of this worksheet should be completed upon receipt of each periodic report received. The "Annual Report Worksheet" should be used for the annual report.

# Appendix D: OCC Acknowledgement of CPA Work Paper Request Letter

When examiners request access to external audit work papers, the external auditor may submit a "work paper access" letter to the examiner or the supervisory office along with a request to acknowledge its receipt. Examiners may use the following template as a written acknowledgement and response if presented with such a letter. They should attach the OCC acknowledgement to the external auditor's original letter and return both to the external auditor. Examiners should also retain a copy of the external auditor's letter and the OCC acknowledgement letter.

_____

[Date]

[Name of firm]

We are in receipt of your letter dated [Insert Date] regarding providing us access to or copies of work papers associated with your [Insert Date of audit] audit of [Insert bank/company name] (see copy attached).

This letter serves as our acknowledgement to confirm receipt of your letter, but does not constitute agreement to any terms specified in your letter that limit our ability to supervise the bank.

We also acknowledge your request for confidential treatment under the Freedom of Information Act or other applicable law. Any request by a third party for disclosure of the information for which you have requested such treatment will be processed pursuant to our regulations governing such requests, which are promulgated at 12 CFR 4.

Office of the Comptroller of the Currency

By: _____ Date: _____

# Appendix E: Internal Audit Review Worksheet

This worksheet is designed as a tool to help examiners evaluate the quality of internal audit programs, work papers, and related reporting for individual bank departments, activities, products, or services. If completed, the worksheet should be provided to the lead audit review examiner to facilitate an overall internal audit assessment. Use of the worksheet is not mandatory.

Unit Audited: _____ Date of audit report: _____
Auditor in Charge: _____ Audit Frequency: _____
Audit Rating: _____ Agree w/Rating: ____ Y ____ N
Management Response: ____ Y ____ N Response Adequate: ____Y ____ N
Risk Rating: _____
Examiner's Summary Comment:

| ***Scope*** | | |
|---|---|---|
| 1. Was the scope of the audit adequate? | ____ Yes<br>____ No | Why or why not: |
| | | |
| 2. Comment on quality of the planning document. | ____ Adequate<br>____ Inadequate<br>____ Not Applicable | Why: |
| | | |
| 3. Is the audit frequency appropriate relative to the level of risk in the area/unit? | ____ Yes<br>____ No | Why or why not: |
| | | |
| 4. Is any portion of this audit outsourced? | ____ All<br>____ Partial<br>____ Not Applicable | |
| a. If so, is the arrangement compliant with OCC 2003-12? | ____ Yes<br>____ No | Why not: |
| b. If so, is the audit work of sufficient detail to draw appropriate conclusions? | ____ Yes<br>____ No | Why not: |
| | | |

| **Risk Assessment** | | |
|---|---|---|
| 5. Were risk assessment matrices used to describe the risk(s)? | ____ Yes<br>____ No | Why not: |
| a. If yes, were they sufficient? | ____ Yes<br>____ No | Why not: |
| | | |
| 6. Was risk assessment used to determine when to audit this area? | ____ Yes<br>____ No | Why not: |
| | | |
| 7. Was risk assessment used to determine the scope of the audit? | ____ Yes<br>____ No | Why not: |
| | | |
| 8. Is the risk assessment of this area adequate? | ____ Yes<br>____ No | Why not: |
| | | |
| ***Audit Work/Findings*** | | |
| 9. Were the audit program and procedures sufficient? | ____ Yes<br>____ No | Describe the deficiencies: |
| | | |
| 10. Were audit procedures performed to ensure compliance with applicable: | | |
| a. Policies | ____ Yes<br>____ No<br>____ Not Applicable | |
| b. Procedures? | ____ Yes<br>____ No<br>____ Not Applicable | |
| c. Plans? | ____ Yes<br>____ No<br>____ Not Applicable | |
| d. Laws/regulations? | ____ Yes<br>____ No<br>____ Not Applicable | |
| | | |
| 11. Were internal controls for the area sufficiently detailed? | ____ Yes<br>____ No | |
| | | |

| | | |
|---|---|---|
| 12. Did the audit contain tests of administrative or operational: | | |
| a. Controls? | ____Yes<br>____ No | |
| b. Policies? | ____ Yes<br>____ No | |
| c. Procedures? | ____ Yes<br>____ No | |
| | | |
| 13. Did the audit note the root cause of deficiencies or symptoms of problems? | ____ Root Cause<br>____ Symptom<br>____ Both<br>____ Not Applicable | |
| | | |
| 14. Was a review of pertinent MIS performed as part of the audit? | ____ Yes<br>____ No<br>____ Not Applicable | Why not: |
| | | |
| 15. What is the quality of the procedures documentation? | ____ High<br>____ Acceptable<br>____ Unacceptable | Support: |
| a. Are audit trails sufficient? | ____ Yes<br>____ No | Why not: |
| | | |
| 16. How well does the audit describe the risk represented in individual findings or groups of findings? | ____ Well<br>____ Acceptable<br>____ Unacceptable<br>____ Not Applicable | Support: |
| | | |
| 17. If the area/unit is internally rated satisfactory, how well does the audit mitigate the existence of significant findings? | ____ Well<br>____ Acceptable<br>____ Unacceptable<br>____ Not Applicable | Support: |
| | | |
| 18. Were all exceptions or weaknesses in the audit WPs noted in the final audit report? | ____ Yes<br>____ No<br>____ Not Applicable | Why not: |
| | | |

| | | |
|---|---|---|
| 19. Were the internal auditors, including outsourced vendors, adequately trained and experienced to complete this program? | ____ Yes<br>____ No | How determined: |
| | | |
| 20. How well does the auditor-in-charge (AIC) support the final audit rating? | ____ Well<br>____ Acceptable<br>____ Unacceptable<br>____ Not Applicable | Support |
| | | |
| 21. Do you agree with the final rating? | ____ Yes<br>____ No<br>____ Not Applicable | Why not: |
| | | |
| **Sampling** | | |
| 22. Did the auditor use statistical sampling? | ____ Yes<br>____ No<br>____ Not Applicable | |
| a. Was the population accurately defined and justified by the auditor? | ____ Yes<br>____ No | Why not: |
| b. Was the selection of the sampling method disclosed? | ____ Yes<br>____ No | Why not: |
| c. Were the sample selection techniques disclosed? | ____ Yes<br>____ No | Why not: |
| d. Were sample evaluation and reporting results criteria established? | ____ Yes<br>____ No | Why not: |
| | | |
| ***Audit Reports*** | | |
| 23. Does the audit report articulate the appropriate conclusions, findings, and recommendations? | ____ Yes<br>____ No | Why not: |
| | | |
| 24. Does the audit report address the root cause of problems and recommend actions to correct problems? | ____ Yes<br>____ No<br>____ Not Applicable | |

| | | |
|---|---|---|
| | | |
| 25. What level of management was notified of the audit findings? | | |
| a. Is this the appropriate level or person? | ____ Yes<br>____ No | If not, who: |
| | | |
| 26. Does the AIC or supervisor make effective use of MIS and have periodic contact with area/unit management? | ____ Yes<br>____ No | Why not: |
| | | |
| ***Audit Follow-up*** | | |
| 27. Was there evidence that prior audit issues were properly followed up during the current audit? | ____ Yes<br>____ No<br>____ Not Applicable | |
| | | |
| 28. Was management's response to audit findings timely? | ____ Yes<br>____ No | |
| | | |
| 29. Was management's response to audit findings acceptable? | ____ Yes<br>____ No | Why not: |
| | | |
| 30. Are corrective action time frames included in management's response? | ____ Yes<br>____ No<br>____ Not Applicable | |
| | | |
| 31. How effective and timely are management's plans for addressing deficiencies? | ____ Adequate<br>____ Inadequate<br>____ Not Applicable | Why inadequate: |
| | | |
| 32. Are audit exceptions in this area sufficiently detailed on an exception tracking report? | ____ Yes<br>____ No<br>____ Not Applicable | Why not: |
| | | |
| 33. Is there sufficient follow-up activity for high-risk areas/units or areas/units adversely rated? | ____ Yes<br>____ No<br>____ Not Applicable | Why not: |

| | | |
|---|---|---|
| | | |
| ***Quality Assurance*** | | |
| 34. Was the audit subject to a Quality Control Review? | ____ Yes<br>____ No<br>____ Not Applicable | Why not: |
| | | |
| ***Meetings with Auditors*** | | |
| 35. Summarize any discussions with internal auditors or outsourced internal auditor vendors (summary should include but not be limited to: participants, date, subject, conclusions or recommendations, and the participants' receptiveness and responses). | | |
| | | |
| ***Overall Conclusion*** | | |
| 36. Did the auditor or audit team involved in the review of this area have the necessary skills, experience, and knowledge required for the review? | _____ Yes<br>_____ No | |
| | | |
| 37. Was the auditor independent of the area under review? | _____ Yes<br>_____ No | |
| | | |
| 38. Should the OCC adjust its strategy for this bank/business unit based upon your review of the audit reports, memos, and WPs? | ____ Yes<br>____ No | Why or why not and what adjustments should be made? |
| | | |

| | | |
|---|---|---|
| 39. Provide any other information deemed appropriate. | | |
| | | |

# Appendix F: Audit Function Questionnaire

This audit function questionnaire (AFQ) is designed as a tool to help examiners evaluate a bank's internal or external audit functions. Its use is not mandatory. Examiners should complete the AFQ only if they determine that the auditors are both competent and independent. Based on the auditors' work and the answers to the specific audit function questions, the examiner can then determine which verification procedures he or she considers necessary to perform.

The following audit function questions are reflective of a simplistic banking environment. Differing banking environments and roles of bank personnel in assessing overall controls and other variables affect the kinds of audit procedures that may be appropriate for a bank. Examiners should refer to individual booklets of the *Comptroller's Handbook* for more detailed audit requirements and worksheets for compliance, complex, or specialty areas or activities. In many cases, for external audits, all of the audit function questions may not be applicable to the type and extent of the audit/review conducted. Review reports, programs and audit work papers to answer the audit function questions. Where appropriate, supporting documentation and pertinent information should be retained or noted under comments.

For the following areas, has the internal auditor (or external auditor if deemed appropriate) within a reasonable audit cycle:

**Cash Accounts**

1. Counted cash on hand (including confirmation of incoming or outgoing cash shipments)?

2. Determined the propriety of amount and classification for cash items?

3. Confirmed clearings and reviewed all incoming returned items for some period after the date clearings were confirmed?

4. Checked adherence to procedures for maintaining records in accordance with 31 CFR 103.21, 103.22, 103.23, 103.25, 103.27, 103.29, 103.32, 103.33, 103.34, 103.35, 103.36, and 103.37?

5. Checked adherence to the provisions of 31 CFR 103, performing the following for:

   a. Reporting Requirements: Determined coverage requirements that include a review of a teller's work and of forms 4789 and 4790?

   b. Record keeping Activities: Tested the bank's adherence to the in-house record retention schedule? This schedule should meet the requirements of the regulation.

   c. Exemptions: Ascertained that the bank maintains a list of exempt customers?

      – Tested the reasonableness of the exemptions granted?
      – Ascertained that the bank completes and maintains the exemption certification?

   d. Foreign Accounts: Ascertained that the bank has filed Form 90-22.1, declaring interest in a foreign financial account?

   e. Volume of Cash Movements: Reviewed cash control records and traced any apparently large or unusual cash movements to or from a department or branch?

6. Checked adherence to 12 CFR 21.21 in establishing a written Bank Secrecy Act compliance program approved by the board of directors?

**Due From Banks**

1. Tested bank reconcilement including the Federal Reserve bank?

2. Received cut-off bank statements as of the examination date and an appropriate date subsequent to the examination date for use in testing bank reconcilement?

3. Reviewed all returned items for an appropriate period subsequent to the examination date?

4. Confirmed due from banks--time accounts with the banks holding the deposits?

5. Determined accuracy and completeness of reports FR 2900 and FR 2950 submitted to the Federal Reserve for calculation of required reserve balances?

**Investments**

1. Tested the appropriateness of classification of held-to-maturity, available-for-sale, and trading securities and confirmed securities balances (including physical count of securities located at the bank, and confirmation of bank ownership and control of securities held in custody outside the bank or in transit)?

2. Determined the book and market value of investment securities?

3. Determined the gain and loss of investment securities sold during the period?

4. Reviewed the accrued interest accounts and tested computation of interest income, including amortization of any premium discount?

5. Checked for compliance with the FFIEC "Supervisory Policy Statement on Investment Securities and End-User Derivatives" (OCC 98-20)?

6. Checked for compliance with the repurchase agreement provision of the Government Securities Act for non-dealer banks (15 USC 78o-5)?

7. Checked for compliance with laws and regulations applicable to those banks engaging in the purchase or sale of securities instruments for their own account or for the account of customers (including furnishing commodity advice to customers)?

**Retail Non-Deposit Investment Sales**

1. Checked monitoring and resolution of customer complaints?

2. Tested customer accounts for proper disclosures, advertising, and suitability determination?

3. Checked for conflicts of interest?

4. Reviewed the bank's compensation program for retail non-deposit investment product sales?

5. If the bank has a separate compliance program for retail non-deposit investment product sales, did audit review the adequacy of the compliance program?

6. Where the bank offers retail non-deposit investment products through an independent third party vendor, did audit review vendor adherence to the governing agreement?

7. Ascertained that sales activities were in keeping with established policies and procedures, applicable laws and regulations, and the February 15, 1994 interagency statement?

**Bank Derivatives**

(The level of internal auditor expertise should be consistent with the level of activity and degree of risk assumed by the bank. In some cases, banks may need to outsource audit coverage of derivative activities to ensure that the persons performing the audit work possess sufficient depth and experience.)

1. Assessed the adequacy and reasonableness of information obtained and used in risk management systems (market, credit, liquidity, and operations/systems)?

2. Validated the data integrity of significant market, liquidity, and risk management models?

3. Determined that contract documentation is properly maintained and safeguarded, and ascertained that legal counsel has properly reviewed documents?

4. Confirmed the effectiveness of internal control systems used for derivatives transaction processing and valuation?

5. Checked compliance with laws, rules, regulations, and proper accounting?

6. Ascertained that derivative activities are performed within the guidelines provided by bank policies and procedures?

7. Participated in the new product review process, approving the audit procedures developed for testing any new products or activities?

**Mortgage Banking Activities**

1. Tested book and fair-market values of mortgage servicing rights (MSR) and servicing fees received (SFR) assigned to pools of loans?

2. Verified accuracy of hedge accounting?

3. Tested the accuracy of tracking systems by verifying that documentation was on hand, or in process of being received, for loans awaiting sales and those being serviced?

   – Followed up on any exceptions outstanding for 120 days or more?

4. Tested servicing rights impairment analyses?

5. Determined the accuracy of financial reporting systems and other management information systems?

6. Checked compliance with established policies and procedures, accounting recognition, and laws, rules and regulations?

**Bank Dealer Activities**

1. Confirmed securities balances (verification included physical count of securities located at the bank, confirmation of securities held outside the bank or in transit, or testing of internal confirmation and reconciliation process)?

2. Determined the book and market value of trading account securities or tested the internal month-end valuation process?

3. Determined the gain and loss on underwriting and trading account transactions?

4. Reviewed the accrued interest accounts and checked computation of interest income?

5. Confirmed “fails” and “due bills"?

6. Confirmed good faith deposits and cash collateral?

7. Reviewed and tested the bank’s municipal securities dealer department, government securities dealer department, or the bank’s discount broker activity for compliance with applicable laws and regulations (12 USC 24, 15 USC 78o-4, 15 USC 78o-5, and 12 CFR 10 and 12)?

8. Determined that the compliance review is conducted pursuant to comprehensive written audit policies and procedures?

9. Determined that violations or suspected violations of laws, rules, and regulations are referred to the legal counsel for review and that the results of that review are made a part of the audit report to the board or its committee?

**Loans**

Commercial

1. Confirmed loan balances?

2. Reviewed, or confirmed with outside custodian, notes and other legal documentation including collateral?

3. Tested the pricing of negotiable collateral?

4. Determined that any necessary insurance coverage is adequate and the bank is named as loss payee?

5. Reviewed the accrued interest accounts and tested computation of interest income?

Accounts Receivable Financing

1. Confirmed loan balances?

2. Reviewed, or confirmed with outside custodian, notes and other legal documentation including collateral?

3. Reviewed the accrued interest accounts and checked computation of interest income?

Direct Lease Financing

1. Confirmed leases and related balance sheet accounts?

2. Reviewed leases and other legal documentation?

3. Tested computation of depreciation expense?

4. Tested computation of interest or rent income?

5. Tested computation of gain or loss on property sales and disposals and traced sales proceeds to cash receipts records?

6. Determined that any deferred tax liability or asset is accurately reflected?

7. Reviewed insurance coverage and determined that property damage coverage is adequate in relation to book value and that liability insurance is in effect?

Installment

1. Confirmed loan balances?

2. Reviewed, or confirmed with outside custodian, notes and other legal documentation including collateral?

3. Determined that any necessary insurance coverage is adequate and the bank is named as loss payee?

4. Reviewed unearned discount and any accrued interest balances and tested the computation of interest income?

5. Reviewed sales of repossessed collateral and determined the propriety of the entries made to record the sales?

6. Tested rebate amounts for loans which have been prepaid?

Floor Plan

1. Confirmed loan balances?

2. Reviewed, or confirmed with outside custodian, notes and other legal documentation?

3. Physically inspected collateral?

4. Determined that any necessary insurance coverage is adequate and the bank is named as loss payee?

5. Reviewed the accrued interest accounts and tested computation of interest income?

Credit Card

1. Confirmed loan balances?

2. Tested the computation of interest income?

Home Equity

1. Confirmed loan balances?

2. Reviewed, or confirmed with outside custodian, notes and other legal documentation?

3. Tested computation of interest income?

Check Credit

1. Confirmed loan balances?

2. Examined, or confirmed with outside custodian, notes and other legal documentation?

3. Tested computation of interest (and service fee, if applicable) income?

Real Estate and Real Estate Construction

1. Confirmed loan and escrow account balances?

2. Examined, or confirmed with outside custodian, notes and other legal documentation including collateral?

3. Determined that any necessary insurance coverage is adequate and the bank is named as loss payee?

4. Reviewed the accrued interest accounts and tested computation of interest income?

5. Tested contingency or escrow account balances?

Oil and Gas

1. Confirmed loan balances?

2. Examined, or confirmed with outside custodian, notes and other legal documentation including collateral?

3. Reviewed division transfer orders or pipeline companies that have been instructed to remit directly to the bank?

4. Determined that any necessary insurance coverage is adequate and the bank is named as loss payee?

5. Reviewed the accrued interest accounts and tested computation of interest income?

**Allowance For Loan and Lease Losses**

1. Confirmed loan balances for loans charged off since their last examination and amounts of debit entries to the reserve account?

2. Examined supporting documentation for loans charged off?

3. Reviewed loan recoveries and agreed amounts to credit entries in the reserve account?

4. Tested the recording of deferred tax credits (charges) if the deduction for loan losses on the bank's tax return was different from that charged to operations?

**Bank Premises and Equipment**

1. Examined support for additions, sales and disposals?

2. Reviewed property transactions with "bank-affiliated personnel"?

3. Verified property balances?

4. Tested computation of depreciation expense?

5. Tested computation of gain or loss on property sales and disposals and traced sales proceeds to cash receipts records?

6. Determined that any deferred tax liability or asset, evolving from the use of different depreciation methods for book and tax purposes, is properly reflected on the bank's books?

**Other Assets**

1. Confirmed other asset balances?

2. Examined support for additions and disposals?

3. Tested the computation of any gains or losses on disposals?

4. Tested the bank's computation of any amortization?

5. Reviewed inter-office transactions?

6. Reviewed suspense accounts to determine whether all items included were temporary?

**Deposits**

Demand and Other Transaction Accounts

1. Confirmed account balances?

2. Tested closed accounts and determined that they were properly closed?

3. Tested account activity in dormant accounts, bank controlled accounts (such as dealers' reserves), employee/officer accounts, and accounts of employees'/officers' business interests?

4. Reviewed overdraft accounts and determined collection potential?

5. Tested computation of service charges and traced postings to appropriate income accounts?

Time Deposit Accounts

1. Confirmed time deposit account balances?

2. Tested closed accounts and determined that they were properly closed?

3. Tested account activity in dormant accounts, bank controlled accounts, employee/officer accounts, and accounts of employees'/officers' business interests?

4. Reviewed the accrued interest accounts and tested computations of interest expense?

5. Accounted for numerical sequence of pre-numbered certificates of deposit?

Official Checks

1. Reconciled account balances and tested control over blank check stocks?

2. Determined the validity and completeness of outstanding checks?

3. Examined documentation supporting paid checks?

4. Tested certified checks to customer's collected funds balances?

**Borrowed Funds**

1. Confirmed borrowed funds balances?

2. Examined supporting legal documents, disclosures, and collateral custody agreements and determined compliance with applicable laws and regulations?

3. Reviewed minutes of the stockholders' and board of directors' meetings for approval of all borrowing requiring such approval?

4. Verified changes in capital notes outstanding?

5. Reviewed the accrued interest accounts and tested computation of interest expense?

**Other Liabilities**

1. Confirmed balances of "other liability" accounts (including tests for unrecorded liabilities as of a given date)?

2. Reviewed the operation and use of any "inter-office" account?

3. Reviewed suspense accounts to determine all items cleared on a timely basis?

## Capital Accounts and Dividends

Capital Stock

1. If a bank acts as its own transfer agent or registrar, accounted for all stock certificates, (issued and unissued) and reconciled par value of outstanding shares to appropriate general ledger control accounts?

2. If bank has an outside transfer agent or registrar, confirmed shares issued and activity since previous examination?

3. Reviewed capital changes since previous examination?

Dividends

1. Tested the computation of dividends paid or accrued?

2. Reviewed minutes of the board of directors' meetings to determine propriety of dividend payments and accruals?

## Consigned Items and Other Non-Ledger Control Accounts

Safe Deposit Boxes

1. Tested rental income?

2. Checked vault entry records for signature(s) of authorized persons?

3. Tested reconcilements of control records?

Safekeeping/Custodial Accounts

1. Examined or confirmed with outside custodian safekeeping/custodial items?

2. Tested completeness of safekeeping/custodial items and records by examining supporting documentation or by confirming with customers?

3. Tested closed safekeeping/custodial accounts?

4. Tested safekeeping/custodial fee income?

Collection Items

1. Tested collection items by examining supporting documentation, subsequent receipt of payments, disbursement to customers of funds collected, or by confirming with customers?

2. Tested collection fee income?

Consigned Items

1. Reconciled physical count of unissued and voided items on hand to memorandum controls?

2. Confirmed with consignor the inventory on hand at the bank?

3. Tested income from sale of consigned items?

**Income and Expenses**

1. Tested income and expenses by examining supporting documentation for authenticity and proper approval?

2. Tested accruals by either recomputing amounts or examining documents supporting such accruals?

**Related Organizations**

1. Reviewed and tested the investment in and the transactions with related organizations?

2. Determined that investments, advances, or transactions with affiliates are consistent with covenants of debt or other instruments as approved by the board of directors or bank management?

**Information System Services**

1. Performed periodic audit procedures for significant IT control functions, including information security, business continuity, project management, and systems development.

2. Performed periodic audit procedures for significant automated applications to determine that workflow is processed accurately and in conformity with operating manuals?

3. Tested adherence authentication and access control requirements within various applications?

4. Verified the adequacy of system logging/audit trails and management monitoring?

5. Controlled or periodically reviewed dormant accounts?

6. Reviewed unposted items?

**Payment Systems Risk**

1. Tested the bank's self-assessment?

2. Reviewed the reasonableness of any de minimis cap?

3. Ascertained compliance with established bank policy?

**Funds Transfer Activities**

1. Reviewed the wire transfer function for segregation of duties involving receipt, processing, settlement, accounting, call-back, and reconciling?

2. Tested staff compliance with credit and personnel procedures, operating instructions, and internal controls?

3. Reviewed intraday and overnight overdrafts resulting from fails or intentional extensions of credit?

**Asset Management**

1. Tested fee income and client reimbursement?

2. Examined asset management client contracts?

3. Checked for compliance with applicable laws, regulations and rulings?

4. Ascertained adherence with established bank policies and procedures?

**Private Placements**

1. Tested transactions for evaluation of both issuer and investor, including suitability of the investment?

2. Checked for possible conflicts of interest?

3. Tested the reasonableness of fees charged for loans or paid on deposits?

4. Ascertained that activities are in keeping with established bank policy and SEC rules and regulations?

**Discount Brokerage Activities**

1. Tested transactions for compliance with 12 CFR 12?

2. Reviewed advertising and customer disclosures for accuracy?

3. Tested customer account statements for accuracy?

4. Tested activities for timeliness of processing/transmitting, reliability of accounting records, and for abuses or irregularities?

5. Ascertained compliance with established bank policies and procedures?

**Safeguarding Customer Information**

1. Determined that the bank has a written information security program, approved by the board or directors or appropriate board committee, that meets the requirements of 12 CFR 30, Appendix B?

2. Tested the program to ascertain that it ensures the security and confidentiality of customer information, protects against anticipated threats or hazards to the security or integrity of such information, and protects against unauthorized access to or use of such information that could result in substantial harm or inconvenience to customers?

3. Reviewed the board's or management's risk assessments of: internal and external threats; the likelihood and potential damage from those threats; and the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks?

4. Review documentation related to selection of service providers; written contracts with service providers; and audits, summaries of test results, or other equivalent evaluations of the bank's service providers?

**Insurance Activities**

1. Check for compliance with applicable laws and regulations and internal policies, procedures, and guidance?

2. Review customer complaints and their resolution?

3. Verify that third-party sales are conducted consistent with governing agreements?

**Branches**

1. Has the internal or external auditor performed appropriate audit procedures in the branches during a reasonable audit cycle that are at least as comprehensive as those listed in the applicable areas above?

# Appendix G: Auditor Independence Worksheet

The following worksheet is designed to help examiners determine whether a bank's external auditor (i.e., CPA) meets AICPA or SEC independence requirements. Examiners may want to share the worksheet with the bank and its external auditor to facilitate discussion of independence. The worksheet reflects the most common independence requirements when a CPA performs a bank's external audit (financial statement audits, control attestations, or other audit services requiring independence). This worksheet is not applicable when CPAs perform outsourced internal audit activities for a bank but do not perform external audit or attestation services for the bank. Use of this worksheet is not mandatory and can be used at the discretion of the EIC. Any independence concerns should be discussed first with the bank and the external auditor. If concerns remain, then discuss with district accountants or the Chief Accountant's office prior to making any recommendations to the bank.

**Note:** Shaded answer blocks indicate situations that do or may impair the external auditor's independence. Examiners should discuss these situations with the bank's board of directors or its audit committee and the external auditor to reach agreement on appropriate corrective action. Examiners should explain any mitigating circumstances, particularly for small community banks, in the Comments column.

| | Yes | No | Comments |
|---|---|---|---|
| **CPA PERFORMS EXTERNAL AUDIT** | | | |
| **AICPA Requirements** [1] | | | |
| During the period of engagement, did the CPA: | | | Explain any Yes answers. |
| a. Have or commit to acquire any direct or material indirect financial interest in the bank? | | | |

[1] The full text of AICPA independence requirements can be found on the AICPA's web site at http://www.aicpa.org/about/code/et101.htm.

| | Yes | No | Comments |
|---|---|---|---|
| b. Act as trustee of any trust or executor or administrator of any estate that has or committed to acquire any direct or material indirect financial interest in the bank? | | | |
| c. Have a joint closely held investment material to the CPA? | | | |
| | | | |
| During the period of engagement, did the CPA have any loan to or from the bank, any officer or director of the bank, or any individual owning 10% or more of the bank's equity securities other than the following: | | | If Yes, explain. |
| a. Grandfathered loans? | | | |
| - Existing as of January 1, 1992 | | | |
| - Obtained prior to engagement by the bank | | | |
| - Obtained from a bank for which independence was not required and subsequently sold to the bank | | | |
| - Obtained from the bank prior to becoming a member of the firm | | | |
| b. Automobile loans and leases? | | | |
| c. Loans fully collateralized by CSV of insurance policy? | | | |
| d. Loans fully collateralized by cash deposits at the bank? | | | |
| e. Aggregate credit card/cash advance debt of $5,000 or less? | | | |
| | | | |

| | Yes | No | Comments |
|---|---|---|---|
| During the period of engagement, did any partner or professional employee of the accounting firm, his or her immediate family, or any group of such persons acting together own more than 5% of the bank's equity securities? | | | If Yes, explain. |
| | | | |
| During the period of engagement or period covered by the financial statements, was any partner or professional employee of the accounting firm associated with the bank as: | | | Explain any Yes answers. |
| a. Director, officer, employee, or any capacity equivalent to that of a member of bank management? | | | |
| b. Promoter, underwriter, or voting trustee? | | | |
| c. Trustee for any pension or profit-sharing trust of the bank? | | | |
| | | | |
| Does the CPA perform other services for the bank that entail: Examples: bookkeeping, payroll, benefit plan administration, investment advice/management, corporate finance consulting/advice, appraisal, valuation, actuarial, executive or employee search, business risk consulting, and information system design, installation or integration. | | | Explain any Yes answers. |
| a. Authorizing, executing or consummating a transaction, or otherwise exercising authority on behalf of a client or having the authority to do so? | | | |

| | Yes | No | Comments |
|---|---|---|---|
| b. Preparing source documents or originating data, in electronic or other form, evidencing the occurrence of a transaction (for example, purchase orders, payroll time records, and customer orders)? | | | |
| c. Having custody of client assets? | | | |
| d. Supervising client employees in the performance of their normal recurring activities? | | | |
| e. Determining which recommendations of the member should be implemented | | | |
| f. Reporting to the board of directors on behalf of management? | | | |
| g. Serving as a client's stock transfer or escrow agent, registrar, general counsel or its equivalent? | | | |
| | | | |
| During the period of engagement, did the CPA's firm have any material cooperative arrangements with the bank such as: | | | |
| a. Prime/subcontractor arrangements to provide services or products to a third party? | | | |
| b. Joint ventures to develop or market products or services? | | | |
| c. Arrangements to combine one or more firm services or products with one or more bank services or products and market the package with references to both parties? | | | |

| | Yes | No | Comments |
|---|---|---|---|
| d. Arrangements under which the firm acts as distributor or marketer of the bank's products or services, or the bank acts as distributor or marketer of the firm's products or services? | | | |
| | | | |
| ***Does the CPA also perform any or all internal audit services for the bank?*** | | | If Yes, answer the following questions. |
| | | | |
| Does the bank assume responsibility for: | | | |
| a. Establishing and maintaining internal control? | | | If not, who does? |
| b. Directing and supervising the internal audit function? | | | If not, who does? |
| c. Establishing guidelines for management and CPA to follow in carrying out their responsibilities? | | | If no, why not? |
| d. Monitoring how well the respective responsibilities of the bank and CPA are met? | | | If no, why not? |
| e. Making the decision on whether to implement the CPA's recommendations? | | | If no, why not? |
| | | | |
| Does bank management rely on the CPA's work as the primary basis for its control assertion? | | | If yes, why? |
| | | | |
| Does the bank monitor internal control processes to assess the quality of control performance over time through: | | | At least one of the below should be Yes. |
| a. Ongoing activities? | | | |
| b. Separate evaluations?[2] | | | |

[2] CPA can perform separate evaluations of bank's control effectiveness, including separate evaluation of bank's ongoing monitoring activities, as part of the external audit.

| | Yes | No | Comments |
|---|---|---|---|
| c. Or a combination of both | | | |
| | | | |
| Does the bank, for internal audit: | | | Explain any No answers. |
| a. Designate a competent individual or individuals, preferably within senior management, to be responsible for the internal audit function? | | | |
| b. Determine the scope, risk, and frequency of internal audit activities, including those performed by the CPA providing outsourced internal audit activities? | | | |
| c. Evaluate the findings and results arising from internal audit activities, including those performed by the CPA providing outsourced internal audit activities? | | | |
| d. Evaluate the adequacy of audit procedures performed and findings resulting from performance of those procedures by, among other things, obtaining reports from the CPA providing outsourced/co-sourced internal audit activities? | | | |
| | | | |
| Does the CPA: | | | |
| a. Inform, using an engagement letter, the bank's board of directors or its audit committee of the respective roles of the bank and the CPA with respect to the outsourced internal audit engagement? | | | If no, why not? |

| | Yes | No | Comments |
|---|---|---|---|
| b. Perform outsourced/co-sourced internal audit procedures in accordance with terms of the engagement, as stipulated in the engagement letter, and report thereon to the bank?[3] | | | If no, why not? |
| c. Direct, review, and supervise day-to-day performance of outsourced/co-sourced internal audit procedures? | | | If not, who does? |
| d. Undertake responsibilities required to be performed by the bank individual responsible for the internal audit function? | | | If Yes, explain. |
| | | | |
| Does the CPA perform any of the following: | | | Explain any Yes answers. |
| a. Ongoing monitoring or control activities that affect transaction execution, ensure that transactions are properly executed, accounted for, or both, and routine activities in connection with bank's operating or production processes equivalent to those of ongoing compliance or quality control functions? | | | |
| b. Determining which, if any, recommendations for improving the internal control system should be implemented? | | | |

[3] CPA independence is not impaired if the CPA performs procedures generally considered extensions of its financial statement audit scope, i.e., confirmations or analysis of fluctuations in account balances.

| | | | |
|---|---|---|---|
| c. Reporting to bank's board of directors or audit committee on behalf of bank management or the individual responsible for the internal audit program? | | | |
| d. Authorizing, executing, or consummating transactions or otherwise exercising authority on behalf of bank? | | | |
| e. Preparing source documents? | | | |
| f. Having custody of assets? | | | |
| g. Approving or being responsible for the overall internal audit work plan, including determination of internal audit risk and scope, project priorities, and frequency of performance of audit procedures? | | | |
| h. Being connected with bank in any capacity equivalent to a member of bank management or as a bank employee (e.g., listed as employee in bank directories or other bank publications, allowing self to be referred to by title or description as supervising or being in charge of bank's internal audit function, or using bank's letterhead or internal correspondence forms in communications)? | | | |
| | | | |
| | | | |
| **SEC Requirements** [4] | | | |
| Are the bank's securities registered with the OCC, or is the bank subject to 12 CFR 363? | | | If Yes, determine the following. |

[4] Applicable for any independent public accountant (IPA) performing external audit work at national banks subject to 12 CFR 363 and national banks whose securities are registered with the OCC, i.e., those subject to the periodic filing and reporting requirements of 12 CFR 11 and 12 CFR 16.20. The full text of the SEC's independence rule can be found at http://www.sec.gov/rules/final/33-8183.htm.

| | | | |
|---|---|---|---|
| During the audit and engagement period, did the accountant, firm, covered persons of the firm, or immediate family members have any financial interests in the bank such as: | | | |
| a. Investments in the bank? | | | |
| - Direct investment in stocks, bonds, notes, options, or other securities | | | |
| - More than 5% ownership in the bank's equity securities or control of the bank | | | |
| - Voting trustee of a trust or executor of an estate having bank securities | | | |
| - Material indirect investment in the bank | | | |
| - Direct or material indirect investment in an entity where | | | |
| > The bank has an investment in an entity material to the bank and significant influence over the entity | | | |
| > The entity has an investment in the bank material to the entity and significant influence over the bank | | | |
| - Any material investment in an entity over which the bank has significant influence | | | |
| - Ability to significantly influence an entity that can significantly influence the bank | | | |
| b. Other financial interests such as | | | |
| - Loans to or from the bank, its directors or officers, or anyone owning more than 10% of the bank's securities, except for: | | | |

| | | | |
|---|---|---|---|
| > Automobile loans/leases | | | |
| > Loans fully collateralized by CSV of insurance policy | | | |
| > Loans fully collateralized by cash deposits at the bank | | | |
| > Mortgage loan collateralized by borrower's primary residence and not obtained while a covered person | | | |
| - Savings or checking accounts at the bank exceeding FDIC insured coverage? | | | |
| - Broker-dealer accounts maintained at the bank? | | | |
| - Future commission merchant account maintained at the bank? | | | |
| - Credit card balances aggregating $10,000 or less? | | | |
| - Insurance products issued by the bank? | | | |
| - Financial interest in an entity that is part of an investment company that includes the bank? | | | |
| c. Bank financial relationships? | | | |
| - Investments by the bank in the firm's stocks, bonds, notes, options, or other securities | | | |
| - Bank officers or directors own more than 5% of the firm's equity securities | | | |
| - Bank acts as underwriter, broker-dealer, market-maker, promoter, or analyst for securities issued by the firm | | | |
| | | | |
| During the audit and engagement period, did the accountant have employment relationships with the bank such as | | | |

| | | | |
|---|---|---|---|
| a. Current partner, principal, shareholder or professional employee of the firm is employed by the bank or serves as a member of the bank's board of directors? | | | |
| b. Close family member of firm's covered persons is in an accounting or financial reporting oversight role at bank, or was in such a role during the period of engagement? | | | |
| c. Former partner, principal, shareholder or professional employee of the firm is in an accounting or financial reporting oversight role at bank, or is in such a role and was a member of the audit engagement team during the prior year's audit of the bank? | | | |
| d. Former officer, director, or employee of bank is employed by the firm and participated in the audit of the bank's financial statements covering any period for which the employee worked for the bank? | | | |
| | | | |
| During the audit and engagement period, did the firm or any covered person in the firm have any direct or material indirect business relationship with the bank or its officers, directors, or substantial shareholders? | | | |
| | | | |
| During the audit and engagement period, did the accountant provide any of the following non-audit services to the bank: | | | |

| | | | |
|---|---|---|---|
| a. Bookkeeping or other services related to the accounting records or financial statements of the bank? | | | |
| b. Financial information system design and implementation? | | | |
| c. Appraisal or valuation services, fairness opinions, or contribution-in-kind reports? | | | |
| d. Actuarial services? | | | |
| e. Internal audit outsourcing services?[5] | | | |
| f. Management functions, either temporary or permanent? | | | |
| g. Human resources? | | | |
| h. Broker-dealer, investment advisor, or investment banking services? | | | |
| i. Legal services? | | | |
| j. Expert services unrelated to the audit? | | | |
| | | | |
| During the audit and period of engagement, did the accountant provide any service or product to the bank for a contingent fee or commission, or receive a contingent fee or commission from the bank? | | | |
| | | | |
| Has the audit engagement team lead and concurring partners performed audit, review or attest services for the bank or any of its significant subsidiaries for more than five consecutive years? | | | |
| | | | |

[5] "Internal audit services" means only that work related to internal accounting controls, financial systems, financial statements, and matters that impact financial statements. Work on other operational internal audit services not related to the above is not included. The key criteria is whether it is reasonable to conclude that the results of these services will not be subject to audit procedures during an audit of the audit client's financial statements.

| | | | |
|---|---|---|---|
| Did the bank's audit committee pre-approve all audit, review and attest engagements performed by the auditor? | | | |
| | | | |
| Did the bank's audit committee pre-approve non-prohibited non-audit services performed by the auditor? | | | |
| | | | |
| Did any partner, principal or shareholder participating on the audit engagement team earn or receive compensation based on the performance of, or procuring of, engagement with the bank to provide any products or services other than audit, review or attest services? | | | |
| | | | |
| Did the audit firm, prior to filing the audit report with the OCC/SEC, report: | | | |
| a. All critical accounting policies and practices to be used? | | | |
| b. All alternative treatments of financial information within GAAP that have been discussed with bank management, including: | | | |
| - Ramifications of the use of alternative disclosures and treatments, and | | | |
| - The treatment preferred by the audit firm? | | | |
| c. Other material written communications between the audit firm and bank management, such as any management letter or schedule of unadjusted differences? | | | |
| | | | |

| **SUMMARY** | | | |
|---|---|---|---|
| Based on responses to the above questions, does the CPA act or appear to act in a capacity equivalent to that of the bank's management? | | | If Yes, explain. |
| | | | |
| Are there any other factors that indicate the CPA does not comply with provisions of the independence standards? | | | If Yes, explain. |
| | | | |

## Appendix H: Board/Audit Committee Oversight Worksheet

The following worksheet is designed to help examiners assess the quality and extent of a bank's audit committee (or board, if there is no audit committee) duties and responsibilities and the qualifications of committee members. Examiners may want to use the worksheet, or share it with the bank's board or audit committee, to facilitate as a tool to facilitate general discussions with banks about audit committee (or board, if there is no audit committee) responsibilities. The worksheet can be used for national banks subject to 12 CFR 363 or those with securities registered with the OCC (i.e., subject to the periodic filing and reporting requirements of 12 CFR 11 and 12 CFR 16.20). It can also be used for banks that are not subject to the statutory requirements (i.e., most community banks). However, in doing the latter, examiners need to be cognizant of the bank's size, operations, and risk profile, and temper such discussions accordingly. Use of this worksheet is not mandatory and it can be used at the discretion of the EIC.

**Note:** A response in a shaded answer block generally indicates an area examiners should discuss with the bank's board of directors or its audit committee and, as appropriate, reach agreement on corrective measures. Examiners should explain any mitigating circumstances, particularly for smaller community banks, in the Comments column.

| | Yes | No | N/A | Comments |
|---|---|---|---|---|
| **General Responsibilities** | | | | |
| Does the board of directors or its audit committee: | | | | |
| a. Review and approve audit strategies, policies, programs (including BSA compliance programs), and organizational structure? | | | | |
| b. Review and approve selection or termination of external auditors and outsourced internal audit vendors? | | | | |

| | Yes | No | N/A | Comments |
|---|---|---|---|---|
| c. Meet regularly with internal and external auditors and outsourced internal audit vendors? | | | | |
| d. Ensure that internal and external auditors and outsourced internal audit vendors are independent and objective? | | | | |
| e. Ensure that comprehensive audit coverage is in place to meet risks and demands posed by current and planned activities? | | | | |
| f. Have significant input into hiring senior internal audit personnel, setting their compensation, and evaluating their performance? | | | | |
| g. Review and approve annual audit plans and schedules, and any changes thereto, for both internal and external audits? | | | | |
| h. Retain internal and external auditors and outsourced vendors qualified to audit the activities in which the bank is engaged? | | | | |
| i. Monitor and track significant control weaknesses and management's progress toward corrective action? | | | | |
| j. Meet with examiners at least once each supervisory cycle to discuss audit review findings? | | | | |

| | Yes | No | N/A | Comments |
|---|---|---|---|---|
| | | | | |
| Is the committee responsible for risk management issues? [1] If so, does it: | | | | |
| a. Communicate risk management concerns to the full board? | | | | |
| b. Ensure that risk management evaluation functions are independent? | | | | |
| c. Review risk management reports and information? | | | | |
| | | | | |
| **Audit Committee** | | | | |
| Does the bank have an audit committee? (Required for 12 CFR 363 or OCC-registered banks)[2] | | | | |
| | | | | |
| Does the committee maintain minutes and other relevant records of their meetings and decisions? (Required for banks subject to 12 CFR 363) | | | | |
| | | | | |
| Has the committee adopted and the board approved a written charter for the audit committee? (Required for OCC-registered banks) | | | | |
| | | | | |
| If so, does the charter address: | | | | |

[1] The bank's board of directors may assign these to another committee or individual designated as responsible for overseeing the bank's overall risk management functions.

[2] National banks whose securities are registered with the OCC and file periodic reports under 12 CFR 11 and 12 CFR 16.20, and national banks subject to 12 CFR 363.

| | Yes | No | N/A | Comments |
|---|---|---|---|---|
| a. The committee's responsibilities and how they carry out those responsibilities (including structure, processes, and membership requirements)? | | | | |
| b. The committee's review and discussion with IPAs of any relationships or services that may affect the IPA's independence or objectivity? (SEC's revised independence rule require OCC-registered bank audit committees to pre-approve all audit, review, attest, and non-prohibited non-audit services.) | | | | |
| c. The IPA's accountability to the board and committee, and the board/committee's authority and responsibility to select, evaluate, and (where appropriate) replace the IPA? | | | | |
| | | | | |
| Are committee members independent of management? (Required for 12 CFR 363 and OCC-registered banks) | | | | |
| | | | | |
| Is the committee<br>a. Made up entirely of outside directors (required for 12 CFR 363 and OCC-registered banks) ? | | | | |
| b. Or a majority of outside directors? | | | | |
| | | | | |

| | Yes | No | N/A | Comments |
|---|---|---|---|---|
| Does the board of directors annually make a determination of committee member independence? (Required for 12 CFR 363 and OCC-registered banks) | | | | |
| | | | | |
| If so, does the board's determination consider whether members: | | | | |
| a. Are, or have been, an officer or employee of the bank or its affiliates? | | | | |
| b. Serve or have served as the bank's or its affiliates' consultant, advisor, promoter, underwriter, legal counsel, or trustee? | | | | |
| c. Are relatives of a bank's or its affiliates' officers or employees? | | | | |
| d. Hold or control, or did not hold or control within the preceding year, either directly or indirectly, a financial interest of 10% or more in the bank or its affiliates? | | | | |
| e. Have outstanding extensions of credit from the bank or its affiliates? | | | | |
| f. Whether any committee member is a large customer of the bank? | | | | |
| | | | | |
| Are committee members: | | | | |
| a. Financially literate? | | | | |

| | Yes | No | N/A | Comments |
|---|---|---|---|---|
| b. Do they have banking or related financial management expertise? (Required for banks subject to 12 CFR 363 and OCC registered banks) | | | | |
| | | | | |
| Does the committee have access to its own counsel at its own discretion and without prior approval of the board or management? (Required for banks subject to 12 CFR 363 and OCC registered banks) | | | | |
| | | | | |
| Does the committee perform all duties as determined by the board of directors, including reviewing, as applicable, with management and the IPA: (Required for 12 CFR 363 and OCC-registered banks) | | | | |
| a. The scope of services required by the external audit (i.e., IPA's responsibilities under GAAS)? | | | | |
| b. The basis of Part 363 required reports? [3] | | | | |
| c. Significant accounting policies? | | | | |
| d. Management judgments and accounting estimates? | | | | |
| e. Audit adjustments and passed or waived adjustments? | | | | |

[3] The required reports are: (1) management's report and assertion on internal controls over financial reporting and compliance with designated laws, (2) independent public accountant's audit and report on the bank's financial statements, and (3) independent public accountant's attestation report on management's control assertion.

| | Yes | No | N/A | Comments |
|---|---|---|---|---|
| f. IPA's judgment about the quality of the bank's accounting principles? | | | | |
| g. Other information in documents containing audited financial statements? | | | | |
| h. Disagreements between the IPA and management? | | | | |
| i. Assessments of internal control adequacy and resolution of identified material internal control weaknesses and reportable conditions? | | | | |
| j. The institution's compliance with laws and regulations? | | | | |
| k. Consultations with other accountants? | | | | |
| l. Major issues discussed with management prior to retention of the IPA? | | | | |
| m. Difficulties encountered in performing the audit? | | | | |
| | | | | |
| Does the committee oversee the internal audit function? (Required for banks subject to 12 CFR 363) | | | | |
| | | | | |
| Does the committee discuss with management the selection and termination of the IPA? (Required for 12 CFR 363 and OCC-registered banks) | | | | |
| | | | | |

| | Yes | No | N/A | Comments |
|---|---|---|---|---|
| Does the audit committee pre-approve all audit and permitted non-audit services provided by the IPA? (Required for OCC-registered banks) | | | | |
| | | | | |
| Does the committee on an annual basis: (Required for OCC-registered banks) | | | | |
| a. Receive and review written disclosures from the IPA disclosing all relationships between the IPA and its related entities and the bank and its related entities that, in the IPA's judgment, may reasonably bear on independence? | | | | |
| b. Review the above letter to ensure that the IPA confirms they are independent of the bank? | | | | |
| c. Discuss the IPA's independence with the IPA? | | | | |
| | | | | |
| Does the committee recommend to the board of directors that the audited financial statements be included in the bank's annual report? (Required for OCC-registered banks) | | | | |
| | | | | |
| Does the committee review the aggregate fees billed by the IPA for: (Required for OCC-registered banks) | | | | |
| a. The annual financial statement audit? | | | | |

| | Yes | No | N/A | Comments |
|---|---|---|---|---|
| b. Other audit-related services? | | | | |
| c. Tax services? | | | | |
| d. All other products and services provided by the IPA for the most recent fiscal year? | | | | |
| | | | | |
| Does the committee review the hours spent on the bank's financial audit by persons other than the IPA's full-time permanent employees? (Required for OCC-registered banks) | | | | |
| | | | | |

# Appendix I: Audit Rating Guidance – Community Banks

Examiners should consider the following key attributes when assessing the quality of a community bank's overall audit program. It is not necessary for the audit program to meet every attribute to be accorded a specific rating of strong, satisfactory, or weak. These key attributes are normally present to distinguish between ratings, but examiners will need to factor in the bank's size, the nature of its activities, and its risk profile to arrive at an overall rating.

**Strong**

Overall, a **strong** audit program is assigned a high level of respect, credibility, and stature in the organization, which is continually confirmed by management and board attitudes, actions, and support. Audit's role is clearly spelled out and incorporated into overall risk management, new product and service deployment, changes in strategy, and organizational and structural changes. The OCC can fully rely on the work and conclusions of the audit function.

Board/Audit Committee Oversight - The board, or its committee assigned audit oversight responsibility, is proactive in dealing with management and risk management issues in a timely manner. Reports and information submitted to the board or committee are clear and understandable in their discussions of issues, emerging risks, corrective actions, testing, and resolution of outstanding items. The board or committee maintains dialogue with internal and external auditors, regulators, and management and involves all appropriate groups in discussions on new business ventures, the potential risks involved, and planned controls. The board or committee takes an active role in reviewing and approving overall annual audit plans, for both internal audit and the external audit engagement, as well as setting expectations for the roles of both internal and external auditors and evaluating their performance under the plan. The use of external auditors is clearly defined in engagement letters.

Audit Management and Processes - Internal audit management possesses industry expertise and knowledge to match the sophistication and complexity of the bank's risk profile and operations. Audit is independent in executing audit plans and audit programs and discussing issues with the board/audit committee and regulators. Audit scopes and report findings are supported by

work papers. Internal auditors address control deficiencies in a timely manner and perform thorough follow-up testing to ensure that corrective measures are effective. Internal audit plans are completed with minimal carryover or have appropriately supported amendments based on significant changes in the bank's risk profile.

The internal and external audit processes are fully effective. Any outsourced or co-sourced internal audit duties or assignments are effective and appropriately managed by the bank. Audit processes include indicators and descriptions of key risks and controls in place. Management information systems are timely, accurate, complete and reliable.

Responsibilities between audit and other risk management oversight functions are well delineated. If appropriate, risk and frequency models are effectively used, and accurately reflect the risk posed by the bank's activities. Overall audit planning is effective and timely in addressing audit needs for low- and moderate-risk areas. Audit scopes are flexible to the extent of addressing new business lines, products, and activities, and, if appropriate, merger/acquisition situations.

Audit Reporting - Internal audit reports clearly outline the causes of problems and specifically point out management issues when present. There are few differences between bank-assigned audit assessments and examiner assessments for internal controls. Internal audit ratings, if used, are well defined and are fully effective in identifying areas where control weaknesses exist. Work paper documentation effectively supports the findings presented in the reports and the audit ratings assigned.

Internal Audit Staffing - Audit staffing and experience fully complements the level of risk undertaken by the bank. Staff turnover is minimal and vacancies are promptly addressed and have little or no affect on internal audit plans or processes. Recruitment and training processes are effective. The audit staff possesses a high level of knowledge of the areas audited.

**Satisfactory**

Overall, a **satisfactory** audit program attains an adequate level of respect and stature in the organization and is generally supported by the actions of management and board. Audit's role in overall risk management and its participation in new product and service deployment, changes in strategy,

and organizational and structural changes may be limited, but is conducted effectively.

Board/Audit Committee Oversight - The board or audit committee is effective in their oversight of the audit program. Reports and information presented to the committee provide sufficient information and discussion of significant audit and control issues. The committee holds senior management accountable for issues in their respective business lines. The committee understands the overall audit plans of internal audit and the engagement of external auditors and the respective roles to be performed by both internal and external auditors. The use of external auditors is clearly defined in engagement letters.

Audit Management and Processes - Internal audit management generally possesses the knowledge and experience to ensure adequate internal audit operations appropriate for the bank's size, activities, and risk profile. For small community banks, the lack of internal audit management independence is mitigated by effective internal controls. Internal audits and follow-up are timely, comprehensive, independent, and effective in assessing and monitoring controls. Audit programs, processes, and information systems are generally sound, and complement the control and risk management environment. Audit policies are generally effective, adhered to, and appropriate for the bank's size, complexity, and risk profile. The bank adequately manages outsourced or co-sourced internal audit duties or assignments.

Audit Reporting - Internal audit reports are clear, concise, and accurately reflect reviews of the area and the root causes of issues. Bank assigned internal audit ratings, if used, or assessments are adequately defined. Conclusion or assessment differences with examination findings may exist, but do not compromise the overall audit program. Internal audit work papers and programs support findings and conclusions.

Internal Audit Staffing - Audit staff is generally competent and experienced. The audit staff may have experienced some turnover and vacancies, but not to the extent of compromising internal audit plans and processes. Staff training is adequate.

**Weak**

Overall, a **weak** audit program is one that is not an integral part of the organization and the OCC cannot rely on the audit function's work or conclusions. The audit program does not have the full support of the board and management. Audit's role is unclear and not utilized in overall risk management, new product and service deployment, changes in strategy, and organizational and structural changes.

Audit Committee - The audit committee (or board if there is no committee) is not effective in their oversight of the audit program. Reports and information submitted to the board or committee are insufficient or not fully understood. The board or committee fails to follow-up on control and risk weaknesses noted by audit or to hold senior management accountable for issues in their respective business lines. The board or committee has a passive role in the overall audit plan or selection of the external audit engagement and is not involved in determining the respective roles of the internal and external auditors. Engagement letters describing the work to be performed by the external auditors are non-existent, incomplete, or not understood.

Audit Management and Processes - Weaknesses exist in internal audit management and processes, such as lack of competence or independence or inadequate scope of review, that are not mitigated by strong internal controls. Audit policies may exist, but need significant enhancements in light of the bank's size, complexity, and risk profile. Audit programs, processes, reports, and information systems are generally ineffective in addressing significant control or risk issues. Outsourced or co-sourced internal audit duties or assignments are ineffective or not appropriately managed by the bank.

Audit Reporting - Internal audit rating or assessment definitions are loosely defined or nonexistent. Audit reports are unclear and do not reflect accurate conclusions or fully identify the root causes of concerns. Significant conclusion or assessment differences exist with examination findings. Internal audit program work papers, in many cases, are insufficient or do not support findings and conclusions.

Internal Audit Staffing - Audit staff is inexperienced or lacks adequate knowledge. The internal audit area is understaffed or suffers from high turnover significantly affecting internal audit plans and processes. Management has failed to maintain the staff levels needed to fully support the internal audit function. Staff training is inadequate.

## Appendix J: Audit Rating Guidance – Large/Mid-size Banks

Examiners should consider the following key attributes when assessing the quality of a large or mid-size bank's overall audit program. It is not necessary for the audit program to meet every attribute to be accorded a specific rating of strong, satisfactory, or weak. These key attributes are normally present to distinguish between ratings, but examiners will need to factor in the bank's size, the nature of its activities, and its risk profile to arrive at an overall rating.

### Strong

Overall, a **strong** audit program attains the highest level of respect and stature in the organization, which is continually confirmed by management and board attitudes, actions, and support. Audit's role is clearly spelled out and incorporated into overall corporate risk management, new product and service deployment, changes in strategy and tactical plans, and organizational and structural changes. The OCC can fully rely on the work and conclusions of the audit function.

Audit Committee – A formal audit committee charter exists, clearly sets out the committee's responsibilities, reflects current industry and regulatory trends, is reviewed on an annual basis and updated as warranted, and is shared with the board of directors, internal auditors, and external auditors. The audit committee ensures adherence to the spirit and intent of legislative and regulatory requirements. The committee's tone is a positive impact on the organization and its audit and internal control culture. The audit committee is effective in holding management accountable for timely and appropriate responses to audit, control, and risk management issues. Reports to the audit committee are clear in their discussions of both horizontal and business line issues. The committee reviews corrective actions, testing, and resolution of significant issues. Reporting and discussions also include emerging issues and a profile of enterprise-wide risk in the company. Risks are reported across the company for all areas and discussed in an appropriate manner given the significance of risk issues. The committee receives presentations on key businesses and risks; maintains frequent dialogue with regulators; and engages in prospective discussions on new business ventures, the potential risks involved, and planned controls. The committee takes an active role in overseeing internal and external audit functions by meeting

regularly with internal and external auditors and examiners, selecting external auditors and pre-approving audit services to be performed (through clearly defined engagement letters), terminating audit engagements, and reviewing and approving the overall annual audit plans of internal audit and external audit engagements. They also set expectations for the roles of both internal and external auditors, evaluate the auditors' performance under the audit plans, and ensure auditor independence and qualifications to perform the work. The committee has significant input regarding hiring, compensation, and performance evaluation of the internal audit manager.

Audit Management and Processes - Internal audit is highly perceived, respected, and visible throughout the organization. Audit management possesses significant industry expertise and knowledge to match the sophistication and complexity of the bank's risk profile and operations and to challenge management when necessary. Internal audit activities integrate compliance, information technology, accounting, and credit areas when those areas overlap. An audit management and subject matter expert succession plan is in place and if audit management turnover occurs the positive aspects outweigh the negative. Internal audit is independent by virtue of reporting lines to the board and the board's support in executing the audit plan and audit programs. Internal audit is very or highly effective in follow-up actions and ensuring change. Follow-up reviews are completed in a timely manner, and testing for management's corrective actions is thorough. Audit processes and teams have been effective in raising and addressing issues in merger activities. Horizontal and silo risk issues across the corporation are effectively addressed, discussed, and reported in real time to the fullest extent possible through the audit processes, i.e., continuous or traditional audit. Audit plans are completed without any carryover or have appropriately supported amendments based on significant changes in the bank's risk profile.

The internal audit process is fully effective and may include results obtained from traditional and/or continuous audit activities, early warning indicators, management call programs, etc. The audit process effectively utilizes a level and combination of audit tools, as well as a balanced approach of core audit and consulting/special request activities, to meet the annual audit plan. Testing and sampling methods, and associated work papers, fully support conclusions reached. Any internal audit duties or assignments that have been outsourced or co-sourced are effective and appropriately managed. Internal audit processes include key indicators and well-developed descriptions of key

risks and controls in place. Audit takes an active role in helping management's FDICIA control assessment and SEC certification process and maintains documentation supporting management's assertions. Key indicators are being effectively used as an early warning tool for risk management. Management information systems are timely, accurate, complete and reliable. An effective quality assurance process is in place that is well staffed and provides timely feedback (i.e., quarterly) on reporting, ratings, testing, documentation, and audit processes. Results of the quality assurance process are used to effect positive changes to the audit function.

Responsibilities between audit and other risk management oversight functions are well delineated. Audit has identified key systems, critical management reports, laws, and regulations relating to each business line. Risk and frequency models are well defined, accurately reflect the risk, and are consistently applied across business lines. The audit planning horizon is long-term and it effectively addresses overall audit needs for low- and moderate-risk areas in a timely fashion. Joint ventures and minority subsidiary activities are appropriately addressed in the internal and external audit program scopes. Audit scopes are flexible to the extent of adding new business lines and merged activities.

Audit Reporting - Internal audit reports clearly outline the causes of problems and specifically point out management issues when present. There are few differences between bank-assigned internal audit ratings or assessments and examiner assessments for internal controls in the business line audits. Internal audit ratings or assessments are well defined and are fully effective in identifying areas of increased levels of control weaknesses. In addition to the control or summary audit rating, each audit report denotes the risk assessment for the unit, including a description of the rationale for the risk assignation. Internal audit work paper documentation fully supports the findings presented in the reports and the audit ratings assigned.

Internal Audit Staffing - Audit staffing is appropriate relative to the level of risk undertaken by the bank. Staff turnover is minimal and vacancies are promptly addressed and have little or no affect on audit plans or processes. Recruitment and training processes are active and ongoing. The audit function is viewed as management training ground, with audit staff rotating into management ranks. The audit staff includes subject matter experts, who are active in industry related organizations. The staffing plan provides for management succession within the internal audit group.

**Satisfactory**

Overall, a **satisfactory** audit program attains an adequate level of respect and stature in the organization and is generally supported by the actions of management and board. Audit's role in overall corporate risk management and participation in new product and service deployment, changes in strategy and tactical plans, and organizational and structural changes may be limited, but is conducted in accordance with its assigned responsibilities. The OCC can rely on a majority of the work and conclusions of the audit function.

Audit Committee – A formal audit committee charter exists and is regularly reviewed and shared with appropriate parties; it adequately sets out the committee's responsibilities, although some enhancements may be needed in light of current industry and regulatory trends. The audit committee's actions are generally effective in overseeing the audit program and setting a good audit and control culture. Reports presented to the committee provide sufficient information and discussion of significant audit, control, and risk issues in light of the organization's activities and risk profile. The committee holds senior management accountable for issues in their respective business lines. The committee understands and approves the overall audit plans for both internal audit and the external audit engagement, and they are involved in setting the respective roles of both internal and external auditors.

Audit Management and Processes - Internal audit management is independent and generally possesses the knowledge and experience to ensure adequate internal audit operations appropriate to the bank's activities and risk profile. An audit management and subject expert succession plan has been informally considered. Audits and follow-up are timely, comprehensive, independent, and effective in assessing and monitoring controls and risk. Audit programs, processes, and information systems are generally sound, adequately meet regulatory requirements and guidance, and complement the control and risk management environment. Annual audit plans reflect some carryover or amendments, but these are fully supported and approved by the audit committee. Audit policies are effective, adhered to, and appropriate for the bank's size, complexity, and risk profile. Senior level audit management adequately manages outsourced or co-sourced internal audit duties or assignments. A quality assurance process is in place that conducts annual or semi-annual reviews and uses significant results to improve the audit function.

Audit Reporting - Internal audit reports are clear, concise, and reflect an assigned rating properly based on reviews of the area and the root causes of issues. Internally assigned audit ratings or risk/control assessments are adequately defined. Any differences with examination findings are adequately explained and do not compromise the overall internal audit program. Internal audit program work papers support findings and conclusions.

Internal Audit Staffing - Audit staff is generally competent and experienced. The internal audit staff, as a whole or in certain groups, experiences some turnover and vacancies, but not to the extent of compromising internal audit plans and processes. Staff training and expertise is adequate.

**Weak**

Overall, a **weak** audit program is one that is not an integral part of the organization. The audit program does not have the full support of or appropriate oversight by the board and management. Audit's role is unclear and not utilized in overall corporate risk management, new product and service deployment, changes in strategy and tactical plans, and organizational and structural changes. Significant internal control weaknesses are not fully identified by the audit function or corrected in a timely manner. The OCC cannot rely on the work and conclusions of the audit function.

Audit Committee – A formal audit committee charter may or may not exist. If one exists, it is not current, does not sufficiently set out the committee's responsibilities, and it has not been shared with the board of directors, internal auditors, or external auditors. The audit committee is complacent, meets infrequently or for short time periods, and its impact on the organization and the audit and control culture is not conducive for effective oversight of the audit program. Reports and information submitted to the committee are insufficient or not fully understood. The committee fails to adequately follow-up on control and risk weaknesses noted by audit or to hold senior management accountable for issues in their respective business lines. The committee has a passive role in overall audit planning or selection and/or oversight of the external audit engagement and is not involved in determining the respective roles of the internal and external auditors. Engagement letters describing the work to be performed by external auditors are non-existent, incomplete, or not understood by the board or audit

committee. The committee has little or no input in the hiring, compensation, or performance evaluation of the internal audit manager.

Audit Management and Processes - Weaknesses exist in internal audit management and processes, such as lack of competence or expertise matching the complexity and risk profile of the organization's operations. Audit management or subject matter expert succession plans are lacking or are ineffective, and audit management turnover is a negative impact on the overall audit process. Independence issues or inadequate scope of reviews are not mitigated by strong internal controls and audit management tends to back off when challenged by senior management. Audit policies exist, but are not current and may need significant enhancements in light of recent industry trends and the bank's size, complexity, and risk profile. Annual audit plans/schedules are not met due to limited resources, poor planning, or an unbalanced approach between core audit activities and special request or consulting activities. Audit programs, processes, reports, and information systems are generally ineffective in addressing significant control or risk issues and supporting conclusions. Audit processes may not reflect effective use of current or appropriate audit tools, and do not meet regulatory requirements and guidance. Risk assessments are ineffective and not reflected in audit planning. Outsourced or co-sourced internal audit duties or assignments are ineffective and have not been appropriately managed by an appropriate level of audit management. A quality assurance process does not exist or is not properly used to enhance the audit function.

Audit Reporting - Bank-assigned internal audit rating or assessment definitions are loosely defined or nonexistent. Internal audit reports are unclear, do not reflect accurate ratings or assessments based on reviews of the area, or do not fully identify the root causes of issues. Significant rating or assessment differences exist with examination findings. Internal audit program work papers, in many cases, are insufficient or do not support findings and conclusions.

Internal Audit Staffing - Audit staff is inexperienced or lacks adequate knowledge and suffers from high turnover/vacancies, which significantly affect internal audit plans and processes. Audit staff levels are significantly smaller than peer. Management has failed to maintain the staff levels and expertise needed to fully support the internal audit program in light of the organization's activities and risk profile. Staff training is inadequate.

# References

**Laws**

12 USC 1831m, Early Identification of Needed Improvements in Financial Management
12 USC 1831p-1, Standards for Safety and Soundness
15 USC 78m, Periodical and Other Reports
Pub. L. 107-204, 116 Stat. 745 (2002), Sarbanes-Oxley Act of 2002

**Regulations**

12 CFR 9.9, Audit of Fiduciary Activities
12 CFR 11.2, Requirements under Certain Sections of the Securities Exchange Act of 1934
12 CFR 21.21, Procedures for Monitoring Bank Secrecy Act Compliance
12 CFR 30, Safety and Soundness Standards
12 CFR 363, Annual Independent Audits and Reporting Requirements
17 CFR 210.1 through 210.4, Form and Content of and Requirements for Financial Statements
17 CFR 229.306, Audit Committee Report
17 CFR 229.309, Audit Committee Financial Experts
17 CFR 240.14a-101, Schedule 14A, Information Required in Proxy Statement

**OCC Issuances**

OCC 2003-12, "Interagency Policy Statement on Internal Audit and Its Outsourcing"
OCC 99-37, "Interagency Policy Statement on External Auditing Programs"
Comptroller's Handbooks:
- Community Bank Supervision
- Compliance Management System
- Large Bank Supervision

"The Director's Book: The Role of a National Bank Director"
Federal Financial Institutions Examination Council, *Information Systems Examination Handbook*

**Industry Reference Sources**

*AICPA Audit and Accounting Guide, Banks and Savings Institutions*
*AICPA Professional Standards*
*AICPA Independence Standards*
(http://www.aicpa.org/about/code/et101.htm)
*AICPA Peer Reviews*
(http://www.aicpa.org/members/div/practmon/index.htm)
AICPA Statement on Auditing Standards:
41, "Working Papers", "Providing Access to or Photocopies of Working Papers to a Regulator" (AU Section 9339)
55, "Consideration of the Internal Control Structure in a Financial Statement Audit"
58, "Reports on Audited Financial Statements"
60, "Communication of Internal Control Structure Related Matters Noted in an Audit"
61, "Communication with Audit Committees"
70, "Reports on the Processing of Transactions by Servicing Organizations"
71, "Interim Financial Information"
78, "Consideration of Internal Control in a Financial Statement Audit: An Amendment to SAS 55"
90, "Audit Committee Communications"
96, "Audit Documentation"

Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Internal Control — Integrated Framework*. Vol. 1, *Executive Summary*. Vol. 2, *Framework*. Vol. 3, *Reporting to External Parties*. Vol. 4, *Evaluation Tools*.

Independence Standards Board
Standard No.1, "Independent Discussions with Audit Committees"
Interpretation 99-1, "FAS 133 Assistance"

The Institute of Internal Auditors, *Standards for The Professional Practice of Internal Auditing*

*Internal Auditor* (periodical)

New York Stock Exchange, National Association of Securities Dealers, "Report and Recommendations of the Blue Ribbon Committee on

Improving the Effectiveness of Corporate Audit Committees" (http://www.nyse.com/, http://www.nasd.com/)

U.S. Securities and Exchange Commission Independence Rule (http://www.sec.gov/rules/final/33-8183.htm)

Securities and Exchange Commission Staff Accounting Bulletin No.99, "Materiality"

**Web Sites**

AICPA (http://www.aicpa.org/)
Bank Administration Institute (http://www.bai.org/)
Independence Standards Board (http://www.cpaindependence.org/)
Institute of Internal Auditors (http://www.theiia.org/)
OCC Library, Banking and Business (OCC intranet)
U.S. Securities and Exchange Commission (http://www.sec.gov/)