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.