Comptroller's Handbook

Safety and Soundness

Capital Adequacy (C) | Asset Quality (A) | **Management (M)** | Earnings (E) | Liquidity (L) | Sensitivity to Market Risk (S) | Other Activities (O)

Internal and External Audits

Version 1.0, December 2016

Version 1.1, July 2019

Office of the Comptroller of the Currency

Contents

Introduction

The Office of the Comptroller of the Currency's (OCC) *Comptroller's Handbook* booklet, "Internal and External Audits," is prepared for use by OCC examiners in connection with their examination and supervision of national banks and federal savings associations (collectively, banks). Each bank is different and may present specific issues. Accordingly, examiners should apply the information in this booklet consistent with each bank's individual circumstances. When it is necessary to distinguish between them, national banks[1] and federal savings associations (FSA) are referred to separately.

This booklet addresses the risks inherent in the audit functions, comprising both internal and external audit functions, and the audit function's role in managing risks. The booklet addresses internal and external audit functions' effect on risk management supervisory expectations and the regulatory requirements for prudent risk management.

The booklet includes guidance and examination procedures to assist examiners in completing bank core assessments that are affected by the audit functions. The procedures include verification procedures to further support the examination process. This booklet's appendixes provide relevant laws and regulations, guidance on internal and external audits, worksheets, a glossary, and other references.

The examination procedures and other reference material in this booklet supplement the core assessment audit guidance in the "Community Bank Supervision," "Federal Branches and Agencies Supervision," and "Large Bank Supervision" booklets of the *Comptroller's Handbook*.

Background

Well-planned, properly structured auditing programs are essential to effective risk management and internal control systems.[2] 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 bank's audit programs are as follows:

[1] Generally, references to "national banks" throughout this booklet also apply to federal branches and agencies of foreign banking organizations unless otherwise specified. Refer to the "Federal Branches and Agencies Supervision" booklet of the *Comptroller's Handbook* for more information regarding applicability of laws, regulations, and guidance to federal branches and agencies. (Footnote added version 1.1)

[2] Refer to the "Internal Control" booklet of the *Comptroller's Handbook* (national banks) and *Office of Thrift Supervision (OTS) Examination Handbook* section 340, "Internal Control" (FSAs), which supplements the internal control core assessment standards in the "Large Bank Supervision" and "Community Bank Supervision" booklets of the *Comptroller's Handbook*. Refer to other *Comptroller's Handbook* booklets for guidance on assessing controls for specific banking products and activities. (Footnote updated version 1.1)

- The board of directors and senior management should not delegate their responsibilities for establishing, maintaining, and operating effective audit programs. (Updated version 1.1)
- Bank audit programs must be performed by independent and competent staff who are objective in evaluating the bank's control environment.[3] (Updated version 1.1)
- Examiners must validate the adequacy of the bank's audit programs.

OCC examiners assess and draw conclusions about the adequacy of the bank's overall audit function as part of every supervisory cycle. This assessment includes some level of audit validation, including verification procedures as necessary. The conclusions can significantly influence the scope of other supervisory activities for the bank. Examiners expand supervisory activities in applicable areas if they identify significant concerns about the quality or extent of audit programs or the control environment.

Three Lines of Defense

The three lines of defense model explains governance and roles among the bank's business units, support functions, and the internal audit function from a risk management perspective. First line of defense risk management activities take place at the frontline units[4] where risks are created. The second line of defense risk management activities occur in an area or function separate from the frontline unit, sometimes referred to as independent risk management.[5] It oversees and assesses frontline units' risk management activities.

The internal audit function is often referred to as the third line of defense in this model. In its primary responsibility of providing independent assurance and challenge, the internal audit function assesses the effectiveness of the policies, processes, personnel, and control systems created in the first and second lines of defense. Refer to the "Corporate and Risk Governance" booklet of the *Comptroller's Handbook* for more information on the three lines of defense.

Risk-Based Auditing

The OCC encourages a risk-based approach for auditing banks. Risk-based auditing is a methodology that links internal auditing to the bank's overall risk management framework. The audit risk assessment is a process by which an auditor identifies and evaluates the quantity of the bank's risks and the quality of its risk controls. The bank's board, or its audit committee, and the auditors use the results of the risk assessments to focus on the areas of

[3] Refer to 12 CFR 30, appendix A, II.B, "Internal Audit System." Also refer to 12 CFR 30, appendix D, I.E.8, "Internal Audit," for large banks covered by the OCC's heightened standards.

[4] The OCC's guidelines establishing heightened standards for certain large banks define the term "front line unit." Refer to 12 CFR 30, appendix D, I.E.6, "Front Line Unit."

[5] The OCC's guidelines establishing heightened standards for certain large banks use the term "independent risk management" for units with the responsibility for identifying, measuring, monitoring, or controlling aggregate risks. Such units maintain independence from frontline units. Refer to 12 CFR 30, appendix D, I.E.7, "Independent Risk Management."

greatest risk and to set priorities for audit work. An internal audit function should not ignore areas that are rated low-risk. An effective risk-based audit program includes adequate audit coverage for all of the bank's auditable activities. The frequency and depth of each area's audit should vary according to the audit risk assessment. Risk-based auditing allows internal audit to provide assurance to the board that risk management processes are managing risks effectively in relation to the bank's risk appetite. The bank's risk appetite should be commensurate with the bank's size and complexity. (Updated version 1.1)

Audit Programs

Effective audit programs should provide

- objective, independent reviews and evaluations of bank activities, internal controls, and management information systems (MIS).
- adequate documentation of tests, findings, and any corrective actions.
- assistance in maintaining or improving the effectiveness of bank risk management processes, controls, and corporate governance. (Updated version 1.1)
- reasonable assurance about the accuracy and timeliness with which transactions are recorded and the accuracy and completeness of financial and regulatory reports.
- validation and review of management actions to address material weaknesses.

The internal audit program is the bank's primary mechanism for assessing controls and operations and performing whatever work is necessary to allow the board and senior management to accurately attest to the adequacy of the bank's internal control system. Refer to the "Internal Audit Function" section of this booklet for more information. (Updated version 1.1)

Internal audit programs (including those that are outsourced or co-sourced) are often associated with

- independent and objective evaluation and testing of the bank's overall internal control system (such as operational and administrative controls beyond those associated with financial statement preparation).
- ensuring the safeguarding and proper recording of the bank's assets.
- determining compliance with laws, regulations, and established bank policies and practices.
- providing consultation and advisory services relating to such areas as new, expanded, or modified products and services, third-party risk management, and significant bank projects and initiatives.

External audit programs complement the internal auditing function of a bank by providing management and the board of directors with an independent and objective view of the reliability of the bank's financial statements and the adequacy of its internal controls over financial reporting. External audit programs typically focus on financial reporting and associated processes, as well as matters that might result in material weaknesses, financial internal control weaknesses, or misstatements that compromise the bank's financial

statements. Outsourced and co-sourced internal audit activities are not considered part of the external audit program. Refer to the "External Audit Function" section of this booklet for more information.

The bank's internal and external audit programs determine the types of audits or control reviews to be performed based on the bank's size, complexity, scope of activities, and risk profile. Auditors may perform these audits separately or integrate elements of each to achieve overall bank audit objectives of providing assurance or advisory services. Refer to appendix B, "Types of Audits and Control Reviews" of this booklet for a list of audits and control reviews typically performed at banks. Also refer to the "External Audit Function" section of this booklet for more information.

Risks Associated With Internal and External Audit Functions

From a supervisory perspective, risk is the potential that events will have an adverse effect on a bank's current or projected financial condition[6] and resilience.[7] The OCC has defined eight categories of risk for bank supervision purposes: credit, interest rate, liquidity, price, operational, compliance, strategic, and reputation. These categories are not mutually exclusive. Any product or service may expose a bank to multiple risks. Risks also may be interdependent and may be positively or negatively correlated. Examiners should be aware of and assess this interdependence. Examiners also should be alert to concentrations that can significantly elevate risk. Concentrations can accumulate within and across products, business lines, geographic areas, countries, and legal entities. Refer to the "Bank Supervision Process" booklet of the *Comptroller's Handbook* for an expanded discussion of banking risks and their definitions. (Updated version 1.1)

The primary risks associated with internal and external audit functions are operational, compliance, strategic, and reputation. The audit functions are key components of managing risks at the bank. Reduction in internal or external audit functions' effectiveness can indirectly increase risk in all categories.

Operational Risk

(Section updated version 1.1)

Operational risk is the risk to current or projected financial condition and resilience arising from inadequate or failed internal processes or systems, human errors or misconduct, or adverse external events. Operational risk is evident in all aspects of banking. A properly functioning audit program can serve to identify and mitigate operational risk.[8]

[6] Financial condition includes impacts from diminished capital and liquidity. Capital in this context includes potential impacts from losses, reduced earnings, and market value of equity.

[7] Resilience recognizes the bank's ability to withstand periods of stress.

[8] Refer to 12 CFR 30, appendix A, II.B. Also refer to the independence requirements in the "Internal Audit Function" and "External Audit Function" sections of this booklet.

Many banks outsource internal audit by using independent accounting firms or outside professionals to perform work traditionally conducted by internal auditors. While this can reduce operational risk by, for example, providing a level of expertise and audit coverage that could not be effectively or efficiently performed in-house, it also introduces third-party relationship risks. The bank board and management should engage in appropriate third-party risk management when outsourcing internal audit.

Compliance Risk

(Section updated version 1.1)

Compliance risk is the risk to current or projected financial condition and resilience arising from violations of laws or regulations, or from nonconformance with prescribed practices, internal bank policies and procedures, or ethical standards. The internal audit function is responsible for testing the adequacy of and compliance with bank policies, procedures, processes, and standards. The internal audit function should also test the bank's compliance with applicable laws and regulations. The audit functions themselves are covered by legal requirements such as 12 CFR 30 and 12 CFR 363. In some cases, such as financial reporting, internal and external audit functions are required to perform specific control assurances and reporting.[9] Noncompliance with legal requirements or with safety and soundness standards can expose the bank to serious consequences, including jeopardizing the reputation or condition of the bank, and may result in increased regulatory actions, including civil money penalties, and customer reimbursements.

Strategic Risk

(Section updated version 1.1)

Strategic risk is the risk to current or projected financial condition and resilience arising from adverse business decisions, poor implementation of business decisions, or lack of responsiveness to changes in the banking industry and operating environment. Although it does not set the bank's policies or make business decisions, the internal audit function can influence them by providing useful insight and advice when it comes to risk assessments, governance structure, and governance processes,[10] particularly over new, modified, or expanded bank products and services (collectively, new activities).[11] A lack of independent assurance by audit functions may result in strategic decisions that increase business line risks

[9] See appendix B, "Types of Audits and Control Reviews," for information on commonly required audits.

[10] Refer to Basel Committee on Banking Supervision (BCBS), "The Internal Audit Function in Banks," for guidance on the value of internal audit in the bank's strategic decision-making process. Refer to paragraph 81.

[11] Refer to OCC Bulletin 2017-43, "New, Modified, or Expanded Bank Products and Services: Risk Management Principles," for more information.

through ineffective policies, procedures, and controls contrary to the bank's risk appetite.[12] The board and management should consider the needs of the internal audit function in its strategic planning process and allocate sufficient resources for independence and appropriate scale as the bank's business strategies, size, complexity, or risk profile change.

Reputation Risk

(Section updated version 1.1)

Reputation risk is the risk to current or projected financial condition and resilience arising from negative public opinion. As the board-delegated independent risk management function of the bank, the audit functions promote safe and sound operation of the bank and compliance with laws and regulations. The audit function also demonstrates the bank's willingness and ability to manage risks. Real or perceived deficiencies in audit practices, which include external, outsourced, and co-sourced audit, may increase reputational risk. Because audit objectivity rarely can be observed directly, external stakeholders' confidence in auditor independence rests in large measure on their perception. A lack of confidence in audit objectivity directly affects confidence in the bank's financial reporting integrity, a situation that can increase likelihood of financial loss.

Risk Management

Each bank should identify, measure, monitor, and control risk by implementing an effective risk management system appropriate for the size and complexity of its operations. When examiners assess the effectiveness of a bank's risk management system, they consider the bank's policies, processes, personnel, and control systems. Refer to the "Corporate and Risk Governance" booklet of the *Comptroller's Handbook* for an expanded discussion of risk management. (Updated version 1.1)

All banks should have an effective audit program. Ideally, such a program consists of a full-time, continuous program of internal audit coupled with a sound external auditing program. An effective audit program substantially lessens the risk of a bank failing to detect potentially serious problems.

[12] Refer to 12 CFR 30, appendix D, III.B, "Provide Active Oversight of Management." The board of a large bank subject to heightened standards may rely on risk assessments and reports by internal audit for support in questioning, challenging, and, when necessary, opposing management recommendations and decisions.

Board and Management Oversight

Board of Directors

(Section updated version 1.1)

The bank board and senior management are responsible for having an effective system of internal controls and an effective internal audit system in place.[13] A system of internal controls is made up of both internal controls and information systems. The system of internal controls and the internal audit function should be appropriate to the bank's size and complexity and the scope and risk of its activities.[14]

The bank board should review the audit functions and should ensure the audit functions[15]

- effectively scope, test, and monitor the system of internal controls.
- promote the timeliness and accuracy of the bank's financial, operational, and regulatory reports.
- adequately document tests, findings, and any corrective actions.
- are sufficiently staffed with qualified persons.
- verify and review management actions to address material weaknesses in a timely manner.
- are independent and objective.[16]
- satisfy statutory, regulatory, and supervisory requirements.

The directors should ensure that the audit programs test internal controls to identify[17]

- inaccurate, incomplete, or unauthorized transactions.
- deficiencies in the safeguarding of assets.
- unreliable financial and regulatory reporting.
- violations of laws or regulations.
- deviations from the bank's policies and procedures.

[13] According to 12 CFR 30, appendix A, II.A, "Internal Controls and Information Systems," internal control systems include internal controls and information systems.

[14] Refer to 12 CFR 30, appendix A, "Interagency Guidelines Establishing Standards for Safety and Soundness." Requirements of the internal audit function are outlined in appendix A, II.B.

[15] Refer to 12 CFR 30, appendix A, II.B, and OCC Bulletin 2003-12, "Interagency Policy Statement on the Internal Audit Function and Its Outsourcing." For a bank whose size, complexity, or scope of operations does not warrant a full-scale internal audit function, a system of independent reviews of key internal controls may be used.

[16] Refer to the "Internal Audit Function" and "External Audit Function" sections of this booklet for further information on independence requirements.

[17] Refer to 12 CFR 30, appendix A.

- thematic control issues across business activities or auditable entities.
- the root cause of any significant control issue.

Directors may delegate the design, implementation, and monitoring of specific internal controls to management and the testing and assessment of internal controls to others. For a bank with trust powers that offers collective investment funds (CIF), the bank board must provide oversight for the annual audit of the CIF.[18] Refer to appendix B, "Types of Audits and Control Reviews," for further details on CIF audits.

When appropriate, the board establishes an independent audit committee to oversee audit functions. The board should maintain an approved set of written criteria for annually determining whether each potential or existing audit committee member is an outside director and is independent of management.[19] When assessing an outside director's relationship with the bank, the board should consider the issue not merely in connection with the director but also in connection with persons or organizations with which the director has an affiliation. Refer to the "Audit Committee" section of this booklet for further details on audit committee composition.

Minutes for board meetings or audit committee meetings, or both, should reflect decisions regarding internal and external audit activities and other audit or assurance activities, such as external audit engagement terms (including any decision to forgo an external audit) and the type of audits to be performed, the level of resources and experience of the auditors, or why an audit of a particular area is not necessary. The board's meeting minutes should also contain the results of and basis for the board's determinations with respect to each existing and potential audit committee member.[20]

Directors should be aware of significant risk and control issues for the bank's operations, especially for emerging technologies, information systems, new activities, and new or revised laws and regulations.[21] The board should consult with internal audit, along with other relevant functional areas, as part of due diligence before introducing new, expanded, or modified products or services.

Refer to the OCC's *The Director's Book: Role of Directors for National Banks and Federal Savings Associations* for more guidance on directors' responsibilities and accountabilities.

[18] Refer to 12 CFR 9.18(b)(6)(i), "Annual Audit," which stipulates direct oversight by the bank board. 12 CFR 150.260(b), "Collective Investment Funds," states that FSAs that invest funds of a fiduciary account in a CIF must comply with 12 CFR 9.18.

[19] Written criteria should demonstrate an understanding of audit committee composition regulatory requirements. For banks that are subject to 12 CFR 363, criteria should assist in determining outside director status (12 CFR 363.5(a)(3)) and in determining "independent of management" status in accordance with 12 CFR 363, appendix A.28, "'Independent of Management' Considerations."

[20] Refer to 12 CFR 363, appendix A, "Guidelines and Interpretations."

[21] Refer to OCC Bulletin 2017-43.

Audit Committee

(Section updated version 1.1)

Establishing an independent audit committee to oversee and maintain the audit functions is a good, and sometimes required, practice. 12 CFR 363.5(a) requires Federal Deposit Insurance Corporation (FDIC)-insured banks with $500 million or more in total assets to have a dedicated audit committee. Because FDIC-insured federal branches do not have separate boards of directors, the audit committee rule does not apply. Nonetheless, the FDIC-insured federal branch's home office and local management should ensure that duties similar to an audit committee are performed by qualified persons.[22] The OCC encourages all other banks to have a similarly structured audit committee.

The U.S. Securities and Exchange Commission (SEC) and the Sarbanes–Oxley Act of 2002 (SOX) also impose specific requirements on audit committees of public reporting companies aimed at strengthening their independence, effectiveness, and accountability. Audit committees of banks subject to 12 CFR 363 or the filing and reporting requirements of 12 CFR 11 and 12 CFR 16.17 must comply with SEC rulings and SOX, as appropriate. Refer to the "Assessment Elements" section of this booklet for further information.

Audit Committee Composition

For banks subject to 12 CFR 363, requirements related to composition of the audit committee vary by bank size.[23] For a bank that has $500 million or more but less than $1 billion in total assets as of the beginning of its fiscal year, all audit committee members must be outside directors, the majority of whom must be independent of management.[24] An outside director is a director who is not, and within the preceding fiscal year has not been, an officer or employee of the bank or an affiliate of the bank. For a bank that has $1 billion or more in total assets as of the beginning of its fiscal year, all audit committee members must be outside directors and independent of management.[25] The audit committee of any bank with more than $3 billion in total assets as of the beginning of its fiscal year must include members with banking or related financial management expertise, have access to its own

[22] 12 CFR 363, appendix A.27, "Composition," outlines audit committee requirements as they should be applied to banks and insured branches of foreign banks.

[23] 12 CFR 363.5(a) allows a bank with $500 million or more but less than $1 billion in total assets to have less than a majority of outside directors who are independent of management if the OCC determines that the bank has encountered hardships. These hardships relate to the retention and recruitment of a sufficient number of competent outside directors to serve on the bank's audit committee. Refer to appendix C, "12 CFR 363 Reporting," and table 1, "12 CFR 363 Applied to Subsidiary Banks of Holding Companies," of this booklet.

[24] Outside director requirements are defined in 12 CFR 363.5(a)(3). Provisions on independence of management are defined in 12 CFR 363, appendix A.28.

[25] Refer to 12 CFR 363.5(a)(1). (Footnote added version 1.1)

outside counsel, and not include any large customers of the bank.[26] The OCC encourages all banks not covered under 12 CFR 363 to establish an audit committee consisting entirely of outside directors.[27] If this is impracticable, outside directors should be the majority of the audit committee.

The board should maintain an approved set of written criteria for annually determining acceptance of existing or potential audit committee members.[28] Refer to the "Board of Directors" section of this booklet for more information.

Banks With Holding Companies

(Section updated version 1.1)

In some situations, the independent audit committee requirement may be satisfied by the bank's top-tier or mid-tier holding company audit committee, known as a consolidated audit committee. The OCC's heightened standards for certain large banks outline when a bank holding company's risk governance framework, including the independent audit committee, may be used for those covered banks. In general, the large bank and its parent company should have a substantially similar risk profile and the bank should represent 95 percent or more of the parent company's average total consolidated assets.[29] For all banks with $500 million or more in total assets, the independent audit committee requirements in 12 CFR 363 may be satisfied at a top-tier or mid-tier holding company level under some circumstances. The holding company must comply with the requirements otherwise applicable to the bank.[30] In addition, the bank must fall into one of two categories, first having total assets of less than $5 billion, or second, having total assets of $5 billion or more

[26] Refer to 12 CFR 363.5(b), "Committees of Large Institutions." "Banking or Related Financial Management Expertise" and "Large Customers" criteria are defined in 12 CFR 363, appendix A.32, "Banking or Related Financial Management Expertise," and 12 CFR 363, appendix A.33, "Large Customers," respectively. Refer to the glossary in appendix I of this booklet.

[27] Refer to OCC Bulletin 1999-37, "Interagency Policy Statement on External Auditing Programs: External Audit."

[28] 12 CFR 363, appendix A.27.

[29] 12 CFR 30, appendix D.I, "Introduction," lists criteria for when a covered bank may use its holding company risk governance framework.

[30] 12 CFR 30, appendix D.I, notes that the bank's use of the holding company audit committee does not negate its obligation to comply with 12 CFR 363 or other applicable laws or regulations.

and a composite CAMELS[31] rating of 1 or 2.[32] If the bank's composite CAMELS rating is downgraded to a 3 or worse, then the bank board should establish its own audit committee.[33]

Bank audit committee composition, whether consolidated or not, takes into account the holding company relationship. Officers and employees of a top-tier or mid-tier holding company may not serve on the bank's audit committee.[34] Members of the holding company audit committee (if the bank uses this committee) must meet all membership requirements of the largest subsidiary bank subject to 12 CFR 363.[35] When the bank maintains its own audit committee, the members of the top-tier or any mid-tier holding company audit committee may serve on the bank audit committee if they are otherwise independent of management of the bank.[36]

Fiduciary Audit Committees

A bank that exercises fiduciary powers must have a fiduciary audit committee.[37] The fiduciary audit committee must consist of the bank's directors or an audit committee of the bank's affiliate. There are two requirements for fiduciary audit committee membership. First, members must not include any officers of the bank or an affiliate who participate significantly in the administration of the bank's fiduciary activities. Second, these regulations limit how many members of a bank's fiduciary audit committee may also be members of any committee to which the board has delegated power to manage and control the bank's fiduciary activities. For national banks, less than half may also be members of such committees. For FSAs, no more than half may also be members of such committees. (Updated version 1.1)

[31] CAMELS integrates ratings from six component areas: capital adequacy, asset quality, management, earnings, liquidity, and sensitivity to market risk. Refer to the "Bank Supervision Process" booklet of the *Comptroller's Handbook* for more information.

[32] Refer to 12 CFR 363.1(b)(2). The OCC may revoke this exception to compliance at the bank level for any bank with total assets of more than $9 billion for any period during which the OCC determines that the exception would create a significant risk to the Federal Deposit Insurance Fund. Also refer to 12 CFR 363.1(b)(3). If a bank with more than $3 billion in total assets relies on the audit committee of the holding company to comply with audit committee composition rules, the holding company's audit committee shall not include any members who are large customers of the subsidiary bank.

[33] Pursuant to 12 CFR 363.1(b)(2), this is a requirement for banks with total assets over $5 billion.

[34] Refer to 12 CFR 363, appendix A.30, "Holding Company Audit Committees."

[35] Refer to 12 CFR 363, appendix A.4, "Comparable Services and Functions."

[36] Refer to 12 CFR 363, appendix A.30. Audit committee members must be independent of management, while banks with $500 million or more and less than $1 billion in total assets require a majority of audit committee members to be independent of management.

[37] Refer to 12 CFR 9.9(c), "Continuous Audit" (national banks), and 12 CFR 150.470, "Who Directs the Conduct of the Audit?" (FSAs).

Audit Committee Responsibilities

The audit committee should perform all duties determined by the bank board and the audit committee should maintain minutes and other relevant records of its meetings and decisions.[38] The bank board may fulfill audit committee responsibilities if the bank is not required to have an audit committee.[39] Refer to the "External Audit Function" and "Internal Audit Function" sections of this booklet for more information.

The audit committee's responsibilities should include the following:

- 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.
- Holding senior management accountable for establishing and maintaining an adequate and effective internal control system and processes.[40] (Updated version 1.1)
- Holding committee meetings with a frequency that facilitates oversight, at least four times a year.
- Establishing schedules and agendas for regular meetings with internal auditors, along with external auditors when providing oversight.
- Carrying out the appointment, termination, compensation, and oversight of the independent public accountant (IPA) or external auditor.[41]
- Ensuring external auditors are independent and objective in their findings and consistent with their independence principles and rules. Ensuring that external auditor engagement letters and any related agreements for services do not contain any unsafe and unsound limitation of liability provisions before commencing engagement.[42]

[38] Regardless of the audit committee being satisfied at the bank holding company level, the bank holding company audit committee records are not a substitute for records of the bank board or the bank audit committee. Refer to 12 CFR 363, appendix A.31, "Duties."

[39] Refer to 12 CFR 363.1(a), "Applicability," and 363.5(a), "Composition and Duties." Also refer to BCBS, principles 9 and 10, paragraphs 48–55.

[40] Refer to BCBS, "The Internal Audit Function in Banks." Annex 2 gives an overview of the responsibilities of an audit committee.

[41] According to 12 CFR 363.3(c), "Notice by Accountant of Termination of Services," 12 CFR 363.4(d), "Notice of Engagement or Change of Accountants," and 12 CFR 363, appendix A.20, "Notice of Termination," official notifications must be made to regulators on termination of the external auditor. Refer to the "External Audit" section of this booklet. Refer also to 12 CFR 19, subpart P, "Removal, Suspension, and Debarment of Accountants from Performing Audit Services," for requirements for other termination practices and procedures. (Footnote updated version 1.1)

[42] The board and an audit committee of a bank have this responsibility. For banks subject to 12 CFR 363, however, these unsafe and unsound provisions include those that indemnify the IPA against claims made by third parties; hold harmless or release the IPA from liability for claims or potential claims that might be asserted by the client bank, other than claims for punitive damages; or limit the remedies available to the client bank. Refer to 12 CFR 363.5(c) and OCC Bulletin 2006-7, "Interagency Advisory on the Unsafe and Unsound Use of Limitation of Liability Provisions in External Audit Engagement Letters."

- Monitoring the financial reporting process and overseeing the bank's establishment of accounting policies and practices. Reviewing the significant qualitative aspects of the bank's accounting practices, including accounting estimates, financial reporting judgments, and financial statement disclosures.
- Establishing and maintaining procedures (also known as whistle-blower procedures) for bank employees to submit confidential and anonymous concerns to the committee about questionable accounting, internal accounting control, or auditing matters.[43] Procedures should be set up for timely investigation of complaints received and appropriate documentation retention.
- Monitoring, tracking, and holding management accountable for effective and timely response in addressing deficiencies that auditors or regulators identify. (Updated version 1.1)

The audit committee's responsibilities may also include the following:

- Reviewing with bank management and the external auditor the scope of services, significant accounting policies, and conclusions regarding significant accounting estimates.
- Reviewing with bank management and the external auditor the effectiveness of internal controls over financial reporting, the resolution of related material weaknesses, and the prevention or detection of management overrides or compromises.
- Discussing with bank management and the external auditor any significant disagreements.
- Reviewing with bank management the bank's compliance with applicable laws and regulations.
- Overseeing the internal audit function.
- Maintaining minutes and other relevant records of audit committee meetings and decisions.
- Meeting with bank examiners at least once each supervisory cycle to discuss findings of OCC reviews, including conclusions regarding audit. (Updated version 1.1)

[43] According to OCC Bulletin 2003-12, in situations when the board fulfills the audit committee responsibilities, the procedures should provide for the submission of employee concerns to an outside director, timely investigation of complaints received, and appropriate documentation retention. Section 301 of the SOX, commonly known as the whistle-blower provision, requires public companies to implement a confidential system for the reporting of information regarding questionable accounting or auditing matters.

In overseeing the internal audit function, the audit committee's responsibilities should include the following:[44]

- Assigning responsibility for the internal audit function (i.e., bank's chief auditor) to a member of bank management.[45]
- Reviewing and approving audit strategies, audit policies, audit programs, and audit organizational structure.
- Documenting any risks and mitigations associated with the audit hierarchy reporting structure.
- Reviewing and approving internal audit's control risk assessments and the scope of the audit plan at least annually.
- Periodically reviewing internal audit's adherence to the audit plan.
- Reviewing and approving the selection and termination of any outsourced internal audit activities.[46]
- Ensuring that internal auditors (in-house or outsourced) are independent and objective in their findings and consistent with their independence principles and rules.
- Providing significant input into selection of senior internal audit personnel, setting compensation, and evaluating the performance of the chief auditor.
- Retaining auditors who are fully qualified to perform the audit activities.
- Establishing objective criteria to oversee the internal audit function and evaluate its performance, which should include any third-party risk management activities.[47]

The audit committee, for certain large banks covered under the OCC's heightened standards, may be appointed by the bank board to review and approve the bank's formal talent management program only with respect to the chief audit executive, his or her direct reports, and other potential successors. The program may be helpful to the audit committee in fulfilling its responsibility to approve all appointments, removals, and annual compensation and salary adjustments of the chief auditor. Refer to the "Audit Programs" section of this booklet for more information. (Updated version 1.1)

[44] Refer to OCC Bulletin 2003-12 for details unless noted otherwise.

[45] According to 12 CFR 30, appendix D, I.E.2, "Chief Audit Executive," which applies to certain large banks, the chief audit executive is the individual who leads the internal audit function and must be one level below the chief executive officer (CEO). Refer to 12 CFR 30, appendix D, I.E.8, and to the "Audit Management" section of this booklet.

[46] Refer to OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance," OCC Bulletin 2017-7, "Third-Party Relationships: Supplemental Examination Procedures," and OCC Bulletin 2017-21, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29," for more information. (Footnote updated version 1.1)

[47] According to OCC Bulletin 2003-12, performance criteria for audit personnel and the audit function as a whole can include the timeliness of each completed audit, comparison of overall performance to plan, and other measures.

Audit Committee Charter

A formal audit committee charter sets forth the objectives, authorities, responsibilities, and organization of the committee.[48] An audit committee charter can serve to remind committee members of their duties and responsibilities and to familiarize new members with these responsibilities. The audit committee should review, update as warranted, and approve its charter on an annual basis. This charter should be approved by the board and shared with internal and external auditors.

The formality and extent of a bank'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 a bank employee (generally referred to as the internal audit manager or chief audit executive) who understands the function, is independent of areas under review, and has no responsibility for operating the system of internal controls.[49] Some small banks do not have a formal internal or external audit program. Instead, 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. This booklet refers to the person with responsibility for the internal audit function as the chief auditor. (Updated version 1.1)

Audit Management

The chief auditor is the bank manager responsible for implementing board-approved audit directives. He or she oversees audit operations and provides leadership and direction in communicating and monitoring audit policies, practices, programs, and processes. The chief auditor should establish clear lines of authority and reporting responsibility for all levels of audit personnel and activities. The chief auditor also should ensure that members of the audit staff have the necessary experience, education, training, and skills to properly conduct assigned activities. In managing the internal audit function, the OCC expects the chief auditor to be responsible for internal audit's control risk assessments, audit plans, audit programs, and audit reports.[50] (Updated version 1.1)

Banks should conduct their internal audit activities according to existing professional standards and guidance. For example, the Institute of Internal Auditors' (IIA) *International Standards for the Professional Practice of Internal Auditing* provides standards and guidance for independence, professional proficiency, scope of work, performance of audit work,

[48] A public company must disclose whether it has an audit committee charter and, if so, make the charter publicly available. Refer to 17 CFR 229.407, "(Item 407) Corporate Governance." A stock exchange may require a company with shares listed on the exchange to have an audit committee charter.

[49] Refer to OCC Bulletin 2003-12.

[50] Ibid.

management of internal auditing, and quality assurance reviews.[51] Internal auditors should be familiar with these or similar standards.

Internal Audit Oversight and Structure

The bank board should have confidence that the reporting hierarchy of the chief auditor and the internal auditors enables the internal audit function to be impartial and not unduly influenced by managers of day-to-day operations. The chief auditor should have no responsibilities for operating the system of internal controls and should report functionally to the bank's audit committee. In the absence of a board audit committee, the chief auditor should functionally report to the board.

A dual bank reporting arrangement may also be used in which the chief auditor is functionally accountable to the audit committee but reports to another senior member of management on administrative matters.[52] Such an arrangement potentially limits the independence and objectivity of the chief auditor when auditing the senior executive's business units. In these circumstances, the chief financial officer, controller, or other similar managers should be excluded from overseeing the internal audit activities. In dual reporting, the objectivity of internal audit is best served when the chief auditor reports administratively to the chief executive officer (CEO). In addition, the chief auditor should have appropriate stature within the bank. The chief auditor should be positioned one level below the bank's CEO.[53] Refer to the "Outsourced Internal Audit Oversight Responsibilities" section of this booklet for other considerations in the reporting hierarchy. (Updated version 1.1)

Some banks seek to coordinate the internal audit function with several risk monitoring functions (e.g., loan review, market risk assessment, and legal compliance departments) by establishing an administrative arrangement under one senior executive. Coordination of these other monitoring activities with the internal audit function can facilitate the reporting of material risk and control issues to the audit committee, increase the overall effectiveness of these monitoring functions, better use available resources, and enhance the bank's ability to comprehensively manage risk. Such an administrative reporting relationship should be designed so as to not interfere with or hinder the chief auditor's functional reporting to and ability to directly communicate with the bank's audit committee. In addition, the audit committee should ensure that efforts to coordinate these monitoring functions do not result in the chief auditor compromising his or her independence. Furthermore, the chief auditor

[51] Refer to the IIA's website for standards and other material on internal auditing.

[52] The "Audit" booklet of the Federal Financial Institutions Examination Council (FFIEC) *Information Technology (IT) Examination Handbook* and the preamble to 12 CFR 30, appendix D, "OCC Guidelines Establishing Heightened Standards For Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches," describe administrative matters in this context to include routine personnel matters such as leave and attendance reporting, expense account management, and other departmental matters. Refer to 79 Fed. Reg. 54518, at 54527.

[53] Refer to 12 CFR 30, appendix D, I.E, "Definitions." For large banks subject to the OCC's heightened standards, the chief audit executive must be positioned one level below the bank's CEO.

should have the ability to independently audit these other risk monitoring functions. (Updated version 1.1)

In structuring the reporting hierarchy, the bank board should periodically weigh the risk of diminished independence against the benefit of reduced administrative burden in adopting any dual reporting organizational structure. The audit committee should document its consideration of reporting hierarchy risks and mitigating controls.[54]

Internal audit functions of foreign banking organizations (FBO) should cover the FBO's U.S. operations.[55] 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 or audit committee and senior management. Refer to the "Federal Branches and Agencies Supervision" booklet of the *Comptroller's Handbook* for more information.

Internal Audit Charter

Each bank should have an internal audit charter or mission statement that formally articulates the purpose, responsibilities, standing, and authority of the bank's internal audit function in a manner that promotes an effective internal audit function.[56]

An internal audit charter should establish the following:

- The objective and scope of the internal audit function.
- The internal audit function's reporting position within the bank and its relationship to other control functions,[57] as well as its responsibility and authority.
- The responsibility and accountability of the chief auditor.
- The internal audit function's responsibility to evaluate effectiveness of the bank's risk management, internal controls, and governance processes.
- The criteria for when and how the internal audit function may be outsourced, in full or in part, to external experts.

[54] Refer to OCC Bulletin 2003-12.

[55] The OCC charters several types of FBOs that include subsidiary charter, federal branch, limited federal branch, federal agency, and loan production office.

[56] Smaller banks may articulate the internal audit charter in a mission statement.

[57] Refer to the "Internal Audit Function" and "Internal Audit Oversight and Structure" sections of this booklet for information on reporting structures and audit committee oversight responsibilities.

The internal audit charter promotes an effective internal audit function by providing guidance on the following:[58]

- The key features for the operation of an internal audit function. These features include independence, objectivity, competence, and due professional care and ethics.
- The terms and conditions according to which the internal audit function can be called on to provide consulting or advisory services or to carry out other special tasks.
- The obligation of the internal auditors to communicate the results of their engagements and a description of how and to whom this should be done (reporting line).
- Compliance with sound internal auditing standards.
- Procedures for the coordination of the internal audit function with the external auditor.

The internal audit charter should provide the internal audit function with the authority for direct access to any records, files, or data (including MIS and board or audit 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.

Bank audit management should develop the charter and periodically review it for any needed changes. The bank board or its audit committee should approve or confirm the audit charter and any subsequent changes made to it. The internal audit charter should be available to all internal stakeholders of the organization and, in certain circumstances, such as listed entities, to external stakeholders and communicated throughout the bank.

Board or Audit Committee Reports

The chief auditor should prepare board or audit committee reports as part of his or her regular reporting to and discussions with the audit committee. (The OCC recommends reporting at least quarterly.) Executive summary reports or audit information packages might include the following:

- Status of meeting the annual audit plan.
- Activity reports for audits completed, in process, and deferred or cancelled.
- Staffing and training reports.
- Discussion of significant accounting issues and regulatory reports and findings, including the root cause of issues and their impact on the organization.
- Summaries of audits.
- Risk assessments or summaries.
- Tracking reports for outstanding audit and control issues.
- Other information the audit committee or internal auditor deems appropriate.

Refer to the "Internal Audit Function" section of this booklet, which provides further information on individual reporting elements in alignment with the given activity.

[58] Refer to BCBS, "The Internal Audit Function in Banks," for information on internal audit charter elements relating to banks operating internationally.

Outsourced Internal Audit Oversight Responsibilities

Internal audit outsourcing is a third-party relationship between the bank and a third party to provide internal audit services. Outsourcing arrangements take many forms and are used by banks of all sizes. The third party may be an outside vendor or a person employed by the bank's holding company or one of its other affiliates (referred to as related organizations). Partial outsourcing, also known as co-sourcing, occurs when the outsourced internal audit services are performed in concert with bank employees. Some banks use these arrangements to enhance the quality of their control environment by obtaining the services of third parties with specialized expertise and knowledge to critically assess and recommend improvements to internal control systems. Banks may also use co-sourcing to help the bank's audit staff members develop their own knowledge and expertise. Large banks and those with international activity are encouraged to use their own staff and limit outsourcing of internal audit activities.[59]

The bank board and senior management should ensure that the outsourced internal audit functions or activities are competently managed and comply with the principles of the bank's internal audit charter.[60] As a matter of safety and soundness, the outsourced internal auditor should not perform management functions, make management decisions, or act or appear to act in a capacity equivalent to that of a member of management or an employee.[61] (Updated version 1.1)

The OCC expects the bank board and audit management to provide active oversight of the outsourced internal audit activities.[62] Larger banks and more formally structured community banks should have internal audit departments or internal audit managers oversee the third party. Small banks should appoint a qualified and competent employee to act as a point of contact between the bank and the third party and to oversee the third party. (This individual may or may not be a formally designated chief auditor). The chief auditor is responsible for approving the audit scope, plan, and procedures to be performed.[63] Furthermore, the chief auditor is responsible for the results of the outsourced audit work, including findings, conclusions, and recommendations. The third party may report these results jointly with the chief auditor to the audit committee.[64] (Updated version 1.1)

---

[59] Refer to BCBS, "The Internal Audit Function in Banks," June 2012, principle 15: "Outsourcing of Internal Audit Activities," which recommends that large banks and internationally active banks perform internal audit activities using their own staff.

[60] Refer to OCC Bulletin 2003-12.

[61] Ibid.

[62] Ibid.

[63] Ibid.

[64] Ibid.

Because the internal audit function is critical to managing the risks of the bank, the bank board and management should employ appropriate third-party risk management.[65] Entering into an internal audit outsourcing arrangement may increase operational and other risks. The board should have a contingency plan in place to mitigate any significant disruption in audit coverage should this arrangement be suddenly terminated. This is particularly important for auditing of high-risk areas or functions. To clearly distinguish the bank's internal audit function's duties from those of the third party, the bank should have a written agreement, often in the form of an engagement letter.[66]

Refer to the "Outsourced Internal Audit" section of this booklet for more information.

Holding Company or Affiliate Party Services

The bank may also employ services from its holding company or one of its affiliates for audit services. In some cases, the bank chief auditor may be associated with the bank's holding company. When the bank chief auditor has a dual related organizational reporting structure, the bank chief auditor may be an employee of the holding company and the bank. While the ideal arrangement is for the bank chief auditor to be solely a bank employee, it may be acceptable to be a dual employee without hindering independence. Examiners should understand the bank chief auditor's employment status when assessing the audit committee's documentation of the audit organizational risks and mitigations. Refer to the "Audit Committee" section of this booklet for more information.

When using affiliates for audit services, the bank must also comply with additional applicable laws and regulations regarding affiliate services. Affiliate services should be conducted in accordance with safe and sound banking practices. Refer to the "Related Organizations" booklet of the *Comptroller's Handbook* (national banks) and the *Office of Thrift Supervision (OTS) Examination Handbook* section 730, "Related Organizations" (FSAs), for more information on affiliate risk management and transactions. (Updated version 1.1)

Internal Audit Function

The internal audit function is the third line of defense.[67] The internal audit function's primary role is to independently and objectively review and evaluate bank activities. This role helps to maintain and improve the efficiency and effectiveness of the bank's risk management system, internal controls systems,[68] and corporate governance. The internal audit function should monitor the bank's internal controls systems by

[65] Refer to OCC Bulletins 2013-29, 2017-7, and 2017-21. (Footnote updated version 1.1)

[66] Refer to OCC Bulletin 2003-12.

[67] Refer to the "Corporate and Risk Governance" booklet of the *Comptroller's Handbook.*

[68] Per 12 CFR 30, appendix A, II.A, internal control systems include internal controls and information systems.

- evaluating the reliability, adequacy, and effectiveness of internal controls that promote the safety and soundness of the bank, whether operated by the bank or a third party.
- ensuring that bank internal controls result in prompt and accurate recording of transactions and proper safeguarding of assets.
- determining whether the bank complies with laws and regulations and adheres to established bank policies, procedures, and processes.
- determining whether management is taking appropriate and timely steps to address control deficiencies and audit report recommendations.
- ensuring that audit activities are performed by qualified persons.[69]

To conduct these activities effectively, the internal audit function should have ongoing communication with its stakeholders. Internal auditors should be aware of and understand the bank's strategic direction, objectives, products, services, and processes, as well as relevant laws and regulations. The auditors communicate findings to the bank board or its audit committee and senior management. The chief auditor should develop an ongoing communication process with management to keep current on changing business and risk issues.

Internal auditors often have an advisory or consulting role in current or emerging risks at the bank. The advisory role serves the bank's board and management in evaluating safeguards and controls, including appropriate documentation and audit trails of the bank's planning and implementation processes. Refer to the "Advisory and Other Activities" section of this booklet for more information.

The internal audit function should appropriately safeguard information in fulfilling its responsibilities. The sophistication of tools and processes used by internal audit may vary based on the size and complexity of the bank. Auditing work program tools, for example, may store audit supporting documents that contain customer data. Appropriate access and other internal controls should be in place to safeguard information.[70] (Updated version 1.1)

Risk-Based Auditing Program Design

Properly designed risk-based audit programs increase audit efficiency and effectiveness. The sophistication and formality of audit approaches vary depending on the bank's size, complexity, scope and risk of activities, staff capabilities, functional quality of controls, geographic diversity, and use of technology. All risk-based audit programs should do the following:

[69] Refer to 12 CFR 30, appendix A, II.B. For certain larger banks, 12 CFR 30, appendix D, further provides that the board or an appropriate board committee should review and approve a written talent management program for development. Refer to 12 CFR 30, appendix D, II.L, "Talent Management Processes."

[70] The Gramm–Leach–Bliley Act (GLBA) calls for safeguarding in the storing, accessing, and transition of customer information and systems. Refer to 15 USC 6801, "Protection of Nonpublic Personal Information," and 6805, "Enforcement." The "Information Security" booklet of the *Federal Financial Institutions Examination Council (FFIEC) Information Technology (IT) Examination Handbook* provides examiners with procedures on bank information security programs in accordance with GLBA.

- Identify all of the bank's businesses, product lines, services, and functions (i.e., the audit universe). This includes the bank's data, application and operating systems, technology, facilities, and personnel.[71]
- Identify the activities and compliance requirements 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 risk measurement or risk scoring system to rank and evaluate business and control risks of significant business units, departments, and products.
- Include bank board or its audit committee approval of risk assessments, or the aggregate result, 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, and reporting that provide appropriate audit coverage to meet current and emerging risks.
- Establish follow-up activities to effectively review and verify corrective actions and successfully track control deficiencies to successful remediation.
- Include systems or processes, or both, that regularly monitor risk assessments and update them for significant business units, departments, and products.

The bank's policies and procedures govern its internal audit program and elements, supporting a risk-based audit program design. The mission statement or audit charter should outline the purpose, objectives, organization, authorities, and responsibilities of the chief auditor, audit department, audit staff, and audit committee. Refer to the "Board and Management Oversight" section of this booklet for more information. The chief auditor should establish policies and procedures to guide the audit staff. The form and content of these policies and procedures should be consistent with the size and complexity of the department and the bank. Many policies and procedures may be communicated informally in small internal audit departments, while larger internal audit departments normally require more formal and comprehensive written guidance.[72] Policies and procedures in smaller banks may not have the same formality or level of detail as those in larger, more complex banks. Examiners assess both the design and operating effectiveness of the elements of the internal audit program that includes these policies and procedures.

[71] Refer to the "Audit" booklet of the *FFIEC IT Examination Handbook.*

[72] OCC Bulletin 2003-12 relates effective internal audit policies and procedures to a competent internal audit function with sufficient expertise and resources to identify the risks inherent in the bank's operations and assess whether internal controls are effective. Refer also to 12 CFR 30, appendix D, II.C, "Roles and Responsibilities." (Footnote updated version 1.1)

Audit Risk Assessment Methodology

The audit risk assessment is a key element in the achievement of the bank's objectives to determine how risks should be managed. The audit risk assessment assists the auditor in understanding the bank, the environment, and the industry in which the bank operates. To determine the appropriate level of audit coverage for the bank, the internal audit function should define an effective audit risk assessment methodology. The methodology should provide the chief auditor and bank board and its audit committee with objective information to properly prioritize the allocation of audit resources. The methodology should include an analysis of individual cross-bank risks and thematic control issues and address the bank's processes and procedures for evaluating the effectiveness of risk management, control, and governance processes. The methodology also should address the role of continuous auditing in determining and evaluating risks, as well as an internal audit process for incorporating other risk identification techniques that the bank's management uses, such as a risk and control self-assessment. The components of an effective methodology should support the internal audit function's assessment of the control environment, beginning with an evaluation of the audit universe.

Audit Universe

The audit universe should represent the bank's auditable entities. Internal audit should have effective processes to identify all auditable entities (e.g., an entity, operation, function, process, or system) within the audit universe. The bank should maintain profiles of significant business units, departments, and products. The number of auditable entities depends on whether entities are captured at individual department levels or at other aggregate organizational levels. Examiners should gain an understanding of any aggregation to properly assess whether the audit universe meets this risk-based audit program element. For certain large banks covered under the OCC's heightened standards, the internal audit function should prepare and maintain a complete and current inventory of all of the bank's material processes, product lines, services, and functions.[73] To address the specific nature of information systems, banks typically create a secondary audit universe for information technology (IT). The bank's IT audit universe should contain an inventory of the bank's data, application and operating systems, technology, facilities, and personnel.[74]

Internal audit should use its knowledge of the bank to determine whether it has identified all current auditable entities. Internal audit may use the general ledger, cost centers, new product approval processes, organization charts, department listings, knowledge of the bank's products and services, major operating and application systems, significant laws and regulations, and other data. Other bank risk assessments, such as the information security risk assessment and risk control self-assessments, can help internal audit in establishing and maintaining its audit universe. Refer to the "Non-Internal Audit Assurance Activities" section of this booklet for more information.

[73] Refer to 12 CFR 30, appendix D, II.C.

[74] Refer to the "Risk Assessment and Risk-Based Auditing" section in the "Audit" booklet of the *FFIEC IT Examination Handbook.*

The audit universe should be documented and reviewed periodically as significant changes occur, or at least during the annual audit planning process.

Audit Risk Assessment

A comprehensive risk assessment should effectively analyze the key risks (and critical risk management functions) for the bank and prioritize auditable entities within the audit universe.

An audit risk assessment should document a bank's significant business activities and associated risks. The chief auditor takes into account the bank's risk management framework, including any established risk appetite levels set by management for the different activities or parts of the organization.[75] The internal audit function can leverage risk assessments conducted by other areas of the bank in establishing and maintaining its overall audit risk assessment. When doing so, the internal audit function should apply independent judgment. For banks covered under 12 CFR 30, appendix D, internal audit is expected to identify and communicate to the audit committee significant instances where frontline units or independent risk management are not adhering to the bank's risk governance framework. Examiners should gain an understanding of the most recent audit results for any leveraged risk assessments. If the bank risk framework does not exist, the chief auditor uses his or her own judgment of risks after consultation with senior management and the bank board or its audit committee.

Major risk factors commonly used in the audit risk assessment are the following:

- Nature and scope of the businesses, product lines, services, and functions relative to the bank and banking industry.
- Nature of transactions (e.g., volume, size, liquidity, and geographic diversity).
- Nature of the operating environment (e.g., technology, compliance with laws and regulations, complexity of transactions, changes in volume, degree of system and reporting centralization, and economic and regulatory environment).
- Nature of reasonable and foreseeable internal or external threats.
- Nature and scope of third-party services and products employed.
- Human resources (e.g., experience of management and staff, turnover, competence, and degree of delegation).
- Nature and strength of internal controls and information systems (e.g., security, MIS, and manual or automated controls).
- Degree and level of governance and oversight by senior management.
- Timing, scope, and results of internal audit assurance of the auditable entity.
- Probable impact and likelihood of a threat event occurring.

Auditors or risk managers should develop written guidelines on the use of risk assessment tools and risk factors and review the guidelines with the board risk committee or audit

[75] Refer to 12 CFR 30, appendix D, II.E, "Risk Appetite Statement," which provides guidelines for certain large banks regarding risk appetite statements.

committee. The sophistication and formality of guidelines varies depending on bank size, complexity, scope of activities, geographic diversity, and technology used. Auditors use the guidelines to grade or assess major risk areas, along with risk themes. The written guidelines should specify the following:

- **Length of the audit cycles:** This guideline is based on the scores or assessments. Audit cycles should be defined and should provide appropriate audit coverage of all auditable entities. For example, some banks follow a four-year audit cycle, with high-risk areas audited every 12 months and low-risk areas every 48 months. Refer to the "Audit Cycles" section of this booklet for more information. (Updated version 1.1)
- **Risk-scoring methodology:** These guidelines define the processes along with the risk scoring and measurements. The risk-scoring methodology defines the basis for assigning risk grades, risk weights, or risk scores (for example, the basis could be normal industry practices or the bank's own experiences). The methodology guidelines also define the range of scores or assessments (for example, low, medium, and high or a numerical sequence such as 1 through 5).
- **Risk assessments overrides:** The guidelines should specify who can override the assessments, the approval process for such overrides, and the reporting process for overrides. The override process should involve the bank 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 and tracked appropriately.
- **Timing of audit risk assessments for each department or activity:** The audit risk assessment, as a whole, is updated as part of internal audit's annual planning. The audit risk assessment should be a dynamic tool for the internal audit function, with periodic updates to reflect changes in the bank's risk profile, key staff, technology, products, services, functions, or activities, along with industry or regulatory changes. Internal auditors should consider reviewing and updating the applicable portion of the audit risk assessment in audits.
- **Thematic control issues:** The guidelines should address the identification of thematic control issues and the determination of the overall impact of such issues on the bank's risk profile.
- **Minimum documentation requirements:** These requirements pertain to documentation required to support development and maintenance of the audit risk assessment, which includes written analysis scoring or assessment decisions.

These assessments typically analyze the risks inherent in a given business line or process, the mitigating control processes, and the resulting residual risk exposure to the bank. The risk measurement or scoring system should be understandable, consider all relevant risk factors, and avoid subjectivity.[76] (Updated version 1.1)

Banks can obtain matrixes, models, or additional information on risk assessments from industry groups such as the American Bankers Association, the American Institute of Certified Public Accountants (AICPA), the IIA, the Financial Managers Society, and many

[76] Refer to the "Audit" booklet of the *FFIEC IT Examination Handbook* for information on risk scoring.

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).

Overall Audit Plan

Internal audit should establish and adhere to an audit plan that is periodically reviewed and updated; takes into account the bank's risk profile, emerging risks, and issues; and establishes the frequency with which activities should be audited.[77] An effective audit risk assessment methodology provides the auditor and the board with objective information to prioritize the allocation of audit resources properly. When the audit risk assessment indicates a change in risk, the audit plans should be reviewed to determine if planned audit coverage should be changed.

Audit Coverage

The audit plan should enable appropriate audit coverage of bank entities and activities. The internal audit plan should consider the audit risk assessments and internal audit's plan strategy. Internal audit coverage should reflect the identification of thematic control issues across the bank's auditable entities. An effective plan covers individual business areas and risk disciplines as well as cross-functional areas. The audit plan should require internal audit to evaluate the adequacy of and compliance with policies, procedures, and processes established by frontline units and independent risk management under the risk governance framework.[78] (Updated version 1.1)

The audit plan details budgeting and planning processes and should describe audit goals, schedules, staffing, and reporting. Audit plans usually include the following:

- Overall and individual audit scope and objectives.
- Summary of audit risk assessments that provides a summary for each auditable entity and related control issues.
- Timing and frequency of planned internal audit work.
- Staff assignments by audit (number, hours, outsourcer, auditor title).
- Resource budget (including outsourced or co-sourced activities).
- Anticipated timing and scope of relevant non-internal audit assurance coverage, such as a service organization control (SOC) audit to attest controls at a third-party servicer.

[77] Refer to the "Corporate and Risk Governance" booklet of the *Comptroller's Handbook* for information on risk governance and a bank's risk appetite.

[78] For banks covered under 12 CFR 30, appendix D, II.C.3, "Role and Responsibilities of Internal Audit," the audit plan should require internal audit to evaluate the adequacy of and compliance with policies, procedures, and processes established by frontline units and independent risk management under the risk governance framework.

The audit plan can be a multi-year approach, with the audit plan revised annually, or an approach that uses the audit risk framework to evaluate risks annually, focusing on the most significant risk. When using this latter approach, there should be a process to identify when a significant risk will not be audited in the specified time frame and to notify the audit committee and seek approval of any exceptions.

Audit Plan Changes

The audit planning process should be dynamic, allowing for change when necessary. The process should provide for modification of the internal audit plan to incorporate significant changes that are identified either through continuous monitoring or during an audit. The chief auditor should review and adjust the plan, as necessary, in response to changes in the bank's risks, operations, programs, systems, and controls.

The audit committee should formally approve the audit plan at least annually and be aware of significant changes. The internal auditor should present any updated audit plan or audit schedule, or both, to the audit committee regularly, typically quarterly, in accordance with established policy. Updated audit plans should compare actual work performed with planned audits and audit hours and explain significant variances from the approved plan. Any significant changes in the plan should be clearly documented and included in quarterly communication to the audit committee. Critical data to be reported to the audit committee should include deferred or cancelled audits for high-risk entities and other significant changes.

Audit Plan Staffing

The audit program should be supported by qualified staff.[79] The chief auditor should ensure that qualified and independent auditors are assigned to execute the audit plan. Audit activities, including various audit types, can be performed by a single auditor or team of auditors. The chief auditor should assign internal audit staff according to the expertise and skills needed to execute a particular audit. Some banks may demonstrate this correlation by denoting auditor job titles, such as IT auditor, or names of individuals assigned within the audit plan. In considering the qualifications of the internal audit staff assigned to a given audit, the chief auditor should look at the skills and expertise of the team collectively. Often, the lead auditor retains the required skills and is able to provide direction and oversight of other auditors. Internal audit position titles may include requirements for education, professional certifications, and work experience levels that help to demonstrate qualifications. Refer to the "Internal Audit Independence" section of this booklet for more information.

Audit Cycles

An audit cycle identifies the frequency of audits. Audit cycles generally fall into monthly time frames (e.g., 12, 18, 24, 36, or 48 months) and are approved in advance by the bank's audit committee. Audit cycles are usually driven by the risk scores of the business activities

[79] Refer to 12 CFR 30, appendix A, II.B.3.

or areas in the audit risk assessment. The audit risk assessment process identifies both an inherent risk score and a residual risk score to each auditable entity. The residual risk score is most commonly used in assigning the audit cycle, taking into account mitigating controls. There are instances, however, when the inherent risk score should be used, specifically when the reliability of the internal audit program or the audit risk assessment process has come into question. It is often not practical to audit each area or business activity annually. In general, auditable entities with higher risk scores are assigned a shorter audit frequency. Areas of high risk, such as information security, funding, lending, or investment/treasury operations, normally warrant more frequent audits than low-risk areas such as bank premises. Regardless of the risk levels, the assigned audit cycle should ensure compliance with any regulatory or supervisory timing requirements.

Audit Work Programs

Audit work programs are sets of procedures used by auditors in performing assurance activities. Audit work programs may include automated processes used by auditors in performing assurance activities and are generally housed within a technology-based tool. 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. Audit work programs help to ensure consistency in conducting audits. Work programs should 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 typically include procedures for the following:

- 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 or ledgers related to general ledger or control records.
  - examination of supporting documentation.
  - direct confirmation and appropriate follow-up for exceptions.
  - physical inspection.
- Surprise audits as appropriate.
- Control over records selected for an audit.

Audit work programs are a key element of the internal audit program. The chief auditor should ensure that the audit work programs are properly maintained and that controls are in place for integrity, confidentiality, and availability of work programs.

Control Testing

Control testing is meant to determine the design appropriateness or operating effectiveness of a given control or set of controls. A control can be a manual process (such as a signature for

wire transfers) or automated (for example, an employee logging onto the bank's general ledger).[80] Controls are generally positioned to prevent, correct, or detect errors and omissions. Control testing can range from a discussion with bank management to using computer-assisted auditing techniques or computer-aided audit tools (CAAT) to verify general ledger transactions. While all types of control tests offer value in providing assurance of the control, the rigor of control testing techniques should align with the risk of the auditable entity or activity being tested.

The chief auditor should ensure that the control testing approach employed in the bank's audit plan provides the appropriate level of assurance. The control testing approach for a given auditable entity or activity may represent a single or aggregate testing of the controls. The chief auditor should take into consideration non-internal audit assurances when determining the appropriateness of control testing.

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 (for example, all items in a group or a sample of items).

When auditors choose to review a sample, they decide whether to use statistical or non-statistical sampling methods. In general, non-statistical sampling should be used only in areas of lower risk or where the process is stable and the internal controls in the area are effective. In smaller banks, non-statistical sampling may be used when 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 specific 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 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.

[80] Refer to the "Internal Control" booklet of the *Comptroller's Handbook* (national banks) and *OTS Examination Handbook* section 340, "Internal Control" (FSAs). (Footnote updated version 1.1)

- evaluating sample results and findings.[81]

Assessing Deficiencies by Internal Audit

The internal auditor should evaluate control deficiencies identified during an audit to determine the risk severity of the deficiencies, whether individually or in combination. Deficiencies can exist in the design of an internal control or in the operating effectiveness of a control. Auditors should assess each control deficiency that comes to their attention, including deficiencies that are self-identified by bank management. Refer to the "Non-Internal Audit Assurance Activities" section of this booklet for more information. The internal auditor should perform root cause analysis that consists of methods used to identify underlying cases of control deficiencies and also assist in the identification of thematic control issues. The internal auditor should apply the bank's approved risk-scoring methodology when assigning the risk severity.

Internal audit policy and its risk-scoring methodology should ensure that control deficiency assessments are consistent and repeatable.

Internal Audit Continuous Auditing

Internal audit is encouraged to use formal continuous auditing practices as part of the function's risk assessment processes to support adjustments to the audit plan or universe as they occur. Continuous auditing can be conducted by an assigned group or by individual internal auditors. Continuous auditing usually uses IT-related tools to monitor processes, transactions, and accounts to enhance efficiency and effectiveness of internal audit efforts.

Continuous auditing results should be documented through a combination of metrics, management reporting, periodic audit summaries, and updated risk assessments to substantiate that the process is operating as designed. Critical issues identified through the auditing process should be communicated to the audit committee. CAATs may assist in searching for irregularities in data files or extrapolating large amounts of data for further analysis. CAATs simplify or automate the data analysis process and help auditors to highlight issues that warrant further consideration within a continuous auditing process.

Internal audit policy and standards should ensure continuous auditing activities are effective, consistent, and repeatable.

[81] Refer to the "Sampling Methodologies" booklet of the *Comptroller's Handbook* (national banks) and the *OTS Examination Handbook* section 209, "Sampling." (FSAs). Also refer to manuals and guidance from auditing industry sources, including accounting firms, the IIA, the Bank Administration Institute, and others.

Non-Internal Audit Assurance Activities

Non-internal audit assurance activities performed for auditable entities in the bank's audit universe can vary by bank. Assurance reports may be obtained by those performing services for the bank, such as an outside third party, the bank's holding company, or another affiliate of the holding company. Within the bank, non-internal audit assurance activities can be categorized as a first line of defense activity or a second line of defense activity. Non-internal audit assurance reports can help to minimize duplication of work and disruption to operations, provide audit coverage, and conserve resources for high-risk processes.

Many service providers have established a means to provide assurance to their clients of the design or operational effectiveness of their controls. The scope and objective of these audits are determined by the service provider, but most follow the industry-accepted standard for reporting. Some of the most common assurance reports include the Service Organization Control (SOC) reports, (type 1 and type 2), International Standard on Assurance Engagements (ISAE) No. 3402, and payment card industry reports. Banks covered under SOX, for example, usually do not accept SOC type 1 reports because these reports do not test control operating effectiveness. Refer to appendix B, "Types of Audits and Control Reviews," of this booklet for more information on service provider audits. (Updated version 1.1)

The holding company of the bank and its affiliates' audit programs generate audit reports in fulfillment of the responsibilities of their respective boards of directors. When the bank employs one of these legal entities for products or services, these audits may pertain to auditable entities that are part of the bank's audit universe. Examiners should be aware that the report content, including overall rating, is governed by the internal audit function conducting the audit and may not reflect the bank's risk perspective.

Other bank assurance activities may be performed by bank organizational units outside of internal audit. Some banks rely on so-called "management self-assessments, or "control self-assessments," in which bank business line managers and their staff evaluate the performance of internal controls within their purview. Such reviews help to underscore management's responsibility for internal control, but they are not independent. Directors and senior management who rely too much on these reviews may not learn of control weaknesses until those weaknesses have become costly problems, particularly if directors are not intimately familiar with the bank's operations. Therefore, banks generally should also have their internal controls tested and evaluated by units without business-line responsibilities, such as internal audit groups.[82] The second line of defense activities often encompass assurance activities performed independently of the control owner. For example, the OCC's heightened standards for certain large banks define the independent risk management unit as independent from the frontline unit and as having the responsibility to identify, measure, monitor, or control aggregate risks.[83]

[82] Refer to OCC Bulletin 2003-12.

[83] Refer to 12 CFR 30, appendix D, I.E.

The chief auditor should establish policies and procedures for non-internal audit assurance reports as they apply to the bank's internal audit program. Guidance should include, but is not limited to, assurance report evaluations, obtaining or requesting additional support information, control issue follow-up, and internal audit reporting. Internal audit should consider not only the scope and objective of the non-internal audit assurance report but also its source, the type of control testing, and the sampling methods employed.

Internal Audit Reports

Audit reports should inform the bank board audit committee and senior bank management whether a department, division, or activity adheres to policies, procedures, and applicable laws or regulations; whether operating processes, internal control systems, and risk management activities are effective; and what corrective action the bank has taken or must take for new or outstanding issues. The internal audit report is seen as a key written communication to the bank board or its audit committee. For certain large banks, the internal audit report should reflect an assessment of risk management activities conducted by the frontline units and the independent risk management function to identify and resolve issues in a timely manner.[84] The report should also address potential and emerging concerns. The auditor should 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, individual internal audit reports and executive summaries of an audit.

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

- A concise summary of key results and conclusions, including an overall assigned audit rating and identification of root causes of significant weaknesses.
- The audit's scope and objectives.
- Detailed audit results.
- 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 the following:

- Established criteria.
- Existing problems.
- The root cause of any noted problem.
- Existing or potential problem impact.
- Recommendations for correcting the problem.

[84] Refer to 12 CFR 30, appendix D, II.C.3.

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 possibly reach agreement on management's commitments and actions. A final audit report is then distributed to the affected business area management, senior management, and the audit committee within an appropriate time after the completion of fieldwork. Compliance with issuance time frames should be monitored and reported to the audit committee. Internal audit should ensure that management considers the level and significance of risk when assigning resources to address and remediate issues. Management should appropriately document the action plans either within the audit report or separately.

Executive summaries of audits provide more concise briefings of the individual audit. Refer to the "Board and Audit Committee Reports" section in this booklet for information on board-level or audit committee-level internal audit function reports.

Follow-Up Activities

Follow-up activities should allow internal auditors to determine the disposition of any agreed-on actions and provide information for future audit activities. The auditors should perform follow-up activities promptly and report the results to the bank board or its audit committee. Follow-up generally consists of first obtaining and reviewing management's response and then confirming that remediation action has been timely and effective.

Internal Audit Issues Tracking

Internal audit should have effective processes to track, monitor, and follow up on open audit issues. Audit issues include those control issues identified in audits performed as part of the internal audit plan, which may include those identified in non-internal audit assurance reports. The timely remediation of open audit issues is an essential component of an organization's risk reduction efforts. Internal audit and the responsible bank management should discuss and agree to an appropriate resolution date, based on the level of work necessary to complete remediation processes. All audit issues should be assigned an individual owner with an appropriate level of accountability in the bank. This ownership is typically assigned during the bank's audit but may be assigned later in the case of audit's review of a non-internal audit assurance report. When an issue owner indicates that work to address the issue is completed, the internal audit function should perform validation work before considering the issue closed. Therefore, audit issue status reporting should make a distinction between an issue considered closed by bank management and one closed by internal audit. The level of validation necessary may vary based on the issue's risk level. For higher-risk issues, internal audit should perform and document substantive testing to validate that the issue has been appropriately remediated. Associated internal controls testing should be conducted over an appropriate period of time and should confirm the sustainability, or operational effectiveness, of the remediation. Approaches to validating issue remediation may vary, from incorporation at the next audit of the auditable entity, to a specific audit to validate multiple issues. The bank's approach to validating issue remediation should be clearly defined in its policies and procedures to promote consistency. (Updated version 1.1)

Internal audit's issue status reporting to the bank board or its audit committee should provide a clear picture of management and internal audit function efforts. The audit issue status report should also include any changes in issue ownership, target remediation dates, remediation plans, or repeat audit issues. Multiple changes and repeat audit issues should trigger additional root cause analysis of management's ability and willingness to correct deficiencies and manage risks.

Quality Assurance and Improvement Programs

The chief auditor should develop and maintain a quality assurance and improvement program that covers all aspects of the internal audit activity.[85] In such programs, internal and external parties periodically assess the performance of the internal audit activities in conforming to applicable policies, laws, regulations, and industry standards and in operating effectively and efficiently. Such programs should also identify opportunities for improvement. The internal audit function's quality assurance and improvement program contributes to the bank's external auditor planning when considering the use of internal audit work. Refer to the "External Audit Function" section of this booklet for more information.

Measurements of performance and risks, also known as key performance indicators and key risk indicators, should be well defined. The auditor's or audit department's performance is normally measured against bank-established standards, the internal audit charter or mission statement, and any other criteria determined appropriate for the internal audit function.

The chief auditor should report results and status of internal assessments to senior management and the audit committee at least annually. The chief auditor should formulate recommendations or actions taken to address deviations from policies. Such actions might include retraining of staff or adjustments to policies.

Generally, large and midsize banks are more likely to have a designated quality assurance and improvement function or unit.

Internal Assessment

Internal assessments take the form of ongoing monitoring of day-to-day audit activities, as well as periodic self-assessments. Internal assessments should be conducted by an individual or team that has clear segregation of duties from the activity being assessed. Internal assessments are often part of the operational activities of the internal audit function. Ongoing monitoring, such as supervision of auditors during an engagement or final review of an audit report, may also enhance the training of auditors. Periodic internal assessments can also be integrated into the internal audit program activities such as the periodic review of the audit risk assessment. The OCC encourages banks to map internal assessments against the internal

[85] IIA, *International Standards for the Professional Practice of Internal Auditing*, nos. 1310–1322, calls for both internal and external quality assurance reviews. The latter is to be conducted every five years. Refer to the IIA's website. Banks subject to 12 CFR 30, appendix D, should refer to appendix D, II.C.3 for quality assurance program guidelines.

audit activities to minimize redundancies and gaps, along with their incorporation of staff development planning.

External Assessment

An external assessment of key internal audit activities should be conducted periodically to provide assurance to the bank board of the design and operational effectiveness of internal audit activities in managing risks.[86] These external assessments can be in the form of a full external assessment or a self-assessment with independent external validation. External assessments of internal audit may also provide valuable information in making strategic decisions relating to establishing, enhancing, and outsourcing (or co-sourcing) of internal audit.

Banks should be careful to engage a qualified, independent assessor or assessment team from outside the organization. Experience in professional practices of internal audit and the external assessment process demonstrates qualifications. Banks may be better served by assessors with experience gained in banks of similar size and complexity. Lack of independence results when the assessor or assessment team is part of, or under the control of, an organization that performs internal audit activities, in full or part, for the bank. Conflicts of interest, or the appearance of such conflicts, compromise independence. Banks should avoid employing a third party to perform an assessment of internal audit where the third party may have real or apparent conflicts of interest or may benefit inappropriately by performing such assessments.

Internal Audit Independence

(Section updated version 1.1)

An independent internal audit function, along with an effective system of internal controls, forms the foundation for safe and sound operations, regardless of a bank's size.[87] Internal auditors must be independent of the activities they audit so that they can carry out their work freely and objectively.[88] The OCC expects internal auditors to render impartial and unbiased judgments.[89] The internal audit function should not be involved in designing, selecting, implementing, or operating specific internal control measures. The chief auditor should report directly and regularly to the bank board or its audit committee. The bank board should

[86] According to section 404 of SOX, title IV, covered banks must report on the effectiveness of internal control structure and procedures for financial reporting, which may include those executed by the internal audit function.

[87] Refer to OCC Bulletin 2003-12.

[88] Refer to 12 CFR 30, appendix A, II.B.3. Also refer to 12 CFR 30, appendix D, I.E.8, for large banks covered by the OCC's heightened standards. Specific independence considerations may also come into play when the bank's external audit function intends to utilize internal audit function work. Refer to the "Use of Internal Audit Work" section of this booklet for further information.

[89] Refer to OCC Bulletin 2003-12.

take extra measures to ensure that the internal audit function's reporting relationships do not impair the auditor's independence or unduly influence the auditor's work. Refer to the "Board and Management Oversight" section of this booklet for more information. Internal audit function independence should also be managed at the individual auditor or audit activity level with appropriate written guidance.[90] At most banks, audit policies restrict internal audit staff from performing audit activities in the auditor's previous employment areas for a set period and require a review or repeat of audit work, or both, for areas to which an internal auditor moved after the audit. Refer to the "Advisory and Other Activities" section of this booklet for other independence considerations.

The OCC expects the bank board to delegate the authority necessary to effectively allow internal auditors to perform their jobs. Auditors should 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 among the bank board, internal auditors, and bank management is critical to timely identification and correction of weaknesses in internal controls and operations.

Internal Audit Competence

The audit program must be staffed by qualified persons.[91] To accomplish this objective, the chief auditor should recruit, retain, and develop internal audit staff. Based on the bank's internal audit needs, the chief auditor should have a clear understanding of the staffing skills needed and those possessed by the internal audit staff. A skills assessment of internal audit staff against these needs helps to identify skill gaps. The chief auditor should document a plan to address short- and long-term staffing needs and communicate such plans to the audit committee as part of the audit plan.[92] (Updated version 1.1)

Internal audit staff should have 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. Members of the audit staff should

- have appropriate education or experience.
- have organizational and technical skills commensurate with the responsibilities assigned.
- be skilled in oral and written communication.
- understand accounting and auditing standards, principles, and techniques.

[90] Refer to BCBS, "The Internal Audit Function in Banks," for guidance on the value of staff rotations within the internal audit function and staff rotations to and from the internal audit function.

[91] Refer to 12 CFR 30, appendix A, II.B.3. Also refer to 12 CFR 30, appendix D, II.C.3(g), for large banks covered by the OCC's heightened standards.

[92] Under the OCC's heightened standards for certain large banks, the board or appropriate board committee should review and approve a written talent management program that provides for development, recruitment, and succession planning regarding the chief audit executive, his or her direct reports, and other potential successors. Refer to 12 CFR 30, appendix D, II.L., "Talent Management Processes."

- 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 chief auditor, 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 the bank, and reviewing current literature on auditing and banking are also means to maintain and enhance auditing skills.

At a small bank, internal auditing may be a one-person department. Nevertheless, the auditor should possess qualifications similar to those mentioned in this section of this booklet.

Professional development programs assist internal audit in satisfying its obligation to ensure that staff is qualified to meet the bank's internal audit needs.[93] The chief auditor should establish individual goals with internal audit staff and keep a record of training. 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 and professional societies). Auditors should be aware of emerging risks related to the banking industry and relevant banking products and services. When the bank co-sources with a third party to obtain subject matter expertise, knowledge should be transferred to current internal audit staff.

Advisory and Other Activities

Internal auditors are increasingly responsible for playing a more proactive role in supporting the bank's overall risk management. The bank board and its audit committee expect internal auditors to provide some degree of risk management analysis or recommendations. The internal audit function should execute this role during a bank's merger, acquisition, corporate reorganizations, and transition activities, as well as in due diligence of critical third-party relationships.[94] Internal auditors 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. To ensure that appropriate independence and objectivity are maintained, however, internal auditors should not approve, design, or implement any operating policies or procedures resulting from or related to their advisory or consulting activities. Internal auditors should not become involved in valuation activities or other management functions.

[93] Refer to 12 CFR 30, appendix A. II.B.

[94] Refer to OCC Bulletins 2013-29, 2017-7, 2017-21, and 2017-43. (Footnote updated version 1.1)

The audit committee, in its oversight of the internal audit staff,[95] should ensure that the function's consulting activities do not interfere or conflict with the objectivity it should have with respect to monitoring the bank's system of internal control. Bank management should make decisions to adopt or implement recommendations resulting from internal audit advisory or consulting services. The OCC encourages internal auditors to follow industry best practices, such as the IIA standards and guidance, related to performing non-assurance services.[96]

Retrospective Reviews

When an adverse event occurs at a bank (for example, fraud or significant loss), management should conduct a post mortem and "lessons learned" analysis. During an adverse event, internal audit should ensure that such a review takes place and remediation actions address identified issues. The internal audit function should evaluate bank management's analysis of the reasons for the adverse event and whether the event was the result of a control breakdown or failure. The internal audit function should identify the measures that should be put in place to prevent a similar event from occurring in the future. In certain situations, the internal audit function should conduct its own post-mortem review and a "lessons learned" analysis outlining the remediation procedures necessary to detect, correct, or prevent future internal control breakdowns.

Preparedness Reviews

Preparedness reviews provide the bank board and senior management with an indication of the bank's readiness for changes, such as new, expanded, or modified products or services; emerging technologies; changes to systems; new or revised regulatory guidance, laws, and regulations; and areas of strong growth. Reviews should come with an opinion about the bank's ability to accomplish these changes, manage associated risks, and achieve desired results.

Look-Back Reviews

Look-back reviews serve to provide the bank board with insight into why critical weaknesses were not appropriately identified by the first, second, and third lines of defense so they can make adjustments to remedy potential weaknesses. Each line of defense should perform an independent review. Internal audit function's failure to identify or properly report weaknesses, for example, may be an indication of inadequate audit coverage, lack of independence or stature of the internal audit function, or simply a result of timing. (Updated version 1.1)

[95] Internal audit staff refers to in-house and outsourced or co-sourced internal audit personnel.

[96] Refer to the IIA's "Principles Guiding the Performance of Consulting Activities of Internal Auditors."

Outsourced Internal Audit

Many banks use independent accounting firms or 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 co-sourcing," or "extended audit services" (collectively, outsourcing).

Managing Outsourcing Risks

As with managing other third-party servicers, the bank board and management should exercise appropriate due diligence before entering a third-party relationship and should implement effective oversight and controls afterward. This due diligence may include the following elements:

- Plans that outline the bank's strategy, identify the inherent risks of the activity, and detail how the bank selects, assesses, and oversees the third party.
- Proper due diligence in selecting a third party.
- Written contracts or agreements that outline the rights and responsibilities of all parties.
- Ongoing monitoring of the third party's activities and performance.
- Clear roles and responsibilities for overseeing and managing the relationship and risk management process.
- Documentation and reporting that facilitate oversight, accountability, monitoring, and risk management.
- Independent reviews that allow bank management to determine that the bank's process aligns with its strategy and effectively manages risks.[97]
- Contingency plans for terminating the relationship in an effective manner.

As mentioned in the "Board and Management Oversight" section of this booklet, outsourcing arrangements should be documented in written agreements. When negotiating the outsourcing arrangement, the bank board and management should carefully consider the bank's current and anticipated business risks in setting each third party's internal audit responsibilities. The outsourcing arrangement should not increase the risk that a breakdown of an internal control will go undetected. When establishing written criteria for evaluating performance of the chief auditor and internal audit function, the audit committee should address effective management of audit outsourcing risks.

[97] The bank board or its audit committee should include in its evaluation of the chief auditor and internal audit function those risk management activities related to any third-party audit services. Refer to the "Board and Management Oversight" section of this booklet.

Written Contracts and Agreements

All banks engaged in outsourcing or co-sourcing of internal audit activities should execute a written contract or agreement governing the terms of the outsourcing arrangement and specifying the roles and responsibilities of both the bank and the third party.[98] The contract should do the following:

- Define the expectations and responsibilities for both parties under the contract.
- Set the scope, frequency, and cost of the third party's work.
- Describe responsibilities for providing and receiving information, such as the type and frequency of the third party's reporting to the bank's chief auditor, senior management, and board or audit committee. This information should include the status of the contracted work.
- 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.
- State that any information pertaining to the bank must be kept confidential, including information accessed, transmitted, or stored.
- Stipulate that the internal audit reports are the property of the bank and specify ownership of associated work papers. If the third party retains ownership of work papers, the contract should stipulate that the bank can get copies of the third party's work papers it deems necessary and that employees authorized by the bank must have reasonable and timely access to third-party work papers.
- State where internal audit reports and related work papers will be stored, and specify retention requirements (e.g., retain for seven years). Give consideration to third-party maintenance of any proprietary software necessary to access records by banks and examiners, as well as a data destruction plan for when the retention period expires.
- Note that the third party's internal audit outsourcing activities are subject to regulatory review and that OCC 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 third party 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.
- State notification responsibilities to the bank in the occurrence of a security breach.
- State the third party's obligation to comply with applicable bank policies and procedures.

[98] OCC Bulletin 2003-12 outlines 10 elements that should be included in all outsourcing contracts. OCC Bulletin 2013-29 outlines the need for proper notification for both security breaches and subcontracting consideration. Refer also to OCC Bulletin 2017-7 and OCC Bulletin 2017-21 for more information. (Footnote updated version 1.1)

- If applicable, state that the third party must comply with AICPA, Public Company Accounting Oversight Board (PCAOB), SEC, or regulatory independence standards.[99] (Updated version 1.1)

Quality of Audit Work

The quality of audit work performed by the third party should be consistent with the bank's standards of work expected to be performed by an in-house internal audit function. Further information supplied by the third party should provide the bank board, its audit committee, and senior management with an accurate report on the control environment, including any changes necessary to enhance controls.

External Audit Function

An external audit program provides the bank board with information about the bank's financial reporting risk areas, e.g., the bank's internal controls over financial reporting, the accuracy of its recording of transactions, and the completeness of its financial reports prepared in accordance with applicable accounting standards. Through its external audit program the bank board or its audit committee engages an independent auditor or audit firm, commonly known as the "external auditor," for planning and execution of the external audit plan. In this capacity, the external auditor may also be referred to as the IPA. Third-party auditors or audit servicers engaged as part of the internal audit function are not considered external auditors. Refer to the "Outsourced Internal Audit" section of this booklet for more information.

The goal of an effective external audit function should be to provide the bank board and management with

- reasonable assurance that the financial statements present fairly, in all material respects, the financial position of the bank in conformity with generally accepted accounting principles (GAAP), and, as applicable, that internal controls over financial reporting are operating effectively.
- an independent and objective view of the bank's financial statements, and, as applicable, the bank's processes related to financial reporting.
- timely oral and written communications that are useful to directors and management in maintaining the bank's risk management processes.

[99] IPAs for banks with securities registered with the OCC must follow the SEC's independence rules regarding prohibited non-audit services (including internal audit outsourcing services). For banks subject to 12 CFR 363, the IPA must comply with the independence standards and interpretations of the AICPA, the SEC, and the PCAOB. To the extent that any of the rules within any one of these independence standards (AICPA, SEC, and PCAOB) is more or less restrictive than the corresponding rule in the other independence standards, the IPA must comply with the more restrictive rule. Refer to 12 CFR 363.3(f), "Independence."

External Audit Plan

The bank board or its audit committee should agree in advance with the external auditor on the objectives and scope of the external audit plan. The bank board or its audit committee at least annually should review the risks inherent in its particular activities to determine the scope of its external audit program. For most banks, the lending and investment securities activities present the most significant risks that affect financial reporting. Thus, the external audit program should include specific procedures designed to test at least annually the risks associated with the loan and investment portfolios. This includes testing of internal control over financial reporting, such as management's process to determine the adequacy of the allowance for loan and lease losses and whether this process is based on a comprehensive, adequately documented, and consistently applied analysis of the bank's loan and lease portfolio.

The bank or its subsidiaries may have other significant financial reporting risk areas, such as material real estate investments, insurance underwriting or sales activities, securities broker-dealer or similar activities (including securities underwriting and investment advisory services), loan servicing activities, or fiduciary activities. The external audit plan should address these and other activities the bank board or its audit committee determines present significant financial reporting risks to the bank.

Refer also the "Fieldwork Standards" and "Special Situations" sections of this booklet for further external audit plan considerations.

Types of External Auditing Programs

When the bank board and management analyze the bank's external auditing needs, they should decide which type of external audit(s) best fit the bank's needs. The FFIECs members recognize that some banks only have agreed-upon procedures or state-required examinations, or both, performed annually as their external audit program.[100]

- **Financial statement audit by an IPA:** External auditing is traditionally associated with independent audits of the bank's financial statements. An independent audit of financial statements is designed to provide reasonable assurance that financial reports are presented fairly, in all material respects, in conformity with GAAP. Independent financial statement audits are performed in accordance with the applicable auditing standards.[101] The scope of these audits is sufficient to enable an IPA to express an opinion on the bank's (or parent holding company's consolidated) financial statements, but does not provide an opinion on the effectiveness of internal controls. Banks with $500 million or

[100] Refer to OCC Bulletin 1999-37.

[101] Audits of publicly traded companies are conducted in accordance with the standards of the PCAOB. Audits of the financial statements of those non-publicly traded banks are to be conducted in accordance with generally accepted auditing standards (GAAS) as issued by the Auditing Standards Board (ASB), a senior committee of the AICPA. Audits of FBOs may be performed in accordance with international standards on auditing.

more in total assets are required by 12 CFR 363 to have an IPA audit their financial statements.[102] The OCC encourages the boards of all other banks to voluntarily engage the services of IPAs to conduct audits of their financial statements.

- **Reporting by an IPA on the 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 over financial reporting. The IPA must use an industry-accepted internal control framework that is identical to the one identified in the management report.[103] 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. Banks with $1 billion or more in total assets at the beginning of the banks' fiscal year are required by 12 CFR 363 to have the IPA attest to the assertion of management concerning the effectiveness of the banks' internal control structure and procedures for financial reporting.[104] The IPA performs the attestation in accordance with generally accepted standards for attestation engagements[105] or PCAOB auditing standards.[106]
- **Integrated audit by an IPA:** In an integrated audit of internal control over financial reporting and the financial statements, the auditor designs his or her testing of controls to accomplish the objectives of both audits simultaneously even though the objectives of the audits are not identical.[107]
- **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 auditing standards 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 review, carried out by bank directors or other independent parties, entails specified or agreed-upon procedural reviews such as procedures related to the adequacy of internal controls not affecting internal controls over

[102] 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 and certain conditions are met. Refer to 12 CFR 363.1(b), "Compliance by Subsidiaries of Holding Companies."

[103] Management's report required to satisfy 12 CFR 363.2(b), "Management Report," must contain a statement identifying the internal control framework used by management to evaluate the effectiveness of the insured depository institution's internal control over financial reporting.

[104] Refer to 12 CFR 363.3(b), "Internal Control Over Financial Reporting." (Footnote added version 1.1)

[105] Refer to the AICPA ASB AU-C section 940, "An Audit of Internal Control Over Financial Reporting That Is Integrated With an Audit of Financial Statements." (Footnote updated version 1.1)

[106] Refer to PCAOB Auditing Standard (AS) 2201, "An Audit of Internal Control Over Financial Reporting That Is Integrated With An Audit of Financial Statements."

[107] Refer to AICPA ASB AU-C section 940 and PCAOB AS 2201.

financial reporting and the accuracy of financial information. Refer to appendix B of this booklet for more information on agreed-upon procedures.[108]

Engagement Letters

The audit committee should have external auditors submit engagement letters for review and approval before commencing audit work.[109] Engagement letters 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 external auditors will omit. Additionally, the letter should specify whether the external auditor is expected to render an opinion on the bank's financial statements.

In performing its duties with respect to the appointment of the bank's IPA, the audit committee for banks covered by 12 CFR 363[110] shall ensure that engagement letters and any related agreements with the IPA for services to be performed do not contain any limitation-of-liability provisions that

- indemnify the IPA against claims made by third parties.
- hold harmless or release the IPA from liability for claims or potential claims that might be asserted by the client insured depository institution, other than claims for punitive damages.
- limit the remedies available to the client insured depository institution.

Alternative dispute resolution agreements and jury trial waiver provisions are permitted in engagement letters provided that they do not incorporate any limitation-of-liability provisions set forth in 12 CFR 363.5(c)(1). When the bank executes agreements that limit the external auditors' liability, the external auditors' objectivity, impartiality, and performance may be weakened or compromised, and the usefulness of the audits for safety and soundness purposes may be diminished.[111]

---

[108] Refer to AICPA ASB SSAE No. 10, Professional Standards, AT section 201, "Agreed-Upon Procedures Engagements."

[109] 12 CFR 363, appendix A.31 outlines audit committee duties, which include ensuring that audit engagement letters comply with the provisions of 12 CFR 363.5(c) before engaging an IPA. 15 USC 78j-1(i), "Preapproval Requirements," requires audit committees of publicly held banks to review and approve all external audit engagement letters prior to beginning any work. Refer to PCAOB AS 1301, "Communications With Audit Committees," and AICPA ASB AU-C section 210, "Terms of Engagement." For non-public banks not covered by 12 CFR 363, refer to ASB AU-C section 210.09–10, "Agreement on Audit Engagement Terms."

[110] Refer to 12 CFR 363.5, "Audit Committees."

[111] Refer to OCC Bulletin 2006-7.

External Audit Independence

External auditors must adhere to independence standards depending on their client banks. Auditor independence standard-setters include the AICPA, PCAOB and SEC. For non-public banks not covered by 12 CFR 363, the OCC expects that an external auditor meet the AICPA independence standards.[112] For banks covered by 12 CFR 363, the IPA must adhere to independence standards and interpretations of the AICPA, PCAOB, and SEC, applying the most restrictive of these independence standards. For audits to be effective, the external auditors, acting as the bank's IPA, must be independent in fact and appearance. External auditors should avoid situations that may lead outsiders to doubt their independence.[113] (Updated version 1.1)

The OCC expects all accounting firms that perform external audit work for banks to be independent.[114] These standards and requirements focus on relationships and services (financial, employment, business, and 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. (Updated version 1.1)

The bank and its external auditors should discuss and consider whether the relationship or services do or could

- create a conflict of interest between the bank and its IPA.
- place the IPA in the position of auditing the IPA's own work.
- result in the IPA acting in the capacity of bank management or a bank employee or being in a position to act as an advocate for the bank.

For banks subject to 12 CFR 363, the external auditor must disclose, in writing, all relationships with the bank and its related entities or persons in financial reporting oversight roles that may reasonably be thought to affect the independence of the external auditor.[115]

At the request of the bank board or its audit committee and senior management, external auditors often provide non-audit services (e.g., advisory) throughout the year. If the bank has a class of securities registered with the OCC under section 12 of the Securities Exchange Act of 1934 or is subject to 12 CFR 363, there are specific non-audit services that the external

[112] Ibid.

[113] Refer to SEC regulations at 17 CFR 210 and 240 and the AICPA Code of Professional Conduct.

[114] Refer to OCC Bulletin 2003-12 and OCC Bulletin 1999-37 for banks subject to 12 CFR 363 or the filing and reporting requirements of 12 CFR 11, and 17 CFR 210.2-01, "Qualifications of Accountants" (public companies) and subsequent revisions for publicly registered companies.

[115] Refer to PCAOB Rule 3526, "Communications With Audit Committees Concerning Independence." Refer also to 12 CFR 363.3(f), which states that an IPA must comply with the independence standards and interpretations of the AICPA, the SEC, and the PCAOB. To the extent that any of the rules within any one of these independence standards is more or less restrictive than the corresponding rule in the other independence standards, the IPA must comply with the more restrictive rule.

financial statement auditor cannot perform for the bank. The following is a list of relationships or non-audit services that would affect the independence of the IPA:

- Financial relationships with the bank held individually or by close family members, such as
  - investments in the bank or bank investment in the accounting firm.
  - the bank acting as underwriter for the auditor.
  - having loans to or from an audit client except for certain consumer loans, such as mortgages or auto loans.
  - maintaining savings, checking, brokerage, or similar accounts in excess of insured amounts.
  - broker/dealer accounts.
  - futures commission merchant accounts.
  - credit card accounts with a balance greater than $10,000.
  - holding individual insurance policies, and for the firm, professional liability policies.
  - investing in an investment company that is in the same investment company complex as the audit client.
- Employment relationships between the bank and the IPA, such as
  - the IPA being employed by the bank or serving on the bank board or in a similar management capacity before a one-year cooling-off period is completed.
  - employments of the accountant's close family members or a former employee of the audit firm at the bank who can influence the bank's financial records.
  - a former bank officer, director, or employee becoming an employee or a partner in the audit firm and participating in the audit.
- The IPA acting, temporarily or permanently, as a director, officer, or employee of a bank, or performing any decision-making, supervisory, or ongoing monitoring function for the bank.
- Providing non-audit services to the bank, such as
  - bookkeeping.
  - financial information systems design and implementation.
  - appraisal or valuation services, fairness opinions, or contribution-in-kind reports.
  - actuarial services.
  - internal audit outsourcing (co-sourced or fully outsourced) services.
  - management functions or human resources.
  - broker/dealer, investment advisor, or investment banking services.
  - legal services and expert services unrelated 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.

External Audit Competence and Peer Review

PCAOB auditing standards and generally accepted auditing standards (GAAS) (collectively, auditing standards) require that an auditor be proficient and competent in auditing and accounting. Audits must be conducted using due professional care in the performance of the

audit and the preparation of the report. In most states, audits of financial statements must be performed by a certified public accountant (CPA). Obtaining a CPA license requires education in accounting and auditing. Most states also require continuing education to renew a CPA license. The AICPA also has continuing education requirements for its members.

Before commencing any services for an insured depository institution subject to 12 CFR 363, the IPA must have received a peer review, or be enrolled in a peer review program, that meets acceptable guidelines.[116] Acceptable peer reviews include those performed in accordance with the AICPA's *Standards for Performing and Reporting on Peer Reviews* (peer review standards) and inspections conducted by the PCAOB.

Fieldwork Standards

Auditing standards require the external auditor to adequately plan the audit and to properly supervise any assistants.[117] The auditor should 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 should be sufficient to allow the auditor to obtain enough information through audit procedures, such as inspection, observation, inquiries, and retesting, to draw a reasonable opinion regarding the financial statements and, as applicable, internal controls under audit. The external audit plan should encompass any use of the bank's internal audit function work. Refer to the "Special Situations" section for information on using internal audit work.

The IPA must retain the work papers related to the audit of the insured depository bank's financial statements and, if applicable, the evaluation of the bank's internal control over financial reporting for seven years from the report release date, unless a longer period is required by law.[118]

Reporting Standards

In accordance with auditing standards, the auditor must provide an opinion on whether the financial statements, including disclosures (such as footnotes to the financial statements) are presented fairly, in all material respects, in conformity with GAAP.[119] The auditor's report must express an opinion regarding the financial statements as a whole or must state that an

[116] 12 CFR 363.3(g)(1) denotes IPA requirements for peer reviews and inspection reports, whereas 12 CFR 363.3(g)(2) stipulates the notification and filing requirements.

[117] Refer to AICPA ASB AU-C section 300, "Planning An Audit," and section 220, "Quality Control for an Engagement Conducted in Accordance With Generally Accepted Auditing Standards." Also refer to PCAOB AS 2101, "Audit Planning," and 1201, "Supervision of the Audit Engagement." (Footnote added version 1.1)

[118] 12 CFR 363.3(e), "Retention of Working Papers," denotes IPA work paper retention requirements.

[119] AICPA ASB AU-C section 700, "Forming an Opinion and Reporting on Financial Statements," and PCAOB AS 3101, "The Auditor's Report on an Audit of Financial Statements When the Auditor Expresses an Unqualified Opinion." (Footnote added version 1.1)

opinion cannot be expressed.[120] If an overall opinion cannot be expressed, the auditor must state the reasons.[121]

Assessing Deficiencies by External Audit

The external auditor evaluates and determines the effect of control deficiencies made known during an audit.[122] Control deficiencies can exist in the design or the operational effectiveness, or both, of an internal control or set of controls. Auditing standards require the auditor to assess each control deficiency that comes to his or her attention and determine its impact, individually or collectively, as of the date of management's assessment. The risk severity assigned depends on whether there is a reasonable possibility that the bank's controls will fail to prevent or detect a misstatement of an account balance or disclosure, as well as on the magnitude of the potential misstatement resulting from the deficiency or deficiencies. Two common terms are used to define the magnitude of a control deficiency:[123]

A **material weakness** is a deficiency, or combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented or detected on a timely basis.

A **significant deficiency** is defined as a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Communication

The OCC encourages communication and cooperation between bank management, external auditors, and the OCC examination team. For an effective relationship to exist, the engagement between the bank and the external auditor should involve individuals who are knowledgeable, informed, and empowered by their respective organizations to exchange information. Communication and cooperation can benefit all parties by helping to improve

[120] Ibid. Refer also to AICPA ASB AU-C section 705, "Modifications to the Opinion in the Independent Auditor's Report," and PCAOB AS 3105, "Departures from Unqualified Opinions and Other Reporting Circumstances." (Footnote added version 1.1)

[121] Ibid. (Footnote added version 1.1)

[122] AICPA ASB AU-C section 265, "Communication of Internal Control Related Matters Identified in an Audit," includes definitions of the kinds of deficiencies in internal control. AICPA ASB AU-C section 265 also includes the guidance for evaluating such deficiencies that is provided in PCAOB AS 2201.

[123] Refer to AICPA ASB AU-C section 265 and PCAOB AS 1305, "Communications About Control Deficiencies in an Audit of Financial Statements."

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.[124]

The statute 12 USC 1831m(h) requires each insured depository institution that has engaged the services of an independent auditor to transmit to the auditor a copy of the most recent report of condition and a copy of the most recent report of examination (ROE). The insured depository institution shall also provide the auditor with a copy of any supervisory memorandum of understanding and any written agreement between the insured depository institution and the OCC and a copy of various types of enforcement action.[125] Also, the FDIC can require the auditor of a large bank to review quarterly financial reports as required by 12 USC 1831m(g)(2).

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

Auditors' Reports

An IPA's report on its audit of the financial statements, and, as applicable, internal control over financial reporting, should include[126]

- the identification of the financial statements that have been audited, including the related disclosures.
- a statement that the financial statements are the responsibility of management.
- a description of the auditor's responsibility and the auditing standards used.
- a brief discussion of what the audit entails.
- the auditor opinion.
- as applicable, explanatory paragraphs.

Further, if the report is for an integrated audit of the financial statements, the auditor includes its opinion on the results of its audit of internal controls over financial reporting.[127] Refer to appendix C, "12 CFR 363 Reporting," of this booklet for more information.

[124] Refer to OCC Bulletin 2016-2, "Interagency Advisory on External Audits of Internationally Active U.S. Financial Institutions," for supervisory expectations regarding differences between U.S. standards and practices and the BCBS External Audit Guidance. One point of distinction relates to communication with the external auditor. This bulletin notes that contrary to the BCBS guidance, part 1 principles 6 and 7, U.S. banks and holding companies are not required by law or regulation to report directly to the institution's primary federal regulator.

[125] Refer to 12 USC 1831m(h)(1)(B)(i). (Footnote added version 1.1)

[126] Refer to AICPA ASB AU-C section 700, and specifically AU-C section 700.25. Refer to PCAOB AS 3101, and specifically paragraph 3101.08.

[127] 12 CFR 363.3(b) requires IPAs of an insured depository institution with total assets of $1 billion or more to examine, attest to, and report separately on the assertion of management.

Audit Opinions

Four types of opinions—unqualified, qualified, adverse, and a disclaimer of opinion—are put forth in IPA reports. The definitions of the different opinions are generally consistent under GAAS[128] and PCAOB auditing standards.[129] Refer to the "Special Situations" section of this booklet for information on international auditing standards.

Unqualified opinion: An unqualified opinion is used when financial statements present fairly, in all material respects, the financial position, results of operations (e.g., 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.

Qualified opinion: A qualified opinion states that, except for the effects of the matter(s) to which the qualification relates, the financial statements present fairly, in all material respects, the financial position, results of operations, and cash flows of the entity in conformity with GAAP. A qualified opinion is used when (1) the auditor, having obtained sufficient appropriate audit evidence, concludes that misstatements, individually or in the aggregate, are material but not pervasive to the financial statements or (2) the auditor is unable to obtain sufficient appropriate audit evidence on which to base the opinion, but the auditor concludes that the possible effects on the financial statements of undetected misstatements, if any, could be material but not pervasive.

Adverse opinion: An adverse opinion is used when the auditor, having obtained sufficient appropriate audit evidence, concludes that misstatements, individually or in the aggregate, are both material and pervasive to the financial statements. An adverse opinion indicates that the financial statements do not present fairly the financial position, results of operations, or cash flows of the entity in conformity with GAAP.

Disclaimer of opinion: A disclaimer of opinion states that the auditor does not express an opinion on the financial statements. Disclaimer of opinion is used when the auditor is unable to obtain sufficient appropriate audit evidence on which to base the opinion, and the auditor concludes that the possible effects on the financial statements of undetected misstatements, if any, could be both material and pervasive.

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 bank board or management, and actions to verify appropriate remediation.[130] If the IPA's opinion is

[128] Refer to AICPA ASB AU-C section 700 and AU-C section 705.

[129] Refer to PCAOB AS 3101.

[130] Refer to 12 CFR 30, appendix A II.B.

anything other than an unqualified opinion, examiners should meet with the external auditor to determine the facts and circumstances that led to the opinion. Examiners should also promptly advise the OCC supervisory office of any qualified or adverse opinion 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 the bank board or its audit committee. The extent of communication varies depending on audit findings and statutory requirements. This communication can best be described in three areas: internal control-related matters, communication with audit committee, and confirmation of audit independence.

Communication of Internal Control-Related Matters Noted in the Audit

Under auditing standards, the auditor is required to communicate, in writing, to management and the audit committee all significant deficiencies and material weaknesses.[131] Under GAAS, the auditor should also communicate to management, either orally or in writing, other deficiencies identified during the audit that have not been communicated to management by other parties and that, in the auditor's professional judgment, are of sufficient importance to merit management's attention.[132] Under PCAOB standards, the auditor should communicate to management or the audit committee deficiencies in internal control over financial reporting identified during the audit that are neither significant deficiencies nor material weaknesses.[133]

Communication With Audit Committees

Auditing standards require the external auditor to communicate the following items to the audit committee:[134]

- Planned scope and timing of audit, including extent of use of the work of the bank's internal auditors.
- Significant risks identified during auditor's risk assessment procedures.
- Auditor responsibilities under the applicable auditing standards.
- Views about qualitative aspects of the entity's significant accounting practices, including accounting policies, accounting estimates, and financial statement disclosures.
- Uncorrected misstatements.

[131] Refer to 12 CFR 363, appendix A, 18A, "Internal Control Attestation Standards for Independent Auditors."

[132] Refer to AICPA ASB Professional Standards section 265, "Communicating Internal Control Related Matters Identified in an Audit."

[133] Refer to AICPA ASB Professional Standards, section 265, paragraph 12b.

[134] Refer to AICPA ASB AU-C section 260, "The Auditor's Communication With Those Charged With Governance." For banks without audit committees, such as insured federal branches, communication should be made to the audit committee's equivalent.

- Disagreements with management.
- Consultation with other accountants.
- Significant difficulties encountered in performing the audit.
- Material, corrected misstatements that the auditor brought to the attention of management as a result of audit procedures.
- Significant findings or issues, if any, arising from the audit that were discussed, or the subject of correspondence, with management.
- The auditor's views about significant matters that were the subject of management's consultations with other accountants on accounting or auditing matters, when the auditor is aware that such consultation has occurred.
- Written representations.

For audits of publicly held banks, the external auditor is required to also communicate the following:[135]

- Extent of use of the work of the bank's internal auditors.
- Significant risks identified during auditor's risk assessment procedures.
- Auditor responsibility for other information in documents containing auditing financial statements.
- Difficult or contentious matters for which the auditor was consulted.
- Matters relating to the company's ability to continue as a going concern, if the auditor believes there is substantial doubt or previous concerns have been alleviated.
- Significant issues discussed with management before retention.

For banks covered by 12 CFR 363,[136] the external auditor must also communicate the following:

- All critical accounting policies and practices to be used by the insured depository institution.
- All alternative accounting treatments within GAAP for policies and practices related to material items that the IPA has discussed with management, including the ramifications of the use of such alternative disclosures and treatments, and the treatment preferred by the IPA.
- Other written communications the IPA has provided to management, such as a management letter or schedule of unadjusted differences.

[135] Refer to PCAOB AS 1301.

[136] 12 CFR 363.3(d) indicates that the IPA must meet communication requirements in accordance with accounting standards, as well as additional items.

Confirmation of Audit Independence

The bank board or its designated audit committee should confirm the independence of the bank's external auditor.[137] IPAs auditing banks covered by 12 CFR 363 must communicate in writing to the audit committee, at least annually, all relationships with the bank and its related entities or persons in financial reporting oversight roles that may reasonably be thought to affect independence.[138] Additionally, this IPA is required to annually affirm its independence to the audit committee, in writing, as of the date of the communication.[139] For banks not covered by 12 CFR 363 the IPAs should comply with relevant AICPA standards for confirmation of independence.

Special Situations

Mergers and Acquisitions

There are two instances when banks are provided relief from the annual reporting requirements of 12 CFR 363.[140] Banks merged out of existence before the filing deadlines are not required to file. When business mergers or acquisition businesses occur close to the filing deadlines, such as when a consummation date is in the same period, a bank is not required to file. In situations such as this, there is insufficient time for management to conduct an assessment of the system of internal controls over financial reporting.

De Novo Banks

As a condition of preliminary approval of a newly chartered bank, the OCC and the FDIC normally require banks to have an annual independent external audit for three years after they open. The first audit should occur no later than 12 months after the bank opens for business. The OCC expects the audit to be of sufficient scope to enable the auditor to render an opinion on the financial statements of the bank or consolidated holding company.[141] (Updated version 1.1)

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

[137] 12 CFR 363.3(f) indicates that auditors of banks covered by 12 CFR 363 must comply with independence standards and interpretations of the AICPA, PCAOB, and SEC, along with following the most stringent standard. Refer to PCAOB rule 3526, "Communication With Audit Committees Concerning Independence," for further information.

[138] Refer to PCAOB Rule 3526. (Footnote added version 1.1)

[139] Ibid. (Footnote added version 1.1)

[140] Refer to 12 CFR 363.2, "Annual Reporting Requirements," and appendix A, 8A, "Management's Reports on Internal Control Over Financial Reporting under 12 CFR 363 and Section 404 of SOX."

[141] Refer to the "Charters" booklet of the *Comptroller's Licensing Manual*.

- the new bank's financial statements are included in the audited consolidated financial statements of the parent holding company of the bank.
- the sponsoring holding company is an existing holding company that has operated for three years or more under the supervision of the Board of Governors of the Federal Reserve System and does not have any banks subject to special supervisory concerns.
- adequate internal audit coverage is 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 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 includes that determination in its preliminary conditional approval letter. If any of these requirements 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 policymaking 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 OCC expects the group to be able to demonstrate that internal expertise or other outside sources can substantially provide the benefits generally associated with an external audit.[142] 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. (Updated version 1.1)

Banks Presenting Supervisory Concern

Sometimes weaknesses in internal controls or MIS adversely affect financial reporting or contribute to a material deterioration in the 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 before any meetings with external auditors.[143]

Holding Company Subsidiaries

When the bank is owned by a holding company, the OCC may address the scope of the bank's external audit program in the context of the bank's relationship to the consolidated

[142] Ibid.

[143] Refer to OCC Bulletin 1999-37.

group. For banks subject to 12 CFR 363, the total assets of the insured depository institutions must make up at least 75 percent of the holding company's consolidated total assets for holding company-level reports to be eligible to meet the audited financial statement requirement in 12 CFR 363.2.[144] The other requirements of 12 CFR 363 (e.g., audit of internal control over financial reporting) for an insured depository institution that is a subsidiary of a holding company may be satisfied by the top-tier or any mid-tier holding company if the insured depository institution meets the criterion specified in 12 CFR 363.1(b)(2).[145]

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 at the insured depository institution level. If the examiner believes transaction testing may not have been sufficient, he or she should discuss the matter with the bank and its external auditor.

Use of Internal Audit Work

An external auditor may consider the use of the internal audit function in planning and conducting an external audit.[146] The use of internal auditor's work may include using the internal audit function in obtaining audit evidence or to provide direct assistance under the direction, supervision, and review of the external auditor, or both. The external auditor must make a determination concerning the nature and extent of the internal audit function's work that can be used.[147] Adequate documentation should be retained to support this planning.

When considering use of the internal audit function in obtaining audit evidence, the external auditor is required to evaluate three areas:[148]

- The function's organizational status and relevant policies and procedures to adequately support the objectivity of the internal auditors.
- The level of competence of the function.
- The application by the function of a systematic and disciplined approach, including the internal audit function quality control activities.

When considering the use of internal auditors to provide direct assistance, the external auditor's evaluation focuses on whether internal auditors can be used and to what extent. The

[144] Refer to 12 CFR 363.1(b). Banks with $5 billion or more in total assets must also have a CAMELS rating of 1 or 2.

[145] Management report signature requirements are described in 12 CFR 363.2(c).

[146] Refer to AICPA ASB AU-C section 610, "Using the Work of Internal Auditors," for more information. Refer to PCAOB AS 2605, "Consideration of the Internal Audit Function."

[147] Ibid. (Footnote added version 1.1)

[148] Ibid. (Footnote added version 1.1)

external auditor considers the internal auditor's objectivity and competence, and risk mitigating factors. Factors determining the extent of the work consider the

- external auditor's evaluation of the existence and significance of threats to the internal auditors' objectivity, the effectiveness of the safeguards applied to reduce or eliminate the threats, and the level of competence of the internal auditors who will be providing such assistance.
- assessed risk of material misstatement.
- amount of judgment involved.

The external auditor should communicate to the bank board or its designated audit committee its plans for using internal audit work.[149] Examiners should be aware that the results of the external auditor's planning around using work of internal auditors may affect the bank's current internal audit plans.

Notice by Accountant of Termination of Services

An external audit firm performing an audit under 12 CFR 363 that ceases to be the IPA for an insured depository institution shall notify the FDIC, the appropriate federal banking agency (such as the OCC), and any appropriate state bank supervisor in writing of such termination within 15 days after the occurrence of such event and set forth in reasonable detail the reasons for such termination.[150] The written notice to the OCC should be filed at the appropriate supervisory office.

Audits Performed in Accordance With International Auditing Standards

Audits of FBOs may be performed in accordance with the International Auditing and Assurance Standards Board's *International Standards on Auditing*.

Unlike other banks, insured branches of foreign banks are not separately incorporated or capitalized. To determine whether 12 CFR 363 applies, an insured branch should use "Total claims on non-related parties" reported on its Report of Assets and Liabilities of U.S. Branches and Agencies of Foreign Banks (form FFIEC 002) in place of total consolidated assets. Most OCC-supervised FBOs are under the $500 million threshold and therefore 12 CFR 363 would not apply.

An insured branch of a foreign bank satisfies the financial statements requirement of 12 CFR 363 by filing one of the following for each of its two most recent fiscal years:

[149] PCAOB AS 1301, and specifically AS 1301.10. AICPA ASB AU-C section 260 provides that the external auditor may include communications regarding how the external auditor and the internal auditors can work together in a constructive and complementary manner, including any planned use of the work of the internal audit function in obtaining audit evidence and the nature and extent of any planned use of internal auditors to provide direct assistance. Refer to ASB AU-C section 260.A20.

[150] Refer to 12 CFR 363.3(c) for the requirement for the IPA to provide notice. Refer to 12 CFR 363.4(d) for the requirement for the bank to provide a copy of the notice to the FDIC, the appropriate federal banking agency (such as the OCC), and any appropriate state bank supervisor in writing of engagement or change of accountant.

- Audited balance sheets, disclosing information about financial instruments with off-balance-sheet risk.
- Assets and liabilities, schedules RAL and L of form FFIEC 002, prepared and audited on the basis of the instructions for its preparation.
- With written approval of the appropriate federal banking agency, consolidated financial statements of the parent bank.

The management report of the insured branch of a foreign bank should be signed by the branch's management official if the branch does not have a CEO or a chief accounting or financial officer. Because an insured branch of a foreign bank does not have a separate bank board, the FDIC does not apply the audit committee requirements of 12 CFR 363 to such branches.[151] Any such branch is encouraged, however, to make a reasonable effort to see that similar duties are performed by persons whose experience is generally consistent with 12 CFR 363 requirements for an institution the size of the insured branch.

International Standards on Auditing

Unmodified opinion: An unmodified opinion is used when the auditor concludes that the financial statements are prepared, in all material respects, in accordance with the applicable financial reporting framework.

Modified (qualified) opinion: A qualified opinion is used when

- the auditor, having obtained sufficient appropriate audit evidence, concludes that misstatements, individually or in the aggregate, are material, but not pervasive, to the financial statements; or
- the auditor is unable to obtain sufficient appropriate audit evidence on which to base the opinion, but the auditor concludes that the possible effects on the financial statements of undetected misstatements, if any, could be material but not pervasive.[152]

Adverse opinion: The auditor shall express an adverse opinion when the auditor, having obtained sufficient appropriate audit evidence, concludes that misstatements, individually or in the aggregate, are both material and pervasive to the financial statements.[153]

[151] Refer to 12 CFR 363, appendix A.27.

[152] Refer to International Standards on Auditing 705, "Modifications to the Opinion in the Independent Auditor's Report." (Footnote added version 1.1)

[153] Ibid. (Footnote added version 1.1)

Disclaimer of opinion: The auditor shall disclaim an opinion when the auditor is unable to obtain sufficient appropriate audit evidence on which to base the opinion, and the auditor concludes that the possible effects on the financial statements of undetected misstatements, if any, could be both material and pervasive.[154]

OCC Assessment of Audit Functions

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

- establish the scopes of current supervisory activities.
- contribute to strategies for future supervisory activities.

The examiner-in-charge (EIC) should tailor the audit review to fit examination objectives.[155] When doing so, the EIC should consider the bank's size, complexity, scope of activities, and risk profile. Examiners must complete the audit core assessment during each supervisory cycle, and may need to perform expanded procedures from this booklet. (Updated version 1.1)

Examiners responsible for audit reviews, through coordination with functional and specialty area examiners, should determine how much reliance the OCC can place on audit work. OCC examiners assess the bank's overall audit function during each supervisory cycle by

- drawing a conclusion about the adequacy and effectiveness of the overall audit program and the bank board's oversight of the audit program.
- assigning a rating to the overall audit program (strong, satisfactory, insufficient, or weak).[156] (Updated version 1.1)

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,

[154] Ibid.

[155] In this context, EIC means the EIC of the supervisory activity, the functional EIC, or bank EIC, as appropriate based on the circumstances. Refer to the "Bank Supervision Process" booklet of the *Comptroller's Handbook* for more information about the various types of EICs.

[156] The "Community Bank Supervision" and "Large Bank Supervision" booklets of the *Comptroller's Handbook* provide guidance for assigning the audit program rating.

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.[157]

Analysis. Examiners should review audit reports and management responses, bank board and audit committee minutes, relevant committee 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 related to the internal audit area, such as organization charts, internal audit charter or mission statement, external auditor engagement letters, outsourcing or co-sourcing written agreements, affiliate agreements, audit manuals, operating instructions, job specifications and descriptions, staff training records, flow charts, and internal control and risk assessments.

Examiners should operate in accordance with their OCC supervisory office guidance and instruction for analysis and documentation of the bank's 12 CFR 363 annual reporting.

Communication: Examiners should maintain ongoing and clear communications with audit-related personnel throughout an examination or supervisory cycle. They should periodically meet with the bank's audit committee, audit management and staff (including outsourced internal audit third parties), and other bank personnel closely associated with risk control functions (e.g., risk managers and control officers). Examiners should establish communication lines and periodically meet with the 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 (e.g., 12 CFR 363 or SEC regulations).

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 the bank should include comments about the adequacy of the bank's audit functions and summarize other appropriate findings and conclusions about audit functions.

Linkage: Examiners should 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 the bank's audit functions.

Interagency coordination: Audit supervision may involve working with the Federal Reserve Board examiners in bank holding company situations, FDIC examiners in problem bank situations, or other functional supervisory agencies such as the SEC and Consumer Financial Protection Bureau. In such cases, the EIC should coordinate the timing of audit reviews and share information with the appropriate supervisory agencies. Examiners

[157] Appendixes in this booklet provide worksheets that can assist examiners in their assessment of audit.

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

Supervisory Reviews

In developing the appropriate scope for audit reviews, examiners of community banks should begin with the core assessment audit objectives and procedures from the "Community Bank Supervision" booklet of the *Comptroller's Handbook*. Examiners of midsize and large banks should begin with the audit core assessment factors from the "Large Bank Supervision" booklet of the *Comptroller's Handbook* and tailor their review of audit to fit their objectives and needs. Examiners should take into consideration audit assessments in other target examinations, along with ongoing supervision activities, when completing the audit core assessment. As part of the audit reviews, examiners may need to perform expanded procedures from this booklet to assess the audit functions. (Updated version 1.1)

Corporate and Risk Governance Reviews

Review of the bank's corporate and risk governance relating to audit should focus on the board and management oversight of the audit functions, along with the audit functions' governance structure. Examiners should assess these elements within their assessments of both internal and external audit functions, but may review it separately. Examiners should determine the adequacy and effectiveness of board and management oversight of the audit functions.

Internal Audit Reviews

Review of the bank's internal 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 deficiencies. (Updated version 1.1)

Reviews for in-house, outsourced, or co-sourced internal audit activities, should encompass

- policies and processes.
- staffing resources and qualifications.
- risk and control assessments.
- annual audit plans, schedules, and budgets.
- frequency of audits and audit cycles.
- individual audit work programs and audit reports.
- quality assurance and improvement activities.
- follow-up activities.
- 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 the bank's overall audit program. The OCC review, however, is not an "audit of the auditors," nor is it designed to determine whether the audit conforms to auditing standards. Reviews of external audit determine whether the bank board or its audit committee effectively oversees the bank's external audit program and whether the program complies with statutory and regulatory requirements, as applicable.

Reviews should focus on

- the oversight of the external audit function.
- the type of external audit activity performed.
- the external auditor's conclusions, findings, and communications to the bank board or its audit committee.
- 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. If external audit communications are not in writing, examiners should ask bank management their reasons for not obtaining written communications.

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

Topics of discussion could include the following:

- Extent of the external auditor's reliance on the work done by internal auditors.
- Extent of the external auditor's assessment and testing of internal controls over financial reporting.
- Results and conclusions of risk assessments, including fraud risk assessment.
- External auditor reliance on internal controls over financial reporting when auditing financial reports.
- Examination and audit results or major findings.
- Upcoming audit and examination activities.
- Assessment of internal controls.
- Reports, management letters, or other documents.
- Other appropriate audit or supervisory topics.

12 CFR 363 Annual Reports Review

The examiner should conduct a review of the 12 CFR 363 annual reports for any bank covered by 12 CFR 363 or voluntary submitters. The primary purpose of this review is to facilitate the early identification of problems in financial management of these banks.

Required reports include financial statement audits conducted by IPAs, information on the structure and effectiveness of internal controls, and other required communications with those charged with governance of the external auditor. Examiners should conduct a review of the 12 CFR 363 annual reports as part of the next quarterly review, target examination, or full-scope examination, no later than the quarter following the bank's submission. Results of this review should be utilized in supervision activities, such as strategy considerations, subsequent examinations, and discussions with bank management. (Updated version 1.1)

Examiners should promptly advise the OCC supervisory office of any qualified or adverse opinion or disclaimer of opinion encountered.

Refer to appendix C, "12 CFR 363 Reporting," of this booklet for more information.

Centralized Third-Party Audit Reviews

When a third party performs internal or external audit work for two or more banks in a geographical area, examiners may choose or be called to perform a centralized review of the third party's work (e.g., centralized third-party audit review). Examiners can coordinate this review with examiners from one field office or with examiners from multiple field offices. A centralized third-party audit review may result in examination efficiencies by reducing the supervisory burden on the bank and the third party, as well as on examiners, and may eliminate duplication of examination efforts. A centralized third-party audit review also may result in a more consistent examination approach for reviewing third-party work. Examiners can use the centralized third-party audit review process to determine the effectiveness and reliability of third-party audit work and can leverage review results in scoping individual examinations and OCC audit reviews at affected banks.

Ideally, centralized third-party audit reviews should be part of the audit review planning process and should take place before the start of any on-site examinations at affected banks. A team of experienced examiners who are familiar with audit processes should perform the reviews. Review team examiners should consult with the assistant deputy comptroller (ADC), EIC, or portfolio manager of each affected bank to help determine which work papers to review at the centralized third-party audit review. The initial centralized third-party audit review should be comprehensive. Subsequent centralized third-party audit reviews could consist of a limited review of work papers and discussions with the third party to determine whether there have been significant changes in the process, system, scope, or findings since the previous review. A more complete centralized third-party audit review of internal audit work papers should be performed every second supervisory cycle or as instructed by the ADC, EIC, or portfolio manager.

The focus of centralized third-party audit reviews is on the quality and reliability of internal or external audit work for each individual bank, rather than a blanket endorsement of the third party. The reviews are not a substitute for or waiver of other work examiners must do as part of their overall audit assessment during on-site examinations or other supervisory activities at the individual banks. Examiners are encouraged and have the flexibility, if appropriate, to undertake additional testing at the bank level or to review additional audit

work papers during on-site and other supervisory activities during a supervisory cycle. Examiners should base that decision on events that have occurred since the most recent centralized third-party audit review and any other matters that come to their attention during supervisory activities (e.g., high-risk areas and new products and services). (Updated version 1.1)

Refer to the "Validation" section of this booklet for more information.

Sarbanes–Oxley Act Section 404 Attestations

Registered Banks

- For banks that have a class of securities registered with the OCC under 12 CFR 11 or 12 CFR 16, examiners are directly responsible for assessing compliance with the requirements of SOX. In these banks, if the review of the overall compliance program, including section 404 supporting documentation, reveals any significant weaknesses, examiners should discuss the matter with bank management and the board and include them in a matters requiring attention (MRA) in the ROE and, if appropriate, cite a violation of law on the specific section of SOX at the bank level.

Registered Holding Companies

- For banks that are subsidiaries of holding companies with securities registered with the SEC, the OCC is not directly responsible for assessing compliance with SOX because compliance is assessed at the holding company level. For these banks, examiners should, however, gain sufficient understanding of the holding companies' overall SOX compliance program to determine any impact on the bank's risk profile. The bank's reputation risk may increase if full compliance with SOX is not achieved at the holding company level. The scope of the supervisory activities required to assess this risk should be based on the banks' size and complexity. If the review of the overall compliance program reveals any significant weaknesses, examiners should discuss the weaknesses with bank management and the board and include them as MRAs in the ROE.

- Violations of law regarding any section of SOX at the holding company level should not be cited at the bank level. Such violations or concerns should be forwarded to the bank's holding company regulator. Examiners should coordinate such communications with their supervisory office.

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 the 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 the following:

- Discussions with bank management and audit personnel.
- Audit work paper reviews.
- Process reviews (such as reviews of policy adherence, scorecards, risk assessments, issues management and follow-up activities, and quality assurance and reporting).

To validate the adequacy of the bank's audit program, OCC examiners should progress, as needed, through three successive steps: work paper review, use of expanded procedures, and verification. (Updated version 1.1)

Work Paper Review: Internal Audit

The OCC considers internal audit a fundamental building block of a sound system of internal controls. Therefore, during each supervisory cycle, examiners must review an appropriate sample of internal audit program work papers. This review also includes work papers for outsourced or co-sourced internal audit work performed by independent third parties and work papers for directors' examinations.

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 or ongoing supervision. The selected sample should do the following:

- Represent a cross section of bank functions, activities, and bank-assigned internal audit ratings.[158]
- Preferably be taken from high-risk, problem, or rapid growth or decline areas, technology audits, and products, services, or activities new to the bank.
- Provide a sufficient basis to
  - validate the scope and quality of the audit program.
  - determine how much reliance, if any, can be placed on the audit program and internal control system.

When the directors' examination serves as the **sole** internal audit function for the bank, a sample of the supporting work papers **must** be reviewed. Many banks that continue to have directors' examinations also have a system of independent reviews of key internal controls in lieu of a full-scale internal audit function. In these cases, when the directors' examination serves as only a piece of the bank's internal audit function, the sample may be selected from the in-house audit work, the directors' examination, or a combination of the two. For example, many small community banks have independent cash counts, reconcilements and other reviews that make up an effective control system. If these independent reviews are

[158] When the directors' examination is the bank's sole audit function, examiners have the flexibility to limit the work paper review to only one segment of the work papers, if the segment selected is sufficient to validate the effectiveness of the audit program.

adequately documented, examiners may choose to review a sample of these work papers in lieu of reviewing work papers from the director's examination.

Work paper documentation should support the internal audit program's conclusions. In reviewing work papers, examiners should not perform the bank's audit procedures.

When the director' examination consists of both internal and external audit work (i.e., serves as the 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 (such as operational and internal control reviews and transaction testing).

The EIC can limit the scope of the work paper reviews (e.g., 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.

Work Paper Review: Outsourced Internal Audit

When internal audit is outsourced to a third party and work papers are stored in that third party'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 on-site examinations; examiners can review the work papers any time during the bank's supervisory cycle (i.e., as part of planning activities, quarterly reviews, periodic monitoring, or targeted reviews). Examiners must review an appropriate sample of outsourced internal audit work papers during every supervisory cycle. The sample should provide a sufficient basis to validate the scope and quality of outsourced internal audit activities and determine to what extent examiners can rely on the bank's internal audit program and internal control system. Examiners should weigh the pros and cons of traveling to the third party's office or having the bank ask the third party to send copies of designated work papers to the bank.

When a third party performs internal audit program work for multiple banks, 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 parties and the application of a consistent supervisory approach to such work paper reviews. Examiners may coordinate centralized outsourced audit reviews with other OCC field offices when a third party performs internal audit work for multiple banks in a geographical area.

Work Paper Review: External Audit

Except for directors' examinations, examiners are not required to review external audit work papers during a supervisory cycle.[159] (Refer to the "Work Paper Review – Internal Audit"

[159] When the directors' examination is the bank's only audit function, examiners have the flexibility to limit the work paper review to only one segment of the work papers, if the segment selected is sufficient to validate the effectiveness of the audit program.

section of this booklet for more information). External audit work papers, however, 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 (such as insufficient internal audit coverage).
- If questions are raised about matters that are normally within the scope of an external audit program.

The following are examples of situations that might trigger an external audit work paper review:

- Unexpected or sudden changes in the bank's external auditor. Examiners should consider having discussions with the previous and current external auditor before embarking on a work paper review. If the discussions raise unanswered questions that might be addressed in the work papers, then a work paper review may be warranted.
- Significant changes in the bank's external audit program. Examiners should contact the external auditor to discuss these changes and determine whether a review of work papers is warranted.
- Significant and unexpected changes in accounting or operating results.
- 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 on request.[160] 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 examiners determine that an external audit program's work papers warrant review, the examiners should discuss the request with bank management and the external auditor. This discussion may make the work paper review unnecessary or may help examiners focus their review on the most relevant work papers.

[160] Refer to 12 CFR 363, appendix A.13, "General Qualifications." Also refer to 12 USC 1831m(g)(3) and OCC Bulletins 2013-29, 2017-7, and 2017-21 for more information. (Footnote updated version 1.1)

Rather than a blanket request to review all external audit work papers, examiners should make specific requests and supporting reasons regarding areas of greatest interest. 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.[161] If presented with such a letter, examiners should not sign it. Instead, examiners should complete the OCC acknowledgment letter template in appendix H, "OCC Acknowledgment of External Audit Work Paper Request Letter," of this booklet and return the letter 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 work papers, examiners should contact the appropriate OCC accounting expert and legal counsel.

The external auditor may need to offer assistance to examiners for the review of 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 be aware that external auditors may charge the bank for time spent 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 external audit firm may also require that its representative(s) be present during the reviews and may not allow photocopying. EICs of community banks and midsize banks should consult with their ADCs and district accountants, and may wish to consult with OCC legal staff, before beginning to review any external audit program work papers. Similarly, large bank EICs should consult with their Large Bank Supervision deputy comptroller and the Chief Accountant's Office, and may wish to consult with OCC legal staff, before beginning such a review.

Use of Expanded Procedures

(Section updated version 1.1)

Examiners determine which expanded procedures to use, if any, during examination planning or after drawing preliminary conclusions during the core assessment. Expanded procedures contain detailed guidance for examining specialized activities or products that warrant extra review beyond the core assessment. In completing the audit core assessment, examiners may identify significant audit or control discrepancies or weaknesses or may raise questions about the audit functions' effectiveness. In those situations, examiners should consider expanding the audit program review by selecting steps from the expanded procedures in the

[161] Refer to AICPA ASB AU-C section 230, "Audit Documentation."

"Examination Procedures" section of this booklet.[162] Examiners should determine, in consultation with the EIC, whether to expand audit examination work in affected operational or functional business areas.

Examiners should consider expanding audit program examination procedures if they encounter or identify the following:

- 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 bank without adequate audit or internal control.
- Inappropriate actions by insiders to influence the findings or scope of audits.
- Identification of significant operational or functional business area(s) not identified by audit.
- Significant concerns about the adequacy of internal audit, the soundness of internal controls, or the integrity of financial or risk management controls for an audited area.
- Any of the following issues:
  - Key account records are significantly or chronically out of balance.
  - Management is uncooperative or poorly manages the bank.
  - Management attempts to restrict access to bank records.
  - Significant accounting, audit, or internal control deficiencies remain uncorrected from previous examinations or from one audit to the next.
  - Bank auditors are unaware of, or unable or unwilling to sufficiently explain, significant deficiencies.
  - Management engages in activities that raise questions about its integrity.
  - Repeated violations of law affect audit, internal controls, or regulatory reports.

The scope of expanded work should be sufficient to determine the extent of problems and their effect on bank operations.

Verification Procedures

When reviewing the audit functions, any significant concerns about the adequacy of an audit or internal controls, or about the integrity of the bank's financial or risk management controls, should result in examiners' consideration of further expanding the audit review to include verification procedures.[163] Verification procedures should be considered even when

[162] Refer to the "Bank Supervision Process" booklet of the *Comptroller's Handbook* for more information on expanded procedures.

[163] Per the "Bank Supervision Process" booklet of the *Comptroller's Handbook*, verification procedures are designed to guide verification of the existence or proper recordation of assets or liabilities, or test the reliability of financial records. Verification procedures can be found in most booklets in the *Safety and Soundness* and *Asset Management* series of the *Comptroller's Handbook*. (Footnote updated version 1.1)

the external auditor issues an unqualified opinion. Discrepancies or weaknesses may call into question the appropriateness of the opinion.

Required Use

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

- Key account records are significantly or chronically out of balance.
- Management is uncooperative or poorly manages the bank.
- Management attempts to restrict access to bank records.
- Significant accounting, audit, or internal control deficiencies remain uncorrected from previous examinations or from one audit to the next.
- Bank auditors are unaware of, or unable or unwilling to sufficiently explain, significant deficiencies.
- Management engages in activities that raise questions about its integrity.
- Repeated violations of laws or regulations that affect audit, internal controls, or regulatory reports. (Updated version 1.1)

There may be other situations when examiners believe audit or controls warrant further investigation. In those cases, examiners should consider the risk posed by any 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 functions 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.
  - management has initiated timely corrective action in the past.
- Have the bank contract with third parties, such as its professional audit firm or other independent party, to perform the verification. Use this alternative when management's capabilities and commitments are inadequate or when substantive problems exist with having the bank or its audit functions perform the procedures.

If examiners choose to use either of the previously mentioned options, the actions taken should resolve each identified supervisory problem in a timely manner. Supervisory follow-up should include a review of audit work papers in areas where the bank audit was expanded. Examiners should review associated audit third-party written agreements to confirm OCC examiners have appropriate access to work papers and reports. (Updated version 1.1)

The supervisory office decides on a case-by-case basis whether to pursue verification and, if so, determines the extent of verification and who performs it. Verification procedures are generally performed only in rare cases when significant concerns exist. Examiners should

consult with the bank's external auditors to determine whether the auditors completed applicable verification procedures. If so, examiners should 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 the bank's audit functions. Examiners should 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, IT, and fiduciary audits using the same criteria they use for any other type of audit. Appendixes in this booklet provide worksheets that may help examiners evaluate the bank's audit functions. Examiners should refer to the relevant booklets of the *Comptroller's Handbook* and *FFIEC IT Examination Handbook* to determine the adequacy of audit coverage and assessment of a particular business entity or function (such as booklets in the *Consumer Compliance* and *Asset Management* series).

Audit Rating

At the conclusion of the audit review, examiners should assign a rating to the audit functions. Regardless of the overall audit rating assigned, the ROE should contain comments summarizing the adequacy of the bank's audit program and any significant audit issues or concerns.[164]

The Uniform Interagency Consumer Compliance Rating System takes into consideration the bank's audit activities. When assigning a consumer compliance rating, examiners must consider the adequacy of the bank's consumer compliance program, including internal policies and procedures, consumer compliance training, consumer complaint response, and monitoring and audit activities that the bank uses to ensure compliance with applicable consumer laws, rules, and regulations. The rating system additionally considers board and management oversight that includes, but is not limited to, the identification and remediation of control deficiencies.[165] (Updated version 1.1)

Under the Uniform Rating System for Information Technology (URSIT), part of the evaluation of the bank's IT system includes an assessment of the IT audit program.

[164] Refer to the "Bank Supervision Process," "Community Bank Supervision," and "Large Bank Supervision" booklets of the *Comptroller's Handbook* for audit rating guidance.

[165] Refer to the "Compliance Management Systems" booklet of the *Comptroller's Handbook* for more information regarding assessing the adequacy of the bank's consumer compliance program and board and management oversight.

Under the Uniform Interagency Trust Rating System (UITRS), the fiduciary activities of national banks, national trust banks, FSAs, and trust-only FSAs are assigned a component rating for five areas. One of those areas is operations, internal controls, and auditing. For this area to be considered adequate, audit coverage should assess the integrity of the financial records, the sufficiency of internal controls, and the adequacy of the compliance process. (Updated version 1.1)

Information regarding these rating systems and other regulatory rating systems, such as CAMELS and ROCA, can be found in the "Bank Supervision Process" booklet of the *Comptroller's Handbook.* (Updated version 1.1)

Examination Procedures

This booklet contains expanded procedures for examining specialized activities or specific products or services that warrant extra attention beyond the core assessment contained in the "Community Bank Supervision," "Federal Branches and Agencies Supervision," and "Large Bank Supervision" booklets of the *Comptroller's Handbook*. Examiners determine which expanded procedures to use, if any, during examination planning or after drawing preliminary conclusions during the core assessment.

Scope

These procedures are designed to help examiners tailor the examination to each bank and determine the scope of the internal and external audits examination. This determination should consider work performed by internal and external auditors and other independent risk control functions and by other examiners on related areas. Examiners need to perform only those objectives and steps that are relevant to the scope of the examination as determined by the following objective. Seldom will every objective or step of the expanded procedures be necessary.

Objective: To determine the scope of the examination of internal and external audits and identify examination objectives and activities necessary to meet the needs of the supervisory strategy for the bank.

1. Review the following sources of information and note any previously identified problems related to internal and external audits that require follow-up:

   (Updated following list version 1.1)

   - Supervisory strategy.
   - Examination scope memorandum.
   - The OCC's supervisory information system.
   - Previous reports of examination and work papers
   - Internal and external audit reports and work papers.
   - Bank management's responses to previous reports of examination and audit reports.
   - Customer complaints and litigation. Examiners should review customer complaint data from the OCC's Customer Assistance Group, the bank, and the Consumer Financial Protection Bureau (when applicable). When possible, examiners should review and leverage complaint analysis already performed during the supervisory cycle to avoid duplication of effort.
   - Centralized audit firm review memorandum, if applicable

2. Obtain the results of such reports as

   - the Uniform Bank Performance Reports (UBPR).

- Canary, an OCC application used as an analytical tool to generate reports containing benchmarked measures.
- PCAOB inspection report pertaining to the bank's external audit firm, if the bank is publicly held.

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

   - OCC audit summary memos and work papers from the previous examinations.
   - Internal audit reports, including audit reports that the auditors may have participated in or relied on to any extent, such as SOC audits. (Updated version 1.1)
   - External auditor reports and other correspondence to the bank or, if applicable, its parent company.
   - Minutes of audit committee meetings and applicable bank board-level committee meetings since the last examination.
   - Audit packages and information submitted to board-level and executive-level committees.
   - Listing of members of the audit committee(s), including those on the fiduciary audit committee, if applicable, and the date of each member's appointment to the committee.
   - Audit plans and schedules.
   - Any engagement letters or written agreements pertaining to external audit or internal audit activities, including related organization services.
   - The bank's annual reports.
   - Correspondence memorandums.

4. Obtain and review the following documents to determine the structure of the bank's internal and external audit functions.

   - Any report of resignation of external auditor of a public company, or of a holding company if the bank is public.
   - Bank organizational chart relative to the internal audit function.
   - Holding company organizational chart relative to the bank's internal audit function.

5. Obtain and review policies, procedures, and reports bank management uses to supervise internal and external audits, including any quality assurance or internal risk assessments.

6. In discussions with bank management determine whether there have been any significant changes. Discussions should address

   - how the audit committee supervises audit activities.
   - any significant changes in business strategy or activities that could affect the audit functions (e.g., third-party relationships, products, services, delivery channels, market geographies).

- any material changes in the audit program, scope, schedule, or staffing related to internal and external audit activities (e.g., external auditor, outsourcing or co-sourcing scope, and audit tools or audit systems).
- any other internal or external factors that could affect the audit functions (e.g., audit projects or initiatives).
- observations from examiner review of internal bank reports, as well as OCC and other third-party-generated reports.

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

   - distributing to each examiner responsible for an examination area a copy of the area's audit report or a list of significant audit deficiencies for that area.
   - requesting that the examiner prepare and return a memorandum stating whether the bank board or management has addressed the audit deficiencies and whether their actions were adequate.

8. For banks with any outsourced internal audit function, obtain the following documents to gain an understanding of the scope of services:

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

9. Identify internal audit work programs, including those from any outsourced internal audit activities and directors' examination, from which to select a reasonable sample of internal audit work papers for validation purposes. Coordinate work paper review efforts with the examiners reviewing functional or specialty areas (such as credit, capital markets, consumer compliance, asset management, or IT) and

   - provide the examiner(s) with the audit program(s) and audit report(s) for the specific area(s) to be tested.
   - request that the examiner(s) review applicable internal audit work papers.

Note: Examiners may want to use appendix E, "Internal Audit Review Worksheet," as an aid in completing work paper reviews.

10. Based on an analysis of information obtained in the previous steps, as well as input from the EIC, determine the scope and objectives of the internal and external audits examination.

11. Select from the following examination procedures the necessary steps to meet examination objectives and the supervisory strategy.

Functional Area Procedures

Board and Management Oversight

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

Objective: To determine the overall quality of bank board and its audit committee oversight of the bank's audit functions.

1. Obtain the bank's risk governance structure that outlines the bank board and relevant committee reporting structures. This information should also include all relevant holding company board or board-level committees. Determine if the bank board has appropriately delegated any audit oversight responsibilities by

   - establishing a bank audit committee for banks with $500 million or more in total assets.
   - establishing a bank fiduciary audit committee for bank organizations with trust powers active.
   - annually approving audit committee charter that outlines the committee's responsibilities, member qualifications, authorities, independence, and bank board reporting.
   - maintaining written, approved criteria for determining whether current or prospective members of the audit committee are independent of management and are outside directors.
   - reflecting record of these decisions in the bank board meeting minutes.

2. By discussing audit activity with bank management, reviewing bank board or audit committee minutes and audit information packages, and performing appropriate examination procedures, determine whether the bank board or its audit committee does the following:

   - Reviews and approves audit strategies, policies, programs (including the Bank Secrecy Act compliance program), audit charter, and organizational structure, including selection, termination, and compensation of external auditors or outsourced internal audit third parties.
   - Establishes schedules and agendas for regular meetings with internal and external auditors. The audit committee should meet at least four times a year.
   - Supervises the audit functions directly to ensure that internal and external auditors are independent and objective in their findings.
   - Works with internal and external auditors to ensure that the bank has comprehensive audit coverage to meet the risks and demands posed by its current and planned activities.

- Has significant input into hiring senior internal audit personnel, setting their compensation, and evaluating the chief auditor's performance.
- Reviews and approves annual audit plans and schedules (and any changes thereto) for both internal and external audits.
- Retains auditors (internally or outsourced) who are fully qualified to audit the kinds of activities in which the bank is engaged.
- Meets with bank examiners at least once each supervisory cycle to discuss findings of OCC reviews of the bank's audit functions.
- Monitors, tracks, and, when necessary, provides discipline to ensure effective and timely response by management to correct control weaknesses and violations of laws or regulations noted in internal or external audit reports or in examination reports.

3. Determine if the bank board or its designated audit committee appropriately evaluates the performance of the audit functions by

   - establishing written objective criteria for evaluating the internal audit function.
   - conducting evaluations of the internal audit function based on these criteria.
   - evaluating activities related to managing risks of any third-party audit services.
   - documenting all such evaluations and related decisions within the committee meeting minutes.

4. Determine if the bank board or its designated audit committee has established and maintains an effective whistle-blower procedure. The whistle-blower procedure enables bank employees to confidentially and anonymously submit concerns to the committee about questionable accounting, internal accounting controls, or auditing matters. Consider

   - the periodic review and approval of the policy related to the whistle-blower procedure.
   - whether the context of the policy provides adequate guidance for roles and responsibilities to support effective whistle-blower procedure execution and maintenance.
   - whether the whistle-blower policy and procedure promote timely investigation of reported information.
   - whether bank employees are aware of whistle-blower procedure.
   - if applicable, the incorporation of holding company whistle-blower activities that affect the bank.
   - whistle-blower submissions, since last examination, and actions.

5. For banks with trust powers that offer CIFs, determine if the bank board retains direct responsibility for the annual audit of CIFs in accordance with 12 CFR 9.18(b)(6)(i). Consider the following:

   - Formal approval of the CIF audit work as part of the external audit program and schedule, if choosing to utilize the bank's external auditor as the third-party auditor.

- Formal approval of engagement or written agreement for conducting the CIF audit before onset of work.
- Discussion of the third-party auditor's independence in conducting the CIF audit.
- Review of third party's CIF audit report with management and third-party auditors in a timely manner.

Objective: To determine if the bank's audit committee structure and activities are appropriate for the bank's size, complexity, scope, and nature.

1. Obtain the bank board's most recent annual audit committee membership determination, which should be reflected in the minutes of board meetings and any bank board's written criteria.

2. For banks covered under 12 CFR 363, the bank board should have written criteria of audit committee composition and structure. Determine if these written criteria ensure conformance with 12 CFR 363 for existing or potential members, which encompass outside director and independence of management status. The bank board may put forth additional criteria as relevant.

   - An outside director is a director who is not, and within the preceding fiscal year has not been, an officer or employee of the bank or any affiliate of the bank.
   - Independence of management considerations include the following:
     – If an outside director, either directly or indirectly, owns or controls, or has owned or controlled within the preceding fiscal year, 10 percent or more of any outstanding class of voting securities of the bank, the bank board should determine, and document its basis and rationale for such determination, whether such ownership of voting securities would interfere with the outside director's exercise of independent judgment in carrying out the responsibilities of an audit committee member, including the ability to evaluate objectively the propriety of management's accounting, internal control, and reporting policies and practices.
     – If the bank board determines that such ownership of voting securities would interfere with the outside director's exercise of independent judgment, the outside director is not considered independent of management.
   - The bank board should not consider an outside director independent of management if any of the following apply:
     – The director serves, or has served within the last three years, as a consultant, advisor, promoter, underwriter, legal counsel, or trustee of or to the bank or its affiliates.
     – The director has been, within the last three years, an employee of the bank or any of its affiliates or an immediate family member is, or has been within the last three years, an executive officer of the bank or any of its affiliates.
     – The director has participated in the preparation of the financial statements of the bank or any of its affiliates at any time during the last three years.
     – The director has received, or has an immediate family member who has received, during any 12-month period within the last three years, more than $100,000 in direct and indirect compensation from the bank, its subsidiaries, and its affiliates

for consulting, advisory, or other services other than director and committee fees and pension or other forms of deferred compensation for prior service (provided such compensation is not contingent in any way on continued service). Direct compensation also would not include compensation received by the director for former service as an interim chair or interim CEO.
  - The director or an immediate family member is a current partner of a firm that performs internal or external auditing services for the bank or any of its affiliates; the director is a current employee of such a firm; the director has an immediate family member who is a current employee of such a firm and who participates in the firm's audit, assurance, or tax compliance practice; or the director or an immediate family member was within the last three years (but no longer is) a partner or employee of such a firm and personally worked on the audit of the insured depository institution or any of its affiliates within that time.
  - The director or an immediate family member is, or has been within the last three years, employed as an executive officer of another entity where any of the present executive officers of the bank or any of its affiliates at the same time serves or served on that entity's compensation committee.
  - The director is a current employee, or an immediate family member is a current executive officer, of an entity that has made payments to, or received payments from, the bank or any of its affiliates for property or services in an amount which, in any of the last three fiscal years, exceeds the greater of $200,000 or 5 percent of such entity's consolidated gross revenues. This amount would include payments made by the bank or any of its affiliates to not-for-profit entities where the director is an executive officer or where an immediate family member of the director is an executive officer.

3. Review the bank audit committee membership and the board determination to see whether the bank board concluded that the committee is made up entirely of outside directors of the bank.

4. If the bank had $500 million or more in total assets at the beginning of its current fiscal year, review the board's determination to see if it also concluded that its audit committee complies with 12 CFR 363 by meeting the following criteria:

   - The committee is made up entirely of outside directors of the bank.
   - For banks with $500 million to $1 billion in total assets, the majority of committee members are independent of management. For banks with $1 billion or more in total assets, each committee member is independent of management.

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

- At least two members of the committee have
  - significant executive, professional, educational, or regulatory experience in financial, auditing, accounting, or banking matters as determined by the bank board, or
  - significant experience as an officer or member of the board or audit committee of a financial services company.
- The committee has access to its own counsel at its discretion and without prior approval of the board or management.
- No committee member is a large customer of the bank.

6. Review the audit committee charter to determine that duties are clearly defined and are appropriate to the size of the bank and the complexity of its operations and include

   - the appointment, termination, compensation, and oversight of the IPA.
   - reviewing with management and the IPA the basis for their respective reports issued under 12 CFR 363.2(a) and 12 CFR 363.2(b) and 12 CFR 363.3(a) and 12 CFR 363.3(b).
   - reviewing and satisfying itself as to the IPA's compliance with the required qualifications for IPAs set forth in 12 CFR 363.3(f), 12 CFR 363.3(g), and 12 CFR 363, appendix A.13-A.16.
   - ensuring that audit engagement letters comply with the provisions of 12 CFR 363.5(c) before engaging an IPA.
   - being familiar with the notice requirements in 12 CFR 363.4(d) and 12 CFR 363, appendix A.20 regarding the selection, change, or termination of an IPA.
   - ensuring that management sends a copy of any notice required under 12 CFR 363.4(d) to the IPA when the notice is filed with the FDIC.
   - working with internal and external auditors to ensure that the bank has appropriate audit coverage.
   - ensuring senior management establishes and maintains an adequate and effective internal control system and processes.
   - monitoring the financial reporting process and overseeing the establishment of accounting policies and practices by the bank and reviewing the significant qualitative aspects of the bank's accounting practices, including accounting estimates, financial reporting judgments, and financial statement disclosures.
   - establishing and maintaining whistle-blower procedure.
   - holding committee meetings at least four times a year.
   - establishing schedules and agendas for regular meetings with internal auditors, along with external auditors when providing oversight.
   - monitoring, tracking, and holding management accountable for effective and timely response in addressing deficiencies that auditors or regulators identify. (Updated version 1.1)

7. Review the audit committee charter to determine that any additional responsibilities are clearly defined. Appropriate additional duties could include the following:

- Reviewing with bank management and the external auditor the scope of services, significant accounting policies, and conclusions regarding significant accounting estimates.
- Reviewing with bank management and the external auditor the effectiveness of internal controls over financial reporting, the resolution of related material weaknesses, and the prevention or detection of management overrides or compromises.
- Discussing with bank management and the external auditor any significant disagreements.
- Reviewing with bank management the bank's compliance with applicable laws and regulations.
- Reviewing and approving a talent management program only as it pertains to the internal audit function. (Updated version 1.1)
- Overseeing the internal audit function.
- Overseeing fiduciary audit responsibilities for bank organizations with trust powers.
- Meeting with bank examiners to discuss findings of OCC reviews, including conclusions regarding audit. (Updated version 1.1)

8. Review the audit committee charter to determine that duties are clearly defined when overseeing the internal audit function. Audit committee's responsibilities when overseeing the internal audit function should include the following: (Updated version 1.1)

    - Appointing, compensating, and overseeing the chief auditor.
    - Reviewing and approving audit strategies, audit policies, audit programs, and audit organizational structure.
    - Documenting risks and mitigations associated with the audit hierarchy reporting structure.
    - Reviewing and approving internal audit's risk assessments and the scope of the internal audit plan.
    - Reviewing and approving the selection and termination of any outsourced internal audit activities.
    - Ensuring that internal auditors are independent and objective in their findings and consistent with their independence principles and rules.
    - Retaining auditors who are qualified to perform the audit activities.
    - Establishing objective criteria to oversee and evaluate the internal audit function, which may include managing risks of outsourced internal audit activities.

9. Determine whether the chief auditor position has the appropriate stature and independence for the size and complexity of the bank. The chief auditor is expected to functionally report directly to the bank board or to its designated audit committee. (Updated version 1.1)

    - Considerations for chief auditor's placement in the organization include that
        - the chief auditor, as expected by the OCC, is an employee of the bank, but may also be an employee of the holding company.

  - the chief auditor should have stature, whereby in large banks subject to 12 CFR 30, appendix D, the chief auditor must be one level below the bank's CEO.
- Considerations for chief auditor's administrative reporting include that
  - administrative activities are limited to routine personnel matters (e.g., leave and attendance reporting).
  - chief auditor may report to the bank's CEO in place of the audit committee.
- Considerations of the bank board or its designated audit committee's decision of chief auditor's placement in dual reporting situations should include
  - the bank board's periodic risk evaluation of diminished independence and any risk mitigants of dual reporting.
  - the audit committee's documentation of its consideration of reporting hierarchy and risk mitigants.

10. Evaluate board and management oversight relative to applicable audit functions. Examiners should complete applicable examination procedures in the sections titled "Internal Audit Function," "Outsourcing Internal Audit," and "External Audit Function."

Objective: To determine whether the board oversight complies with 12 CFR 9 (national banks) or 12 CFR 150.440 (FSAs), respectively.

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

1. Determine whether the bank has fiduciary powers and engages in fiduciary activities. If so, proceed with steps 2 through 4 by reviewing previously requested materials.

2. Determine whether the national bank has a fiduciary audit committee that meets the following requirements as established at 12 CFR 9.9(c):

   - The fiduciary audit committee is a committee of the bank's directors or an audit committee of an affiliate of the bank.
   - Members of the fiduciary audit committee do not include any officers who participate significantly in the administration of the national bank's fiduciary activities (12 CFR 9.9(c)(1)).
   - A majority of fiduciary audit committee members are not also members of any other committees to which the bank board has delegated power to manage and control the national bank's fiduciary activities (12 CFR 9.9(c)(2)).

3. Determine whether the FSA has a fiduciary audit committee that meets the following requirements as established at 12 CFR 150.470:

   - The fiduciary audit committee is a committee of the FSA's directors or an audit committee of an affiliate.

- The officers of the FSA and the officers of an affiliate who participate significantly in administering the FSA's fiduciary activities do not serve on the fiduciary audit committee (12 CFR 150.470(a)).
- A majority of the members of the fiduciary audit committee cannot serve on any committee to which the board has delegated power to manage and control the FSA's fiduciary activities (12 CFR 150.470(b)).

4. Determine whether the bank board meeting minutes meet the following requirements:

   - For banks that arrange an annual fiduciary audit, results (including significant actions taken as a result of the audit) must be noted in the minutes of the bank board meetings in accordance with 12 CFR 9.9(a) for national banks or 12 CFR 150.480(a) for FSAs.
   - For banks that use a continuous audit system for fiduciary activities, results of all discrete audits performed since the last audit report (including significant actions taken as a result of the audits) must be noted in the minutes of the bank board meetings at least once during each calendar year, in accordance with 12 CFR 9.9(b) for national banks or 12 CFR 150.480(b) for FSAs.

Annual Filing and Reporting

Objective: If the bank is covered under 12 CFR 363, to determine compliance with annual filing and reporting requirements.

Note: Examiners may want to use appendix D, "12 CFR 363 Report Worksheet," as an aid in completing this portion of the examination procedures.

1. Review the bank's most recent fiscal year-end management report (12 CFR 363.2(b)) and determine whether the report fulfills the following criteria:

   - The report is appropriately signed by
     - the bank CEO and chief accounting or chief financial officer when the audited financial report and management report requirements are satisfied solely at the bank.
     - the bank CEO and chief accounting or chief financial officer, along with the holding company CEO or chief accounting or chief financial officer, when the report requirements are satisfied by any portion of the bank (i.e., management report components).
     - the holding company CEO and chief accounting or financial officer when filing requirements of annual audited financials and management report are satisfied solely at the holding company.
     - the branch's managing official of a foreign bank when the branch does not have a CEO or a chief accounting or financial officer.
   - The report contains a statement of management's responsibilities for
     - preparing the bank's annual financial statements.

  - establishing and maintaining adequate internal control structures and procedures for financial reporting.
  - complying with laws and regulations relating to safety and soundness that are designated by the FDIC and the OCC (12 CFR 363.2(b)(1)).[166]
- The report contains an assessment by management of the bank's compliance with designated safety and soundness laws and regulations during the fiscal year. The assessment must state management's conclusion as to whether the bank has complied with the designated safety and soundness laws and regulations during the fiscal year and disclose any noncompliance with these laws and regulations (12 CFR 363.2(b)(2)).
- If the bank had $1 billion or more in total assets at the beginning of the fiscal year, the report contains the following:
  - A statement identifying the internal control framework used by management to evaluate the effectiveness of the bank's internal control over financial reporting.
  - A statement that the assessment included controls over the preparation of regulatory financial statements in accordance with regulatory reporting instructions, including identification of such regulatory reporting instructions.
  - A statement expressing management's conclusion as to whether the bank's internal control over financial reporting is effective as of the end of its fiscal year. Management must disclose all material weaknesses in internal control over financial reporting, if any, that it has identified that have not been remediated before the bank's fiscal year-end. Management is precluded from concluding that the bank's internal control over financial reporting is effective if there are one or more material weaknesses.

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

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

3. Review the bank's determination that it met the filing and notice requirements of 12 CFR 363.4. Does the determination indicate that

   - the bank that is neither a public company nor a subsidiary of a public company that meets the criterion specified in 12 CFR 363.1(b)(1) filed its 12 CFR 363 annual report within 120 days after the end of its fiscal year?

[166] Refer to 12 CFR 363, appendix A, table 1.

- the bank that is a public company or a subsidiary of a public company that has total assets of $1 billion or more at the beginning of its fiscal year filed its 12 CFR 363 annual report within 90 days after the end of its fiscal year?
- the bank's annual report required by 12 CFR 363.4(a) to be filed is available for public inspection (12 CFR 363.4(b))?

Objective: If the bank is subject to the periodic filing and reporting requirements of 12 CFR 11 (i.e., the bank has registered its securities with the OCC), to determine compliance with certain SEC requirements.

1. Review correspondence or other communications issued by the OCC's Chief Counsel's Office, Securities and Corporate Practices Division, resulting from its review of the bank's proxy material and annual reports.

2. Determine whether the bank has adequately addressed issues requiring attention resulting from the review by the OCC's Chief Counsel's Office, Securities and Corporate Practices Division.

Internal Audit Function

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

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

   - adequately monitors internal control systems.
   - is independent and objective.
   - is staffed by qualified persons.
   - adequately tests and reviews information systems.
   - adequately documents tests, findings, and corrective actions.
   - verifies and reviews management actions addressing material weaknesses.
   - requires the bank board or its audit committee to review the internal audit systems' effectiveness.

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

2. Determine whether the bank's internal audit program has

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

- an audit plan that addresses goals, schedules, staffing budget, reporting, and, if applicable, financial budgets.
- policies and procedures that appropriately govern the activities of its internal audit program and are utilized by appropriate audit personnel.
- a program for professional development and training of audit personnel including orientation and in-house and external training opportunities.
- a quality assurance program performed by internal or external parties to evaluate the operations of the internal audit function.

3. Review bank board and its audit committee meeting minutes, or summaries, and audit information submitted or presented to the bank board or its audit committee. Determine whether

   - the bank board or its audit committee has formally approved the internal audit program, including mission statement or audit charter, and annual audit plan and schedule.
   - internal audit reports and other audit-related information submitted regularly to the board or audit committee are sufficient for effective monitoring of internal audit's performance and progress toward meeting approved audit plans and schedules. Consider
     – status reports of the annual audit plan and schedules.
     – activity reports for audits completed, in process, and deferred or cancelled.
     – staffing and training reports.
     – tracking reports for significant outstanding audit and control issues.
     – discussion of significant regulatory or accounting issues.
     – risk assessments, evaluations, or summaries.
     – results of regulatory examinations.
     – other information the audit committee or internal auditor deems appropriate.
   - the internal audit program and annual plan or schedule are periodically reviewed and updated by the chief auditor, with changes reported to the board or audit committee.
   - progress has been made toward completing the audit program or schedule, and whether the board or audit committee has approved significant audit program or audit schedule changes.
   - consideration is given to staffing, compensation, and training requirements.
   - management does not unduly participate in or dominate the directors' or audit committee's supervision of the internal audit function.

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

   - Determine whether management's standards for measuring the adequacy and effectiveness of internal controls over financial reporting are appropriate. Consider
     – sources of established standards (e.g., AICPA, OCC, and COSO).
     – risk analyses or assessments.

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

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

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

7. Evaluate the adequacy and effectiveness of the quality assurance and improvement function by determining whether

   - a formal quality assurance and improvement program is established and maintained (for large banks, refer to 12 CFR 30, appendix D).
   - standards and criteria have been established for evaluating the performance of the internal audit function.
   - quality assurance is conducted by
     - continuous supervision by the chief auditor,
     - periodic internal reviews by a team or individual from the internal audit staff, or
     - external reviews by qualified persons independent of the bank.
   - any type of formal report, written or oral, is generated and to whom the report is directed (e.g., chief auditor, senior management, or the bank board or its audit committee).
   - quality assurance reviews are conducted regularly.

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

   - are adequately reviewed and approved by the bank board or its audit committee annually.
   - properly reflect authorities and responsibilities established by the audit charter or mission statement.
   - establish appropriate use and development of audit work programs, tools, and information. Consider
     - change management.
     - confidentiality, integrity, and availability.
   - establish adequate audit risk assessment guidance to effectively analyze risks that includes, but is not limited to
     - maintenance of an inventory of all material processes (for large banks, refer to 12 CFR 30, appendix D).
     - the leveraging of non-internal audit assurance activities.

  - risk-scoring methodology.
  - audit risk assessment overrides.
  - minimum documentation requirements.
- establish proper scope and frequency for internal audits. Consider
  - statutory requirements and regulatory guidelines.
  - purpose and objectives of audits.
  - control and risk assessments.
  - audit cycles.
  - audit plan changes or overrides.
  - reporting relationships and requirements.
- establish adequate guidelines for human resources involved in the audit function. Consider
  - organization and independence of the audit department.
  - responsibilities of audit staff.
  - job standards and qualifications.
  - training and development.
  - performance evaluations.

Objective: To evaluate the independence and competence of those who manage and perform internal audit functions.

1. Obtain the following:

   - Résumés of the chief auditor, new internal audit staff, or those recently promoted to senior levels.
   - Job descriptions for various bank audit positions.
   - List of those that are employees of the bank or other related organizations, or both.
   - As deemed appropriate, performance evaluations of the chief auditor and selected audit staff.

2. Determine whether there are any reporting lines or operational duties assigned to the chief auditor that are incompatible with the internal audit function, such as

   - reporting to a senior bank management official (e.g., chief financial officer).
   - a dual reporting scenario in which functional reporting is not to the audit committee or administrative reporting is to someone other than the CEO.
   - responsibilities for development of or operating a system of internal controls or actually performing operational duties or activities.

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

3. Assess the educational and professional experience of the chief auditor and staff by reviewing résumés and noting the following:

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

4. Review job descriptions and discuss the following with the chief auditor:

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

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

6. Assess audit personnel turnover and vacancies, focusing on the reasons for turnover or vacancies and their effect on the internal audit function.

7. Evaluate the actions to identify and remediate any undue influence of staff that could compromise their independence. Consider

   - transfers into or from auditee areas.
   - rotational or temporary auditor assignments.

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

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

Objective: To determine the adequacy and the reliability of work performed by the internal auditors.

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

   - internal audit reports.
   - internal audit work programs.
   - internal audit work papers.

2. Using internal audit work programs previously identified in the “Scope” section of these examination procedures, obtain or request access to internal audit work papers to

complete this objective and its steps. Consider having examiners responsible for other areas of the bank (e.g., credit, capital markets, consumer compliance, information systems, or fiduciary) review internal audit work programs and work papers associated with those activities.

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

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

5. Determine the appropriateness of the bank's internal audit program in analyzing non-internal audit assurances and integration into the audit plan. Obtain and review the service provider's reports and other non-internal audit assurance reports. Consider the following: (Updated version 1.1)

   - The reliability of the non-internal audit assurance source.
   - The timing and scope (i.e., tested user controls) of the assurance report.
   - Incorporation into the audit risk assessment and plan.
   - Follow-up activities of user considerations or issues identified in the assurance report.

6. Review internal audit reports to determine whether they are adequate and prepared in accordance with established audit policy. Consider the following elements of the reports:

   - Distribution
     – To division heads or senior management responsible for taking action.
     – To internal audit staff, as appropriate.
     – To the bank board or its audit committee.
   - Time frames
     – Audit findings discussed with appropriate parties (e.g., division personnel or senior management) after completion of audit work.
     – Responses obtained from appropriate parties after discussion of audit findings.
     – Final report issued after discussion of audit findings and receipt of responses.
   - Content
     – Executive summary or opening paragraph.
     – Statements on the audit's purpose, objectives, and scope.
     – Findings, recommendations, root causes of deficiencies, and other comments.
     – Management commitments.
     – Opinion or grading summary.
   - Follow-up
     – Written responses from audited parties to division or senior management and the internal auditor.
     – Auditor's review and discussion of corrective action efforts or results with appropriate parties.
     – A re-audit, if performed.

7. Review the bank's audit plan(s) and audit schedule. Determine whether adequate coverage and internal risk assessment are provided for all areas and activities of the bank, including those operated by third parties.

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

   - objectives of testing.
   - procedures to meet objectives.
   - populations subject to sampling.
   - method of sampling (e.g., statistical or judgmental).
   - selecting and justifying a representative sample sufficient to support conclusions.
   - evaluation of results and documentation of conclusions.

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

   - Do the work papers disclose that specific program steps, calculations, or other evidence supports the procedures and conclusions set forth in the reports? Consider the following:
     – Verification of account balances (reconciliation, confirmation, and physical count).
     – Review or test of income and expense accounts, accruals, gains and losses, including computations.
     – Transaction testing and testing the value or pricing of assets (e.g., investments, collateral).
     – Physical inspection of legal and supporting documentation, including validation of authorities granted (e.g., making or approving loans, signing official bank documents, etc.).
     – Review of information system data controls.
     – Review and evaluation of policies, procedures, and internal controls.
     – Checks of compliance with laws and regulations.
     – Checks of adherence to bank policy.
   - Is the scope of the internal audit procedures adequate and properly documented? Consider the following:
     – Audit planning memorandums.
     – Checklists.
     – Internal control questionnaires.
     – Control and risk assessments.
     – Previous audit reports, responses, and follow-up.
     – Procedures performed (general and specific).
     – Type of testing conducted.

10. Review the activities to manage audit issues. Determine the adequacy to track, monitor, and follow up on identified audit issues. Audit issues include those control issues

identified in audits performed as part of the internal audit plan, which may include those identified in non-internal audit assurance reports. Consider the following:

- Remediation ownership is assigned to an individual with appropriate level of accountability.
- Status reflects distinction between management closure and internal audit closure.
- Level of internal audit validation correlates to control risk.
- Issue status reporting to the board or audit committee is accurate and timely.
- Status reporting also includes any changes in remediation ownership, target remediation dates, remediation plans, or repeat audit issues.
- Policy and procedures provide clear guidance.

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

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

   - Identify businesses, product lines, services, or functions and the activities and compliance issues within those areas that should be audited.
   - Develop risk profiles that identify and define the risk and control factors to assess and the risk management and control structures for each business, product line, service, or function.
   - Establish the process for grading or assessing risk factors for business units, departments, products, services, or functions, including time frames.
   - Describe how the process is used to set audit plans, resource allocations, scope of audits, and audit cycle frequency.
   - Implement audit plans through planning, execution, reporting, and follow-up.
   - Establish minimum documentation requirements to support scoring or assessment decisions and draw conclusions.
   - Define when overrides of risk-based scores or assessments are acceptable or necessary, including which level of authority approves overrides.
   - Provide for confirming the system regularly, i.e., annually or whenever significant changes occur within a department or function.

2. Review the bank's audit universe and supporting documents to determine whether it

   - represents all of the bank's auditable entities.
   - is based on a current inventory of all bank's material processes, product lines, services, and functions.
   - defines an IT audit universe that contains an inventory of the bank's data, application, operating systems, technology, facilities, and personnel.

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

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

5. If audit management has overridden risk-based audit schedules, discuss justifications with the chief auditor.

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

Objective: To determine whether the bank's fiduciary audit complies with 12 CFR 9.9 (national banks) or 12 CFR 150.440 (FSAs).

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

1. Determine whether the bank has fiduciary powers and engages in fiduciary activities. If so, proceed with steps 2 through 3 by reviewing previously requested materials.

2. Determine appropriateness of fiduciary audit coverage. Determine whether the following conditions apply:

   - The audit of fiduciary activities is accomplished in an annual audit or multiple discrete audits (aka continuous audit system).
   - The fiduciary audit is undertaken at the direction of the fiduciary audit committee in accordance with 12 CFR 9.9(a) and (b) for national banks or 12 CFR 150.470 for FSAs.
   - The fiduciary audit is conducted by independent and qualified persons in compliance with professional auditing standards (i.e., GAAS) and applicable OCC standards.
   - The bank's audit risk assessment and audit plan appropriately reflect all significant fiduciary activities.
   - The fiduciary audit
     – encompasses review of all significant fiduciary activities.
     – determines whether internal control policies and procedures provide reasonable assurance that the bank is
       ▪ administering fiduciary activities in accordance with applicable law.
       ▪ properly safeguarding fiduciary assets.
       ▪ accurately recording transactions in appropriate accounts in a timely manner.
     – determines the effectiveness of bank risk management and compliance function activities in managing fiduciary risk.

3. If the national bank maintains CIFs, verify that an audit was performed at least once during each 12-month period in accordance with 12 CFR 9.18(b)(6).

Objective: To determine the adequacy, effectiveness, and quality of the bank's directors' examination.

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

1. Determine whether the bank's bylaws, articles of association, or charter require the bank board to have independent parties periodically review and report on certain aspects of the bank's books and records, including policies and procedures (e.g., require a director's examination). (Updated version 1.1)

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

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

   - substantively test financial integrity.
   - reconcile accounts.
   - verify assets.
   - complete internal control questionnaires and assess control risk.
   - assess the quality of loans and investments.
   - verify some or all call report data.
   - review MIS.
   - confirm the bank's compliance with laws, regulations, and internal policies.
   - review acquisition and merger activities.
   - review new products and services.

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

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

5. Determine whether the board determined that independent parties selected to perform the directors' examination possessed (Updated version 1.1)

   - sufficient knowledge and understanding of banking.
   - knowledge and understanding of the bank's operations and activities.
   - ability to apply GAAP and auditing standards.
   - familiarity with the bank's information systems and technology.

Outsourced Internal Audit

Note: If performing a centralized third-party audit review, examiners should contact the relevant ADCs, EICs, or portfolio managers and discuss the scope of the review. In addition to the previously mentioned information, also obtain and review the supervisory strategy, EIC scope memorandum (if applicable), and previous ROE and OCC database summary comments for each of the banks included in the centralized review.

Objective: To determine the adequacy of board and management oversight of the bank's internal audit outsourced activities.

1. Review the outsourcing arrangement contract(s) between the third party and bank and determine its adequacy to address the following:

   - Defines the expectations and responsibilities under the contract for both parties.
   - Sets the scope, frequency, and fees to be paid for work to be performed by the outside third party.
   - Describes responsibilities for providing and receiving information, such as the type and frequency of third-party reporting to the bank chief auditor, senior management, and audit committee or the bank board about the results and status of work.
   - Establishes protocol for changing the terms of the engagement, especially for expansion of audit work if significant issues arise, as well as stipulations for default and termination of the contract.
   - States that internal audit reports are the property of the bank and specifies ownership of internal audit work papers. If the third party retains ownership of the work papers, the contract should stipulate that the bank will be provided copies of related work papers it deems necessary and that bank-authorized employees will have reasonable and timely access to third-party work papers.
   - Notes that the third party's internal audit activities are subject to OCC review and that examiners will be granted full and timely access to all related outsourced internal audit reports, audit programs, audit work papers, and memorandums and correspondence prepared by the third party.
   - Specifies the locations of, and how long (generally seven years) the third party will retain, outsourced internal audit reports and related work papers. If the work papers are in electronic format, the agreement should also address third-party maintenance of proprietary software to facilitate bank or examiner reviews of work papers.
   - Establishes processes (arbitration, mediation, or other means) for resolving disputes, as well as indemnification provisions for determining who bears the cost of consequential damages arising from errors, omissions, and negligence.
   - States that the third party will not perform management functions, make management decisions, or act or appear to act in a capacity equivalent to a member of bank management or a bank employee.
   - As applicable, states the third party will comply with AICPA, PCAOB, SEC, or other regulatory independence standards. (Updated version 1.1)

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

   - Available third-party services (including specialized areas) and work arrangements.
   - Costs and benefits of third-party services to be provided.
   - Ability and flexibility of the third party to perform the services in a timely manner and maintain the confidentiality of bank data.
   - Experience level, technical expertise, and credentials of third-party staff (including specialized areas such as IT, international, trust, compliance and capital markets).
   - Notifications of any changes in third-party processes, staffing, or other changes affecting assigned staff.
   - Third party's approach for conducting outsourced internal audits (e.g., risk-based or traditional, use of audit tools and audit technology).
   - Reference checks.
   - Third party's internal quality control processes (peer review and quality assurance).
   - Discussions of third-party independence, objectivity, integrity, and conflict of interest standards (such as AICPA, IIA, PCAOB, and SEC standards) applicable to the engagement.
   - Contingency plans for terminating the relationship in an effective manner.

Objective: To determine the adequacy and the reliability of work performed by the outsourced internal audit third party.

1. Arrange a meeting with the third party and discuss the third party's outsourced internal audit program. Consider the following:

   - Third party's understanding of the bank's risk profile and business.
   - Third party's sampling techniques for testing internal controls.
   - Third party's training program for its audit staff.
   - Communication with and reporting to the bank board, audit committee, and management.
   - Whether the third party's audit procedures are customized for each bank client or are generic.
   - Third party's method for reviewing internal controls.
   - Methods used to structure third-party contracts or agreements.
   - How the third party maintains independence. (Updated version 1.1)
   - Work paper documentation standards.

2. Determine how the bank and third party address internal control weaknesses or other matters noted by the third party during internal audits. Consider whether

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

3. Review outsourced internal audit reports issued and a sample of outsourced internal audit work papers to determine their adequacy and preparation in accordance with the audit program and the outsourcing agreement for the bank. Determine whether

   - work program steps, calculations, or other evidence support the audit's objectives, scope, procedures, and conclusions set forth in the outsourced internal audit reports. Consider
     - procedures performed.
     - testing and sampling methods used.
     - adequacy of sampling techniques used.
     - risk and control assessments.
     - approval of the chief auditor.
     - independence from external audit activities.
   - the scope of the outsourced internal audit procedures and work is adequate in light of risk and control assessments for the area audited.
   - the work program and audit reports adequately document material findings, including root causes of significant weaknesses, and whether follow-up on noted weaknesses and committed corrective action is adequate.
   - examiners, as a result of centralized outsourced audit reviews, perform additional testing or validation of the internal audit program at the individual bank level.

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

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

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

6. If performing a centralized third-party audit review, discuss findings from previously mentioned steps with the third party and do the following:

- Draft a memorandum summarizing the results of the centralized outsourced audit review. The memorandum should address the following issues as they pertain to each individual bank:
  - Adequacy of the third party's work paper documentation.
  - Reliance of the audit work performed by the third party.
  - Evaluation of the third party's work, including the scope and timing of procedures, extent of testing, and basis of conclusions.
  - Recommendations to enhance the third party's audit program.
  - Follow-up needed on any deficiencies noted and corrective actions.
  - Recommended updates to OCC audit review strategy or scope for individual banks.
- Distribute the memorandum, customized as warranted, to each EIC of banks for which the third party performs outsourced internal audit work.
- Bank EICs or portfolio managers should do the following:
  - Use the memorandum to set the scope of and gain efficiencies in their bank examination.
  - Discuss centralized outsourced audit review findings with the bank board or audit committee and management.
  - Validate board and management oversight of the bank's internal audit program during the on-site examination, using appropriate objectives and steps from the internal audit examination procedures in this booklet.
  - Undertake additional testing or review of internal audit work papers, if desired or warranted, at the bank level during on-site examinations or other supervisory activities during a supervisory cycle. Examiners should base that decision on events occurring since the third-party review was performed and any other matters that come to their attention during supervisory activities (e.g., high-risk areas and new products and services).

7. Determine, by discussion with the chief auditor and the third party, whether the bank and its third party have discussed and determined that applicable independence standards are being met. Examiners may want to provide bankers a copy of appendix F, "External Auditor Independence Worksheet," to help them assess external auditor independence. Consider the following:

   - If the third party is an IPA who does not also perform the bank's financial statement audit, have any potential conflicts of interest been properly addressed?
   - If the third party is part of or in a related organization to the bank's external audit firm, do the entities have adequate segregation?[167]
   - If the third party is a registered public accountant who also performs the bank's financial statement audit and the bank's securities are registered with the OCC, cite a violation of 15 USC 78j-1(g) or 17 CFR 210.2-01(c)(4).

[167] Examiners should gain confirmation from the EIC or OCC legal counsel of the third-party independence in these situations, taking into account the legal structure of the third party.

8. Determine whether publicly registered banks and banks subject to 12 CFR 363 comply with the SEC's independence regulation regarding internal audit outsourcing services by considering whether the following conditions are met:

   - The public accountant
     - does not act or appear to act in a capacity equivalent to a member of bank management or as a bank employee.
     - does not provide more than 40 percent of the total hours spent (by the bank, the accountant, or anyone else) on internal audit matters related to internal accounting controls, financial systems, financial statements, and matters affecting financial statements. Banks with less than $200 million in total assets are exempt from the 40 percent limit.
   - The bank
     - acknowledges, preferably in writing to the third party and the bank's audit committee or board, its responsibility to establish and maintain an effective system of internal accounting controls.
     - designates a competent bank employee or employees, preferably within senior management, to be responsible for the internal audit function.
     - determines the scope, risk, and frequency of internal audit activities, including those to be performed by the third party.
     - evaluates the findings and results arising from internal audit activities, including those performed by the third party.
     - evaluates the adequacy of the audit procedures performed and the findings resulting from performance of those procedures by, among other things, obtaining reports from the third party.
     - does not rely on the third party's work as the primary basis for determining the adequacy of the bank's internal controls.

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

   - If appropriate, request through the bank that additional work papers be made available or meet with the third party to discuss the concerns.
   - If significant concerns remain unresolved, contact the OCC district accountant or the Chief Accountant's Office, district counsel or the Chief Counsel's Office, and discuss measures to be taken.

10. If the OCC determines that it cannot rely on the third party's work, discuss that assessment with the bank board, bank management, and the affected party before finalizing the ROE.

External Audit Function

Objective: To determine the adequacy of the bank board oversight of the bank's external audit function.

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

   - Formal approval of the external audit program and schedule, or reasons supporting any decision to forgo an external audit program.
   - Formal approval of engagement or written agreements before onset of work.
   - The monitoring of external audit reports to determine whether the approved external audit program and schedule are being followed.
   - The results of any vote taken regarding external audit.
   - Confirmation that the audit committee reviews external audit reports with management and the external auditors in a timely manner.
   - Discussion of the external auditor's independence.
   - Approval of written criteria to evaluate the performance of the third-party external audit services based on a risk assessment and mitigating controls.

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

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

4. Determine whether the bank board or its audit committee identifies risks associated with the third-party external auditor and any necessary mitigating controls. If the PCAOB has issued a report on the bank's external audit firm, determine the board or audit committee consideration of this information and decisions.

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

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

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

8. If the external auditor is using the work of internal auditors, determine whether external auditor communications with the bank board or its audit committee include the evaluations of using internal auditors' work.

Objective: To review the independence and objectivity of those who provide the external audit function.

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

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

   - Has the audit committee pre-approved all audit, review, and attestation engagements, including any non-prohibited non-audit services? (17 CFR 210.2-01(c)(7))
   - Has any partner, principal, or shareholder of the audit firm who was a member of the audit engagement team at any point during the audit engagement period earned or received compensation based on the performance of, or procuring of, engagements with the bank or its affiliates to provide any products or services other than audit, review, or attestation services? (17 CFR 210.2-01(c)(8))
   - Has a PCAOB inspection report pertaining to the firm raised concerns about the independence or objectivity of the external auditor?

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

   - Employment relationships between the bank and the IPA, such as the following:
     – The IPA being employed by the bank or serving on the bank board or in a similar management capacity before a one-year cooling-off period is completed.
     – Employments of the accountant's close family members or a former employee of the audit firm at the bank who can influence the bank's financial records.
     – A former bank officer, director, or employee becoming an employee or a partner in the audit firm and participating in the audit.
   - Direct or material indirect financial interests between the accountant and the bank, such as the following:
     – Investments in the bank or bank investment in the accounting firm.
     – Bank acting as underwriter for the auditor.
     – Having loans to or from an audit client except for certain consumer loans, such as mortgages or auto loans.
     – Maintaining savings, checking, brokerage, or similar accounts in excess of insured amounts.
     – Broker/dealer accounts.
     – Futures commission merchant accounts.
     – Credit card accounts with a balance greater than $10,000.

  - Holding individual insurance policies, and for the firm, professional liability policies.
  - Investing in an investment company that is in the same investment company complex as the audit client.
- The IPA acting, temporarily or permanently, as a director, officer, or employee of the bank, or performing any decision-making, supervisory, or ongoing monitoring function for the bank.
- The accountant providing non-audit services to the bank, such as the following:
  - Bookkeeping.
  - Financial information systems design and implementation.
  - Appraisal or valuation services, fairness opinions, or contribution-in-kind reports.
  - Actuarial services.
  - Internal audit outsourcing services.
  - Management functions or human resources.
  - Broker/dealer, investment advisor, or investment banking services.
  - Legal services and expert services unrelated 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.
- The external auditors compromising their independence by performing any of the bank's internal audit work. If so, perform the second objective under the "Outsourced Internal Audit" section to determine that the auditor's independence is not compromised and is maintained in accordance with established rulings and guidelines.
- The professional reputation of the auditors.

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

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

   - Level of education attained, including any training in specialized areas such as capital markets, information systems, fiduciary activities, and subsidiary activities.
   - Significant banking industry audit experience, including specialized areas.
   - Certification as a chartered bank auditor, certified internal auditor, etc.
   - Commitment to a program of continuing education and professional development.

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

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

- If significant concerns are unresolved, discuss the issues with the bank board, bank management, and the affected party.
- Contact OCC staff (district accountant, Chief Accountant's Office, district counsel, or Chief Counsel's Office as appropriate) before finalizing the ROE.

Objective: To determine the extent of and reliability of work performed by the external auditors.

1. Obtain copies of the following:

   - Engagement letters.
   - 12 CFR 363 annual reports or other audit reports issued to the bank by the external auditor.
   - Letters, communications, and other correspondence pertaining to external audits issued to or by bank management.

2. Determine whom bank engages to perform the bank's external audit and the type of external audit performed:

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

3. If the bank is subject to 12 CFR 363, determine whether it has engaged an IPA to audit and report on its financial statements in accordance with the applicable auditing standards.

4. If the bank's securities are registered with the OCC or it is a public entity, determine whether it has engaged an IPA registered with the PCAOB (SOX section 102(a)).

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

   - in writing.
   - within 15 days of the event.
   - giving reasons for the event.

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

- Audit planning methodologies, risk assessments, sampling techniques, and (if applicable) 12 CFR 363 control attestation.
- How much the external auditor relies on the work of internal auditors.
- The extent of the external auditor's assessment and testing of financial reporting controls and how much the external auditor relies on those controls when auditing financial reports.
- Current examination and external audit results or significant findings.
- Upcoming external audit and examination activities.
- Reports, management letters, and other communications issued by the external auditors to the bank.
- Assigned audit staff experience and familiarity with banking and bank auditing, particularly in specialized areas.
- Any other pertinent information.

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

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

8. Determine the type of opinion rendered by an audit of the bank's financial statements. If other than an unqualified opinion has been issued, discuss with the external auditor and determine the facts and circumstances that led to the opinion.

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

   - Communication of matters related to internal controls over financial reporting noted in the audit. This communication is issued when the auditor notes reportable conditions identified as material weaknesses or significant deficiencies in internal controls over financial reporting.
   - Communication with the audit committee. This communication may be either oral or written and generally includes the following:
     – Planned scope and timing of audit, including extent of use of the work of the bank's internal auditors.
     – Significant risks identified during auditor's risk assessment procedures.
     – Auditor responsibilities under the applicable auditing standards.
     – Views about qualitative aspects of the entity's significant accounting practices, including accounting policies, accounting estimates, and financial statement disclosures.
     – Uncorrected misstatements.

  - Auditor responsibility for other information in documents containing audited financial statements.
  - Disagreements with management.
  - Consultation with other accountants.
  - Significant issues discussed with management before retention.
  - Significant difficulties encountered in performing the audit.
  - Written representations.

  If the bank is subject to 12 CFR 363, before filing of annual reports, an IPA must also report to the audit committee the following matters as required by 12 CFR 363.3(d):

  - All critical accounting policies and practices.
  - All alternative treatments of financial information within GAAP that have been discussed with bank management, including ramifications of the use of such alternate disclosures and treatments, and the treatment preferred by the firm.
  - Other written communications between the IPA and bank management, such as management letters or schedules of unadjusted differences.

- Confirmation of audit independence (required for banks subject to filing and reporting requirements of 12 CFR 11 and 12 CFR 16, publicly registered holding companies subject to SEC rules, and banks with $500 million or more in total assets that are subject to 12 CFR 363.3 and did not satisfy the audit requirements at the holding company level). For affected banks, auditors must disclose, in writing, all relationships with the bank and its related entities that could affect the auditor's objectivity. Auditors must also confirm they are independent in accordance with SEC requirements and discuss their independence with the bank's audit committee.

10. If any of the previously mentioned communications that are required to be in writing are not in writing, discuss with the bank board, its audit committee, and external auditor to determine why written communications were not requested or provided.

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

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

13. Consider asking to review appropriate external audit work papers if any of the following circumstances exist:

    - Unexpected or sudden changes in the bank's external auditor. Examiners should have discussions with the previous and current external auditor before embarking on a

work paper review. If the discussions raise unanswered questions that might be addressed in the work papers, then a work paper review may be warranted
- Significant changes in the bank's external audit program. Examiners should contact the external auditor to discuss these changes and determine whether a review of work papers is warranted.
- Significant and unexpected changes in accounting or operating results. Examiners should discuss such changes with the external auditor and determine whether a review of work papers is warranted.
- Issues that affect the bank's safety and soundness. There may be instances when the external auditor raises safety and soundness concerns, or when examiners or internal auditors discover safety and soundness concerns in areas normally within the scope of an external audit program. In such cases, examiners should obtain information from the bank, discuss the issues with bank management and the external auditor, and consider reviewing work papers related to those matters or findings.
- Issues about the independence, objectivity, or competence of the external auditor.
- Recalcitrant external audit firm or staff.

14. If reviewing external audit work papers, determine (and discuss with the external auditor as warranted) whether selected work papers contain information documenting whether

    - a written audit program (including appropriate audit procedures) was in place for the area audited.
    - work was adequately planned and supervised.
    - sufficient understanding of internal control was obtained to plan the audit and determine the nature, timing, and extent of tests to perform.
    - audit procedures obtained sufficient competent evidential material to provide a reasonable basis for the audit opinion or conclusion about
        - sampling and testing bases and results.
        - risk assessments.
        - whether accounting records agree or reconcile with financial statements or other information reported on.
        - supporting documentation of audit findings or issues that in the auditor's judgment are significant, actions taken to address the issues, and the basis for the conclusions reached.

    Additional or tailored procedures may be necessary depending on the facts and circumstances of why review of external auditor work papers was necessary.

15. If, after reviewing external audit work papers, significant concerns remain about the adequacy of external audit, the effectiveness of internal controls, or the accuracy of the audit opinion rendered, consider whether to perform verification procedures for the applicable areas of concern. Verification procedures are required in certain situations. Refer to the "OCC Assessment of Audit Functions" section of this booklet for more information.

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

- the bank perform verification procedures, or
- the bank board or its audit committee ask its external auditor or other independent third party to perform verification procedures.

If one of these two alternatives is chosen, follow up with a review of applicable work papers to determine whether identified supervisory issues are resolved in a timely manner. (Updated version 1.1)

Conclusions

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

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

The board of directors (has, has not) implemented and (does, does not) effectively oversee an external audit function that is appropriate for the bank and that (complies, does not comply) with established statutory and regulatory requirements. (Updated version 1.1)

The quality of the bank's audit function rating is (strong, satisfactory, insufficient, or weak).

Objective: To determine, document, and communicate overall findings and conclusions regarding the examination of internal and external audits.

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

   - Audit stature and ability of audit to effect change in the organization.
   - Ability and effectiveness of the bank's audit processes to assess and detect risk in bank operations.
   - Adequacy of audit policies, procedures, programs, and the board's or audit committee's oversight.
   - Whether internal and external auditors and third parties operate in conformance with established policies, standards, rules, and regulations.
   - Adequacy and availability of information about or generated by the audit function and provided to management and the bank board or its audit committee.
   - Significant areas of weaknesses identified by internal or external audits and management's progress in correcting those weaknesses.
   - Internal or external audit report findings not acted on by management, as well as any other concerns or recommendations resulting from the review of audit functions.
   - Recommended corrective actions, if applicable, and management's commitments.

Summary of Risks Associated With Internal and External Audit Functions				
Risk category	**Quantity of risk** (Low, moderate, high)	**Quality of risk management** (Weak, insufficient, satisfactory, strong)	**Aggregate level of risk** (Low, moderate, high)	**Direction of risk** (Increasing, stable, decreasing)
Operational				
Compliance				
Strategic				
Reputation				

2. Assignment of an overall audit rating. Determine how the quality of the audit function affects the aggregate level and direction of OCC risk assessments. Examiners should refer to the risk assessment systems guidance in the "Community Bank Supervision" and "Large Bank Supervision" booklets. (Updated version 1.1)

3. Discuss examination findings with bank management, including violations, deficient practices, and conclusions about risks and risk management practices. If necessary, obtain commitments for corrective action. (Updated version 1.1)

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

   - The adequacy of audit policies, processes, personnel, control systems, overall audit programs, and board or audit committee oversight.
   - Significant problems discerned by the auditors that have not been corrected.
   - Any deficiencies or concerns reviewed with management, any corrective actions recommended by examiners, and management's commitment to corrective actions.

5. Consider citing a violation of 12 CFR 30 (appendix A or appendix D) if audit is rated weak because of significant deficiencies in the internal audit function or its oversight, if MRAs pertaining to internal audit are being issued, or if a recommended enforcement action includes article(s) related to internal audit. (Updated version 1.1)

6. Document recommendations for the supervisory strategy (e.g., what the OCC should do in the future to effectively supervise the bank's internal and external audit functions, including time periods, staffing, and workdays required). Include recommendations about the scope of the next audit review and recommend whether audit findings should change the scope of other supervisory activity reviews. (Updated version 1.1)

7. Update the OCC's supervisory information system and any applicable ROE schedules or tables. For fiduciary, IT, and consumer compliance examinations, update the applicable audit component rating factor and communicate audit findings and rating to the

appropriate EIC for incorporation into other rating systems (e.g., UITRS, URSIT, or Consumer Compliance Rating System). (Updated version 1.1)

8. Update, organize, and reference work papers in accordance with OCC policy.

9. Appropriately dispose of or secure any paper or electronic media that contain sensitive bank or customer information. (Updated version 1.1)

Appendixes

Appendix A: Laws, Regulations, and Policy Guidance

The following laws and regulations[168] establish minimum requirements for internal and external audit programs and are referenced throughout this booklet:

- 12 CFR 9.9(a) and 12 CFR 9.9(b) establish audit requirements for the fiduciary activity of national banks. 12 CFR 9.9(c) provides the requirements for a national bank's fiduciary audit committee. 12 CFR 9.18(b)(6) establishes an audit requirement for banks that maintain CIFs.

- 12 CFR 19 establishes practices and procedures for the removal, suspension, and debarment of accountants for national banks performing section 36 of the Federal Deposit Insurance Act (FDI Act)[169] and 12 CFR 363 audit services, including attestation services. 12 CFR 19 includes standards for good cause for removal, suspension, or debarment. (Updated version 1.1)

- 12 CFR 21.21 establishes requirements for banks to have a board-approved ongoing Bank Secrecy Act compliance program that includes, in part, provisions for independent testing by bank personnel or outside parties. (Updated version 1.1)

- 12 CFR 30, appendix A, establishes operational and managerial standards for internal audit systems for FDIC-insured banks. The regulation outlines the responsibilities of the bank board related to the bank's internal control systems and the internal audit program. Appendix A to 12 CFR 30 is pursuant to sections 36 and 39 of the FDI Act. (Updated version 1.1)

- 12 CFR 30, appendix D codifies the three lines of defense risk framework. Generally, FDIC-insured banks with average total consolidated assets of $50 billion or greater should have a risk governance framework that includes an internal audit function that complies with the guidelines contained in 12 CFR 30, appendix D (heightened standards). Covered banks should refer to the heightened standards for further information on the guidelines applicable to a covered bank's lines of defense, including definitions of relevant terms.

- 12 CFR 150.440–460 establish audit requirements for the fiduciary activities of FSAs. 12 CFR 150.470 provides the requirements for an FSA's fiduciary audit committee. 12 CFR 150.260(b) requires that FSAs that administer CIFs comply with the requirements of 12 CFR 9.18, which include specific audit requirements as noted above.

[168] For complete details, refer to the full text of published laws and regulations.

[169] Section 36(g)(4)(A) of the FDI Act (12 USC 1831m(g)(4)(A)) empowers the OCC to remove, suspend, or bar an independent public accountant from performing audit services required by section 36 at institutions the OCC supervises.

- 12 CFR 363, "Annual Independent Audits and Reporting Requirements," applies to insured depository institutions having $500 million or more in total consolidated assets. 12 CFR 363 establishes requirements, some of which may be satisfied at the holding company level, for independent financial statement audits; timing, contents, and types of management and auditor reporting; and the board's audit committee structure and responsibilities. External auditors engaged by banks subject to 12 CFR 363 must follow the most stringent independence requirements set by the AICPA, the SEC, and the PCAOB. (Refer to appendix C, "12 CFR 363 Reporting," for additional information). 12 CFR 363 is pursuant to section 36 of the FDI Act (12 USC 1831m).

- Banks that are public companies are subject to additional requirements with respect to their audits and audit committees.[170] The federal securities laws and regulations of the SEC establish standards and procedures for registered public accounting firms that audit public companies. The laws and regulations also require public companies to make disclosures about their audit committees. For public companies with shares listed on a securities exchange, the regulations and rules of the exchanges establish requirements for independent financial statement audits; qualifications and independence of public accountants; and qualifications and responsibilities of audit committees.[171]

In addition, the federal financial regulatory agencies have issued several interagency policy statements and an advisory related to internal and external audit functions:

- "Interagency Advisory on External Audits of Internationally Active U.S. Financial Institutions," issued with OCC Bulletin 2016-2.

- "Interagency Advisory on the Unsafe and Unsound Use of Limitation of Liability Provisions in External Audit Engagement Letters," issued with OCC Bulletin 2006-7.

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

- "Interagency Policy Statement on External Auditing Programs of Banks and Savings Associations: External Audit," issued with OCC Bulletin 1999-37.

- "Interagency Policy Statement on Coordination and Communication Between External Auditors and Examiners," issued with Banking Bulletin 1992-42.

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

[170] The bank is a public company if it has a class of securities registered with the SEC or OCC under section 12 of the Securities Exchange Act of 1934.

[171] SOX added the audit requirements in section 10A of the Securities Exchange Act of 1934, 15 USC 78j-1. Also refer to 17 CFR 210, 229 and 240.

Appendix B: Types of Audits and Control Reviews

The following are the audit types most typically performed at banks.

Operational Audits

Operational audits generally include procedures to test the integrity of accounts, regulatory reports, MIS, and other aspects of operations as part of the review of a specific department, division, or area of the 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 the bank significantly relies on IT for transaction testing, record storage, and communications, IT audit coverage 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

Financial audits are audits of the bank's financial statements, a specific account, or a group of accounts within the financial statements. The purpose of these audits 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. IPAs perform this type of audit primarily to render an opinion about whether the financial statements are presented fairly and in accordance with GAAP. An internal auditor may assist the external auditors during an annual financial statement audit. Refer to the "Types of External Auditing Programs" section of this booklet for more information.

Cybersecurity Audits

Cybersecurity audits assess the bank's oversight and risk management associated with cyber threats and attacks. The audit should use an industry cybersecurity control framework (i.e., National Institute of Standards and Technology or COSO) as a basis for audit scope and objective, taking into account the bank's risk and complexity. The bank's cybersecurity environment also determines the impact of third-party relationships. The audit should validate that its cyber risk management oversight, threat intelligence and collaboration, controls, external dependency management, and incident management and resilience are commensurate with the bank's risk and complexity. The audit should review the bank's process for determining when and how management reviews the bank's cybersecurity risk profile to determine if the review process sufficiently addresses changes to the bank's business, operations, and threat environment.

Fiduciary Audits

The OCC requires that banks arrange a suitable audit of all significant fiduciary activities under the direction of their fiduciary audit committees at least once during each calendar year (in accordance with 12 CFR 9.9(a) for national banks and 12 CFR 150.440(a) for FSAs).

As an alternative to an annual audit (in accordance with 12 CFR 9.9(b) for national banks and 12 CFR 150.440(b) for FSAs), a bank may adopt a continuous audit system under which it arranges for discrete audits of each significant fiduciary activity at an interval commensurate with the risk of the activity. A fiduciary audit should ascertain whether the bank's internal control policies and procedures provide reasonable assurance that the bank is administering fiduciary activities in accordance with applicable law, properly safeguarding fiduciary assets, and accurately recording transactions in appropriate accounts in a timely manner.[172] The fiduciary audit should also include the review of the bank's risk management and compliance function activities to assess their effectiveness in managing fiduciary activity risk. (Updated version 1.1)

Collective Investment Fund Audits

Bank fiduciaries that offer one or more CIFs are required under 12 CFR 9.18(b)(6)(i) to arrange an annual audit of each CIF by auditors that are responsible only to the board. This is principally a financial statement audit that confirms the existence and values of the CIF's holdings. 12 CFR 9.18(b)(6)(ii) requires that such banks prepare a financial report for each CIF based on this audit. The financial report discloses fees and expenses and specific information about the fund's investments and activities at least once during each calendar year. In light of the importance of the annual CIF financial report to fund participants, bank audit, compliance, and risk management, it is a best practice for a bank to make arrangements for the audits of its CIFs no later than 90 to 120 days following the end of the fund's fiscal year. Absent extenuating circumstances, it would be an unsafe and unsound banking practice to delay a CIF's annual audit beyond this point.

It would be difficult for the internal auditor function, including outsourced activities, to have the necessary independence to perform a 12 CFR 9.18(b)(6) audit. The internal audit function's assurance activity, encompassing the bank's fiduciary activities, would eliminate their independence for conducting the CIF audit. To provide appropriate independent assurance, the CIF audit should not be performed by the bank's internal audit function or by the same third-party firm engaged to perform all or part of the bank's fiduciary audit activities. (Updated version 1.1)

Regulatory/Compliance Audits

Regulatory compliance audits determine whether the bank is complying with applicable laws and regulations. While applicability of specific audits for regulatory compliance may differ from one bank to another, there are some common compliance audits, such as consumer compliance, Bank Secrecy Act/anti-money laundering, and Gramm–Leach–Bliley Act (GLBA). (Updated version 1.1)

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 the bank's compliance

[172] These are requirements for FSAs under 12 CFR 150.450 and are viewed as a safe and sound banking practice for national banks.

management system, enables the bank board and senior management to monitor the effectiveness of the bank's compliance program. The compliance audit's formality and structure depend on the 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.

Regulatory compliance audits should address all bank products and services, all aspects of applicable operations, all departments (such as trust and private banking), and all delivery channels. The audit should appropriately address compliance risk exposure, allowing for more frequent and intense reviews of high- and moderate-risk areas.

For details on regulatory audit or control tests, refer to FFIEC and OCC booklets related to specific areas (e.g., the *FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual* or the "Information Security" booklet of the *FFIEC IT Examination Handbook* and booklets in the *Consumer Compliance* series of the OCC *Comptroller's Handbook*). (Updated version 1.1)

Audits of automated clearing house (ACH) rules compliance are required by NACHA[173] to be completed for each calendar year. Refer to the "Retail Payment Systems" booklet of the *FFIEC IT Examination Handbook.* (Updated version 1.1)

Heightened Standards Assessments

A heightened standards assessment evaluates the compliance of certain large banks with the OCC's heightened standards.[174] Internal audit for banks covered by 12 CFR 30, appendix D, should conduct an annual independent assessment of the design and ongoing effectiveness of the risk governance framework. The independent assessment should include a conclusion on the covered bank's compliance with the standards set forth in the heightened standards guidelines. An external assessment of internal audit or non-internal audit assurance may be used for internal audit function elements of the risk governance framework. Refer to the "Quality Assurance and Improvement Programs" section of this booklet for more information on external assessments.

Information Technology Audits

IT audits assess the controls, accuracy, and integrity of the bank's information systems processing and technology infrastructure.[175] 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 IT. The bank's internal auditor, external auditor, a service provider's internal auditor, a third party, or any combination of these can perform

[173] NACHA (formerly the National Automated Clearing House Association) is the body that establishes the rules and procedures governing the exchange of automated clearing house payments. Refer to NACHA 1.2.2, "Audits of Rules Compliance."

[174] Refer to 12 CFR 30, appendix D, II.C.

[175] Refer to the *FFIEC IT Examination Handbook* for examination procedures specifically for IT audits.

these assessments. IT audit often includes both targeted audits of IT functions and integrated reviews of IT functions as part of other operational audits, while taking into account service provider audits.

IT audits should address the risk exposures inherent in IT systems and applications throughout the bank 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 sensitive information.
- IT risk management.

IT audits might also include a review of technology system architecture and network management, end-user reports, payment systems, and service provider activities.

The audit scope usually validates the confidentiality, integrity, and availability 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 or automated reports, or "through the computer," by using independent audit software to independently test the production processing environment.

Within the category of IT audits, banks may also perform a GLBA audit. To meet compliance with the "Interagency Guidelines Establishing Information Security Standards"[176] portion of the GLBA, banks must provide an annual report to the bank board or an appropriate committee of the bank board. This annual report includes results of key controls, systems, and procedures of the information security program over customer information and customer information systems. These control tests should be conducted or reviewed by independent third parties or staff independent of those who develop or maintain the security programs.

[176] The "Interagency Guidelines Establishing Information Security Standards" (guidelines) set forth standards pursuant to section 39(a) of the Federal Deposit Insurance Act (12 USC 1831p-1) and sections 501 and 505(b) of the GLBA (15 USC 6801 and 15 USC 6805(b)). These guidelines address standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. These guidelines also address standards for the proper disposal of consumer information, pursuant to sections 621 and 628 of the Fair Credit Reporting Act (15 USC 1681s and 15 USC 1681w).

Service Organization Control Audits

SOC audits report on controls at a service provider that are likely to be relevant to clients' systems of internal controls. There are several kinds of SOC audits.

- SOC 1: Report on Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting. SOC 1 audits, type 1 or type 2, are conducted in accordance with AICPA SSAE 18, "Concepts Common to all Attestation Engagements." SOC 1 reports on controls placed in operation, describes controls in the audit, whether such controls are suitably designed to achieve specific control objectives, and whether the controls have been in operation as of a specific date. (Updated version 1.1)
- SOC 2: Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy. SOC 2 audits, type 1 or type 2, are conducted in accordance with the AICPA guide "Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy."
- SOC 3: Trust Services Report for Service Organizations. These are general reports that can be freely distributed as a marketing tool. They are designed to meet the needs of users who need assurance about the controls at a service organization that affect the security, availability, and processing integrity of the service organization's systems for processing users' information, and assurance about the confidentiality or privacy of that information, but do not have the need for or the knowledge necessary to make effective use of an SOC 2 report.

Banks should take steps to evaluate SOC audits to determine relevance in their audit programs. Type 2 reports are generally preferred, because type 1 reports do not address the operating effectiveness of controls or provide an opinion throughout a period of time. Industry organizations, such as the IIA, provide best practices on this subject that detail the internal auditor's responsibility to obtain sufficient and appropriate audit evidence when using the services of one or more service providers.

Directors' Examinations

(Section updated version 1.1)

The bylaws, articles of association, or charters of many banks require that the directors have independent parties periodically review certain aspects of the bank's books and records, including policies and procedures. In these cases, the board is responsible for determining that agreed-upon procedures adequately meet the bank's internal or external auditing needs.[177] 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. The bank's bylaws, articles of association, or charters may also require that directors or a directors' committee review the directors' examination report with the engaged consultant. After reviewing the findings of

[177] Refer to the "Types of External Audits" section of this booklet for more information.

this type of review, the board or audit committee draws its own conclusions about the quality of financial reporting and adequacy of internal controls.

Effective directors' examinations enable boards to form their own conclusion on the safety and soundness of the bank. The examinations normally focus on major risk areas and internal controls and ensure that all areas are adequately covered on a regular or rotational basis. A directors' examination provides information to enable the board to take action to address noted issues or problems. Directors' examinations should include a review of major bank acquisitions, along with new activities.[178] These examinations should substantially test financial integrity and internal controls and normally include

- account reconciliations.
- asset verification.
- completion of internal control questionnaires.
- quality assessment of loans and investments.
- verification of some or all call report data.
- review of MIS.
- checks for compliance with laws, regulations, and internal policies.

These reviews help ensure that management is following acceptable bank policies and procedures and management 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 GAAP and auditing standards and be familiar with the bank's information systems and technology.

Agreed-Upon Procedures

This type of review is carried out by an independent party engaged to perform specified or agreed-upon procedures and report findings.[179] The recipients of the report, mostly the bank board, form their own conclusions on the subject matter of the report. This review is not considered an audit. The independent party does not render an opinion or make any assertion about the subject matter. The AICPA standards govern third-party CPAs or audit firms in conducting agreed-upon procedures reviews and reporting. The independent parties can be CPAs, public accountants, certified internal auditors, certified bank auditors, certified information systems auditors, bank management firms, bank consulting firms, or other parties knowledgeable about the subject matter. Examples of agreed-upon procedures reviews include due diligence in buying a business, director's examinations, or financial forecasts.

[178] Refer to OCC Bulletin 2017-43.

[179] Refer to AICPA ASB SSAE No. 10, "Agreed-Upon Procedures Engagements."

Appendix C: 12 CFR 363 Reporting

Annual Independent Audit and Reporting Requirements

Following are the specific requirements of 12 CFR 363 on auditing, reporting, and audit committees. The requirements are applicable to all banks with $500 million or more in total assets. Banks below this asset threshold may choose to voluntarily comply with some or all of 12 CFR 363's requirements.

Reports to Regulators

Banks with $500 million or more in total assets must send the following reports to the FDIC and the appropriate OCC supervisory office:

- An annual report, due within 90 days after the fiscal year-end, consisting of the following:
  - Financial statements that include
    - comparative consolidated financial statements for each of the two most recent fiscal years prepared in accordance with GAAP and audited in accordance with GAAS by an IPA.
    - an audit report.
  - A management report that contains the following:
    - A statement of management's responsibilities for financial statements, establishing and maintaining an internal control structure and procedures for financial reporting, and complying with safety and soundness laws concerning loans to insiders and dividend restrictions.
    - Management's assessment of the effectiveness of the bank's internal control structure and procedures for financial reporting as of the end of the fiscal year (internal controls that safeguard assets, such as loan underwriting and documentation standards, must be considered) and the bank's compliance with designated laws and regulations during the most recent fiscal year.
  - A report by the IPA attesting to management's assertions regarding internal control structure and procedures for financial reporting.[180] The attestation is to be made in accordance with generally accepted standards for attestation engagements.

- Management letters and certain reports prepared for the bank, due within 15 days after they are received, that include the following:
  - Audit reports and any qualification to the audit reports.
  - Any management letter.
  - Any other reports, including attestation reports, from the IPA.
  - A notification of the selection, change, or termination of the bank's IPA, due within 15 days after the event. The report must include a statement of the reasons in sufficient detail for the examiner to evaluate the decision.

[180] 12 CFR 363.3(b) requires IPAs of an insured depository institution with total assets of $1 billion or more to examine, attest to, and report separately on the assertion of management. (Footnote updated version 1.1)

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

Unlike other banks, insured branches of foreign banks are not separately incorporated or capitalized. To determine whether 12 CFR 363 applies, an insured branch should measure claims on non-related parties reported on its Report of Assets and Liabilities of U.S. Branches and Agencies of Foreign Banks (form FFIEC 002). Most of the OCC-supervised FBOs, however, are not FDIC-insured or do not meet the requirements of 12 CFR 363.

The management report of the insured branch of a foreign bank should be signed by the branch's management official if the branch does not have a CEO or a chief accounting or financial officer. Because an insured branch of a foreign bank does not have a separate board of directors, the regulators do not apply the audit committee requirements of 12 CFR 363 to such branches. Any such branch, however, is encouraged to make a reasonable good faith effort to see that similar duties are performed by persons whose experience is generally consistent with 12 CFR 363 requirements for an institution the size of the insured branch.

Filing reports: Banks covered under 12 CFR 363, including branches of foreign banks, are required to file two copies of each required report at each of **two** locations—the appropriate OCC supervisory office and the appropriate FDIC regional office. Of the OCC's copies, one is maintained at the supervisory office, and the other is forwarded to the bank's portfolio manager. The exception to this rule is the IPA's peer review report, which is required to be filed only with the FDIC.

Disclosing reports: Annual reports required by 12 CFR 363 are available to anyone, from the bank, on request. The OCC may designate certain information as privileged and confidential, however, and such information may not be available to the public.

The peer review report is also publicly available. The list of clients subject to 12 CFR 363, however, is exempt from public disclosure.

Reports to IPAs

Every covered bank also must provide its IPA with copies of the following reports:[181]

- Most recent OCC examination report and related correspondence.
- Most recent Reports of Condition and Income or Report of Assets and Liabilities of U.S. Branches and Agencies of Foreign Banks (form FFIEC 002).
- Any supervisory memorandums of understanding, written agreements, requests for corrective action, notices of intent to commence an action, records of enforcement action taken, or notices of change in the bank's prompt corrective action capital category during the audit period.

[181] Refer to 12 USC 1831m(h), "Exchange of Reports and Information." Also refer to 12 CFR 363, appendix A.17, "Information to be Provided to the Independent Public Accountant."

Reports to the FDIC Only

IPAs for covered banks must file the following reports with the Washington office of the FDIC:

- A peer review report for each covered bank or, if no peer review has been performed, a statement of the IPA's enrollment in a peer review program. This report is due within 15 days of receipt, or before commencing any services under 12 CFR 363.
- A list of clients subject to 12 CFR 363, due at the IPA's option as a substitute for the peer review report or statement for each client.

Special Reporting Situations

Consolidated Reporting by Holding Company Subsidiaries

The chart at the end of this appendix summarizes the responsibilities of holding company member banks. To simplify, any bank that is a subsidiary of a holding company may, regardless of its size, file the audited consolidated financial statements of the holding company in place of separate financial statements, provided that the bank comprises 75 percent or more of the consolidated total assets of the holding company at the beginning of its fiscal year.

All other report and notice requirements of the 12 CFR 363 rule may be satisfied at the holding company level if the following conditions apply:

- The bank has total assets of less than $5 billion, or of $5 billion or more with a composite CAMELS rating of 1 or 2.
- The holding company provides the bank with comparable services and functions for other reports and notices required by 12 CFR 363, such as
  - preparing reports used by subsidiary national banks to meet 12 CFR 363 requirements,
  - having an audit committee that meets 12 CFR 363 requirements appropriate to its largest subsidiary bank, and
  - preparing and submitting reports on internal control and compliance with designated laws based on the activities and operations of all subsidiary banks.

Reporting by Insured U.S. Branches of Foreign Banks

Under the guidelines, contained in 12 CFR 363, appendix A, insured branches of foreign banks may satisfy the financial statement requirement by filing one of the following for each of its two most recent fiscal years:

- Audited balance sheets that also disclose information about financial instruments with off-balance-sheet risk.
- Audited call report schedules RAL and L of the Report of Assets and Liabilities of U.S. Branches and Agencies of Foreign Banks (form FFIEC 002).

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

The management report of the insured branch of a foreign bank should be signed by the branch's management official if the branch does not have a CEO or a chief accounting or financial officer.

Reporting by Merged or Consolidated Institutions

Insured banks that had more than $500 million in total assets at the beginning of their fiscal year but that no longer exist as a separate entity at the end of their fiscal year have no responsibility under this 12 CFR 363 rule to file reports due after the date they cease to exist.

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

Banks should consult with their OCC supervisory office concerning the statements and reports that would be required under such circumstances.

IPA Eligibility Requirements

The IPA must satisfy certain requirements to perform an audit or attestation for a covered bank. Specifically, the IPA must

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

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

Table 1: 12 CFR 363 Applied to Subsidiary Banks of Holding Companies

Insured depository institutions–subsidiaries of holding companies with total assets of	Audit committee requirements	Reporting requirements[a]
Less than $500 million	None.[b] (12 CFR 363.1(a))	None.[b] (12 CFR 363.1(a))
$500 million up to $1 billion	Committee must consist of outside directors, the majority of whom shall be independent of management.[c] (12 CFR 363.5(a)(2))	Annual report, including • audited financial statements, • audit report, and • management report. Requirement may be satisfied at the holding company level, provided certain conditions are met.
$1 billion up to $3 billion	Committee must consist entirely of independent outside directors and may be satisfied at the holding company level. (12 CFR 363.5(a)(1))	Same as for banks $500 million up to $1 billion, plus annual report must include IPA's report on the effectiveness of internal controls over financial reporting. Requirement may be satisfied at the holding company level, provided certain conditions are met.
More than $3 billion and less than $5 billion (12 CFR 363.5(b)) $5 billion or more and CAMELS composite rating of 1 or 2 (12 CFR 363.1(b)(2)(ii))	Committee must • consist entirely of independent outside directors, • include members with banking and related financial management expertise, • have access to its own outside counsel, and • not include large customers of the bank.[d] Requirements may be satisfied at the holding company level, provided certain conditions are met.[e]	
$5 billion or more and CAMELS composite rating of 3 or worse	Committee requirements same as above, but must be satisfied at the bank level.	Banks may submit holding company financial statements and audit reports, but all other reports listed above must be at the bank level.

a. Refer to 12 CFR 363 for further details on reporting requirements for each of these reports. Particular attention should be paid to 12 CFR 363.1, "Scope and Objectives," 12 CFR 363.2, "Annual Reporting Requirements," and 12 CFR 363.3, "Independent Public Accountant," where acceptability and specific reporting requirements are defined for these reporting components.

b. The federal banking agencies, however, continue to encourage all banks, regardless of size, to have annual audits and to establish audit committees made up entirely of outside directors. See OCC Bulletin 1999-37.

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

d. Large customers are defined in 12 CFR 363 appendix A.33.

e. The insured depository institution must meet the criteria in 12 CFR 363.1(b)(1). In addition, the holding company services and functions must be comparable to those required of the institution by 12 CFR 363 and provided at the top-tier or mid-tier holding company level. (12 CFR 363.1(b)(2)(i)).

Note: The appropriate federal banking agency may require a bank with total assets of $9 billion or more to comply with requirements of 12 CFR 363 at the bank level if the agency determines that exemptions as noted above, if applied to the bank, would create a significant risk to the Deposit Insurance Fund.

Appendix D: 12 CFR 363 Report Worksheets

The Worksheet: 12 CFR 363 Annual Report Review is a tool to be prepared each year on receipt of either the annual report or the Laws and Regulations Attestation Report. Review of any other reports received periodically should be recorded on the 12 CFR 363 Periodic Reports Worksheet. Use of these worksheets is not mandatory.

<table>
<tr><th colspan="2">Worksheet: 12 CFR 363 Annual Report Review</th></tr>
<tr><td>Name of reporting institution or holding company</td><td>Charter no.</td></tr>
<tr><td>City and state</td><td>Date received</td></tr>
<tr><td>Name and address (city, state) of IPA</td><td>Year end</td></tr>
<tr><td rowspan="2">If holding company, names and addresses of subsidiary institution(s) subject to 12 CFR 363 (attach list if needed)</td><td>Date of last peer review</td></tr>
<tr><td>Reviewer</td></tr>
<tr><td colspan="2">ANNUAL REPORT (Check attachments)
☐ Financial statements and notes ☐ Audit report ☐ Management report
☐ IPA’s attestation on internal controls</td></tr>
<tr><td colspan="2">REVIEWER Complete all sections and answer the following questions:</td></tr>
<tr><td colspan="2">Describe any item in the report that may adversely influence the bank’s safety and soundness. (Reference should be made to the discussion in other sections.)</td></tr>
<tr><td colspan="2">As a result of this review, is any follow-up action required or change in supervisory strategy warranted? Yes ☐ No ☐

If yes, attach a memorandum outlining your recommendations.</td></tr>
</table>

Worksheet: 12 CFR 363 Annual Report Review		
ANNUAL REPORT		
Do the report and financial statements cover a holding company or an individual institution?	HC ☐	Inst. ☐
Has the report been signed and dated?	Yes ☐	No ☐
Does the report have any explanatory paragraphs in addition to the three paragraphs of the standard auditor's report?	Yes ☐	No ☐
If yes, briefly describe the matter(s) covered in these paragraphs.		

FINANCIAL STATEMENTS AND NOTES

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

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

Securities
Derivatives
Other real estate
Related party transactions
Pensions or deferred compensation plans
Loans and leases
Servicing rights
Allowance for loan and lease losses
Taxes
Off-balance-sheet activities
Business combinations/pushdown accounting
Nontraditional activities

Worksheet: 12 CFR 363 Annual Report Review		
MANAGEMENT REPORT		
Does the report cover a holding company or an individual institution?	HC ☐	Inst. ☐
Has the report been signed by both the CEO and the chief financial or chief accounting officer?	Yes ☐	No ☐
Does the report state management's responsibilities for		
• preparing financial statements?	Yes ☐	No ☐
• establishing and maintaining an adequate internal control structure and procedures for financial reporting?	Yes ☐	No ☐
• complying with designated laws and regulations?	Yes ☐	No ☐
Does the report assess the		
• effectiveness of the aforementioned internal controls at the end of the most recent year?	Yes ☐	No ☐
• compliance with the designated laws and regulations during the year?	Yes ☐	No ☐
Briefly describe any instances of ineffectiveness or noncompliance reported by management or apparent deficiencies in reporting.		
INDEPENDENT PUBLIC ACCOUNTANT'S ATTESTATION ON INTERNAL CONTROLS		
Has the report been signed and dated?	Yes ☐	No ☐
Does the report indicate material weaknesses in the internal structure and procedures for financial reporting?	Yes ☐	No ☐
If so, briefly describe:		

Worksheet 2: 12 CFR 363 Periodic Report Review		
Name of reporting bank or holding company	Charter no.	
City and state	Date received	
Name and address (city, state) of IPA	Year end	
If holding company, names and addresses of subsidiary institution(s) subject to 12 CFR 363 (attach list if needed)	Date of last peer review	
	Reviewer	
REPORT FILED ☐ Change of accountant report ☐ Termination of services report ☐ Management letter ☐ Other report (describe)		
REVIEWER – Complete the following sections:		
Describe briefly any item in the report that may adversely influence the bank's safety and soundness.		
As a result of this review, is any follow-up action required or change in supervisory strategy warranted?	Yes ☐	No ☐
If yes, attach a memorandum outlining your recommendations.		

Appendix E: Internal Audit Review Worksheet

This worksheet is designed as a tool to help examiners evaluate the quality of internal audit programs, work papers, and related reporting for individual bank departments, activities, products, or services. If completed, the worksheet should be provided to the applicable examiner leading supervision of the internal audit function to facilitate an overall internal audit assessment. Use of this worksheet is not mandatory.

Note: NA means "not applicable."

Worksheet: Internal Audit Review		
Unit audited:	Date of audit report:	
Auditor in charge:	Audit frequency:	
Audit rating:	Agree with rating: Yes ☐ No ☐	
Management response: Yes ☐ No ☐	Response adequate: Yes ☐ No ☐	
Risk rating:		
Examiner's summary comment:		
Scope		
1. Was the scope of the audit adequate?	___ Yes ___ No ___ NA	Why or why not:
2. Is there evidence that prior audit issues were included in the scope for proper follow-up?	___ Yes ___ No ___ NA	If no, explain:
3. If the original scope was adjusted, was it adequately explained?	___ Yes ___ No ___ NA	If no, explain:
4. If automated testing was used, was it adequately documented or explained in the scope or planning stage?	___ Yes ___ No ___ NA	If no, explain:
5. If models are relied on in the business unit, has audit incorporated a review of validation activities into the scope of activities?	___ Yes ___ No ___ NA	If no, explain:
6. Comment on the quality of the planning document.	___ Adequate ___ Inadequate ___ NA	Why:
7. Is the audit frequency appropriate relative to the level of risk in the area or unit?	___ Yes ___ No	Why or why not:
8. Is any portion of this audit outsourced?	___ All ___ Partial ___ NA	
a. If so, is the arrangement conducted in a safe and sound manner? For more information, refer to OCC Bulletin 2003-12. (Question updated version 1.1)	___ Yes ___ No	Why not:
b. If so, is the audit work of sufficient detail to draw appropriate conclusions?	___ Yes ___ No	Why not:

Worksheet: Internal Audit Review		
Unit audited:	Date of audit report:	
Auditor in charge:	Audit frequency:	
Audit Risk Assessment		
9. Were audit risk assessment matrixes used to describe the risk(s)?	__ Yes __ No	Why not:
a. If yes, were the matrixes sufficient?	__ Yes __ No	Why not:
10. Was audit risk assessment used to determine when to audit this area?	__ Yes __ No	Why not:
11. Was audit risk assessment used to determine the scope of the audit?	__ Yes __ No	Why not:
12. Is the audit risk assessment of this area adequate?	__ Yes __ No	Why not:
Audit Work and Findings		
13. Were the audit program and procedures sufficient?	__ Yes __ No	Describe the deficiencies:
14. Were audit procedures performed to ensure compliance with applicable	__ Yes __ No	
a. policies?	__ NA	
b. procedures?	__ Yes __ No __ NA	
c. plans?	__ Yes __ No __ NA	
d. laws and regulations?	__ Yes __ No __ NA	
15. Were internal controls for the area sufficiently detailed?	__ Yes __ No	
16. Did the audit contain tests of administrative or operational	__ Yes __ No	
a. controls?	__ Yes __ No	
b. policies?	__ Yes __ No	
c. procedures?	__ Yes __ No	
17. Did the audit note the root cause of deficiencies or symptoms of problems?	__ Root cause __ Symptom __ Both __ NA	
18. Was a review of pertinent MIS performed as part of the audit?	__ Yes __ No __ NA	Why not:

Worksheet: Internal Audit Review		
Unit audited:	Date of audit report:	
Auditor in charge:	Audit frequency:	
19. What is the quality of the procedures documentation?	__ High __ Acceptable __ Unacceptable	Support:
a. Are audit trails sufficient?	__ Yes __ No	Why not:
20. How well does the audit describe the risk represented in individual findings or groups of findings?	__ Well __ Acceptable __ Unacceptable __ NA	Support:
21. If the area or unit is internally rated satisfactory, how well does the audit mitigate the existence of significant findings?	__ Well __ Acceptable __ Unacceptable __ NA	Support:
22. Were all exceptions or weaknesses in the audit work papers noted in the final audit report?	__ Yes __ No __ NA	Why not:
23. Were the internal auditors (in-house or outsourced), including third parties, adequately qualified to complete this program?	__ Yes __ No	How determined:
24. How well does the auditor in charge support the final audit rating?	__ Well __ Acceptable __ Unacceptable __ NA	Support:
25. Do you agree with the final rating?	__ Yes __ No __ NA	Why not:
26. Were any horizontal or silo emerging or systemic risks identified during the audit review? Should there have been?	__ Yes __ No	Explain:
a. If yes, was the information appropriately addressed, discussed, and reported in a reasonable time frame to the fullest extent possible across the enterprise?	__ Yes __ No	Why not:
27. If automated testing or continuous auditing was used, was its use independent, appropriate, and effective?	__ Yes __ No	Explain:
Sampling		
28. Did the auditor use statistical sampling?	__ Yes __ No __ NA	
a. Was the population accurately defined and justified by the auditor?	__ Yes __ No	Why not:
b. Was the selection of the sampling method disclosed?	__ Yes __ No	Why not:
c. Were the sample selection techniques disclosed?	__ Yes __ No	Why not:
d. Were sample evaluation and reporting results criteria established?	__ Yes __ No	Why not:

Worksheet: Internal Audit Review		
Unit audited:	Date of audit report:	
Auditor in charge:	Audit frequency:	
e. Did documentation provide adequate support for the sample size and coverage?	__Yes __No __NA	
Audit Reports		
29. Does the audit report articulate the appropriate conclusions, findings, and recommendations?	__Yes __No	Why not:
30. Does the audit report address the root cause of problems and recommend actions to correct problems?	__Yes __No __NA	
31. What level of management was notified of the audit findings?		
a. Is this the appropriate level or person?	__Yes __No	If not, who:
32. Does the auditor in charge or supervisor make effective use of MIS and have periodic contact with area or unit management?	__Yes __No	Why not:
Audit Follow-Up		
33. Was there evidence that prior audit issues were properly followed up during the current audit?	__Yes __No __NA	
34. Was management's response to audit findings timely?	__Yes __No	
35. Was management's response to audit findings acceptable?	__Yes __No	Why not:
36. Are corrective action time frames included in management's response?	__Yes __No __NA	
37. How effective and timely are management's plans for addressing deficiencies?	__Adequate __Inadequate __NA	Why inadequate:
38. Are audit exceptions in this area sufficiently detailed on an exception tracking report?	__Yes __No __NA	Why not:
39. Is there sufficient follow-up activity for high-risk or adversely rated areas or units?	__Yes __No __NA	Why not:
Quality Assurance		
40. Was the audit subject to a quality control review and is the audit unit addressing any quality assurance concerns?	__Yes __No __NA	Why not:
Meetings With Auditors		
41. Summarize any discussions with internal auditors or outsourced internal auditors. (Summary should include but not be limited to: participants, date, subject, conclusions or recommendations, and the participants' receptiveness and responses.)		

Worksheet: Internal Audit Review		
Unit audited:	Date of audit report:	
Auditor in charge:	Audit frequency:	
Conclusion		
42. Can activities performed (scope, work performed, follow-up, findings, etc.) and documentation supporting the audit review be relied on to evaluate the effectiveness of operations, risk management, control, and governance processes either on a standalone basis or with consideration for other planned activities within the audit cycle? In other words, can the OCC and the board fully rely on the work and conclusions for this area?	__Yes __No	If no, describe what needs to be done to rely on audit work.
43. Did the auditor or audit team involved in the review of this area have the necessary skills, experience, and knowledge required for the review?	__Yes __No	
44. Was the auditor independent of the area under review?	__Yes __No	
45. Should the OCC adjust its strategy for this bank or business unit based on your review of the audit reports, memos, and work papers?	__Yes __No	Why or why not and what adjustments should be made?
46. Provide any other information deemed appropriate.		

Appendix F: External Auditor Independence Worksheet

The following worksheet is designed to help examiners determine whether the bank's external auditor meets AICPA, PCAOB, or SEC independence requirements. This worksheet is a summary and not intended to be a complete listing of external auditor independence requirements. Where a rule set by one independence standard is more or less restrictive than the corresponding rule in the other independence standards, the IPA must comply with the most restrictive rule.[182] Examiners should consult specific requirements and interpretations that might apply to an individual bank.

This worksheet is not applicable when IPAs perform outsourced internal audit activities for the bank but do not perform external audit or attestation services for the bank. Use of this worksheet is not mandatory.

Note: Shaded answer blocks indicate situations that do or may impair the external auditor's independence.

Worksheet: External Auditor Independence			
	Yes	**No**	**Comments**
IPA PERFORMS EXTERNAL AUDIT			
1. During the period of engagement, did the IPA a. have or commit to acquire any direct or material indirect financial interest in the bank? b. act as trustee of any trust or executor or administrator of any estate that has or committed to acquire any direct or material indirect financial interest in the bank? c. have a joint closely held investment material to the IPA?			Explain any yes answers.
2. During the period of engagement, did the IPA have any loan to or from the bank, any officer or director of the bank, or any individual owning 10 percent or more of the bank's equity securities other than the following: a. Grandfathered loans i. existing as of January 1, 1992? ii. obtained before engagement by the bank? iii. obtained from the bank for which independence was not required and subsequently sold to the bank? iv. obtained from the bank before becoming a member of the firm? b. Automobile loans and leases? c. Loans fully collateralized by cash surrender value of insurance policy? d. Loans fully collateralized by cash deposits at the bank?			If yes, explain.

[182] 12 CFR 363.3(f) indicates that auditors of banks covered by 12 CFR 363 must comply with independence standards and interpretations of the AICPA, PCAOB, and SEC, following the most stringent standard in any corresponding rules. (Footnote added version 1.1)

Worksheet: External Auditor Independence			
	Yes	**No**	**Comments**
e. Aggregate credit card or cash advance debt of $5,000 or less?			
3. During the period of engagement, did any partner or professional employee of the accounting firm, his or her immediate family, or any group of such persons acting together own more than 5 percent of the bank's equity securities?			If yes, explain.
4. During the period of engagement or period covered by the financial statements, was any partner or professional employee of the accounting firm associated with the bank as a. director, officer, employee, or any capacity equivalent to that of a member of bank management? b. promoter, underwriter, or voting trustee? c. trustee for any pension or profit-sharing trust of the bank?			Explain any yes answers.
5. Does the IPA perform other services for the bank that entail a. authorizing, executing or consummating a transaction, or otherwise exercising authority on behalf of a client or having the authority to do so? b. preparing source documents or originating data, in electronic or other form, evidencing the occurrence of a transaction (for example, purchase orders, payroll time records, and customer orders)? c. having custody of client assets? d. supervising client employees in the performance of their normal recurring activities? e. determining which recommendations should be implemented? f. reporting to the bank board on behalf of management? g. serving as a client's stock transfer or escrow agent, registrar, general counsel or its equivalent?			Explain any yes answers.
6. During the period of engagement, did the IPA's firm have any material cooperative arrangements with the bank such as the following: a. Prime or subcontractor arrangements to provide services or products to a third party? b. Joint ventures to develop or market products or services? c. Arrangements to combine one or more firm services or products with one or more bank services or products and market the package with references to both parties? d. Arrangements under which the firm acts as distributor or marketer of the bank's products or services, or the bank acts as distributor or marketer of the firm's products or services?			Explain any yes answers.
7. Does the IPA perform any or all internal audit services for the bank?			Explain any yes answers and give time of these services.
8. Does bank management make decisions on whether to implement the IPA's recommendations?			If no, why not?

Worksheet: External Auditor Independence			
	Yes	**No**	**Comments**
9. Does bank management rely on the IPA's work as the primary basis for its control assertion?			If yes, why?
10. Does the bank monitor internal control processes to assess the quality of control performance over time through: a. Ongoing activities? b. Separate evaluations? **Note:** IPA can perform separate evaluations of bank's control effectiveness, including separate evaluation of bank's ongoing monitoring activities, as part of the external audit. c. Or a combination of both?			At least one of the below should be yes.
11. Does the bank, for internal audit: a. Designate a competent individual or individuals, preferably within senior management, to be responsible for the internal audit function? b. Determine the scope, risk, and frequency of internal audit activities, including those performed by the IPA providing outsourced internal audit activities? c. Evaluate the findings and results arising from internal audit activities, including those performed by the IPA providing outsourced internal audit activities? d. Evaluate the adequacy of audit procedures performed and findings resulting from performance of those procedures by, among other things, obtaining reports from the IPA providing outsourced or co-sourced internal audit activities?			Explain any no answers.
12. Does the IPA: a. Inform, using an engagement letter, the bank board or its audit committee of the respective roles of the bank and the IPA with respect to the outsourced internal audit engagement?			If no, why not?
b. Perform outsourced or co-sourced internal audit procedures in accordance with terms of the engagement, as stipulated in the engagement letter, and report thereon to the bank? **Note:** IPA independence is not impaired if the IPA performs procedures generally considered extensions of its financial statement audit scope (e.g., confirmations or analysis of fluctuations in account balances, comfort letters, etc.).			If no, why not?
c. Direct, review, and supervise day-to-day performance of outsourced or co-sourced internal audit procedures?			If no, who does?
d. Undertake responsibilities required to be performed by the bank individual responsible for the internal audit function?			If yes, explain.

Worksheet: External Auditor Independence			
	Yes	**No**	**Comments**
13. Does the IPA perform any of the following: a. Ongoing monitoring or control activities that affect transaction execution; ensuring that transactions are properly executed, accounted for, or both; and routine activities in connection with bank's operating or production processes equivalent to those of ongoing compliance or quality control functions? b. Determining which, if any, recommendations for improving the internal control system should be implemented? c. Reporting to bank board or audit committee on behalf of bank management or the individual responsible for the internal audit program? d. Authorizing, executing, or consummating transactions or otherwise exercising authority on behalf of bank? e. Preparing source documents? f. Having custody of assets? g. Approving or being responsible for the overall internal audit work plan, including determination of internal audit risk and scope, project priorities, and frequency of performance of audit procedures? h. Being connected with bank in any capacity equivalent to a member of bank management or as a bank employee (e.g., listed as employee in bank directories or other bank publications, allowing self to be referred to by title or description as supervising or being in charge of bank's internal audit function, or using bank's letterhead or internal correspondence forms in communications)?			Explain any yes answers.
SEC Requirements Applicable for any IPA performing external audit work at banks subject to 12 CFR 363 and banks whose securities are registered with the OCC, i.e., those subject to the periodic filing and reporting requirements of 12 CFR 11. The full text of the SEC's independence rule can be found on the SEC site. (Updated version 1.1)			
14. Are the bank's securities registered with the OCC, or is the bank subject to 12 CFR 363?			If yes, complete questions 15-24.
15. During the audit and engagement period, did the accountant, firm, covered persons of the firm, or immediate family members have any financial interests in the bank such as the following:			Explain any yes answers.

Worksheet: External Auditor Independence			
	Yes	**No**	**Comments**
a. Investments in the bank? For example: i. Direct investment in stocks, bonds, notes, options, or other securities. ii. More than 5 percent ownership in the bank's equity securities or control of the bank. iii. Voting trustee of a trust or executor of an estate having bank securities. iv. Material indirect investment in the bank. v. Direct or material indirect investment in an entity where • the bank has an investment in an entity material to the bank and significant influence over the entity. • the entity has an investment in the bank material to the entity and significant influence over the bank. vi. Any material investment in an entity over which the bank has significant influence. vii. Ability to significantly influence an entity that can significantly influence the bank. b. Other financial interests? For example: i. Loans to or from the bank, its directors or officers, or anyone owning more than 10 percent of the bank's securities, except for			
• automobile loans or leases. • loans fully collateralized by cash surrender value of insurance policy. • loans fully collateralized by cash deposits at the bank. • mortgage loan collateralized by borrower's primary residence and not obtained while a covered person.			
ii. Savings or checking accounts at the bank exceeding FDIC-insured coverage. iii. Broker/dealer accounts maintained at the bank. iv. Future commission merchant account maintained at the bank. v. Credit card balances aggregating $10,000 or more vi. Insurance products issued by the bank. vii. Financial interest in an entity that is part of an investment company that includes the bank. c. Bank financial relationships? For example: i. Investments by the bank in the firm's stocks, bonds, notes, options, or other securities. ii. Bank officers or directors own more than 5 percent of the firm's equity securities. iii. Bank acts as underwriter, broker/dealer, market-maker, promoter, or analyst for securities issued by the firm.			

Worksheet: External Auditor Independence			
	Yes	**No**	**Comments**
16. During the audit and engagement period, did the accountant have employment relationships with the bank such as the following: a. Current partner, principal, shareholder or professional employee of the firm is employed by the bank or serves as a member of the bank board? b. Close family member of firm's covered persons is in an accounting or financial reporting oversight role at the bank, or was in such a role during the period of engagement? c. Former partner, principal, shareholder or professional employee of the firm is in an accounting or financial reporting oversight role at the bank, or is in such a role and was a member of the audit engagement team during the prior year's audit of the bank? d. Former officer, director, or employee of bank is employed by the firm and participated in the audit of the bank's financial statements covering any period for which the employee worked for the bank?			Explain any yes answers.
17. During the audit and engagement period, did the firm or any covered person in the firm have any direct or material indirect business relationship with the bank or its officers, directors, or substantial shareholders?			
18. During the audit and engagement period, did the accountant provide any of the following non-audit services to the bank: a. Bookkeeping or other services related to the accounting records or financial statements of the bank? b. Financial information system design and implementation? c. Appraisal or valuation services, fairness opinions, or contribution-in-kind reports? d. Actuarial services? e. Internal audit outsourcing services? **Note:** "Internal audit services" means only that work related to internal accounting controls, financial systems, financial statements, and matters that affect financial statements. Work on other operational internal audit services not related to the above is not included. The key criteria is whether it is reasonable to conclude that the results of these services will not be subject to audit procedures during an audit of the audit client's financial statements. f. Management functions, either temporary or permanent? g. Human resources? h. Broker/dealer, investment advisor, or investment banking services? i. Legal services? j. Expert services unrelated to the audit?			
19. During the audit and period of engagement, did the accountant provide any service or product to the bank for a contingent fee or commission, or receive a contingent fee or commission from the bank?			

Worksheet: External Auditor Independence			
	Yes	**No**	**Comments**
20. Has the audit engagement team lead and concurring partners performed audit, review or attest services for the bank or any of its significant subsidiaries for more than five consecutive years?			
21. Did the bank's audit committee pre-approve all audit, review and attestation engagements performed by the auditor?			
22. Did the bank's audit committee pre-approve non-prohibited non-audit services performed by the auditor?			
23. Did any partner, principal or shareholder participating on the audit engagement team earn or receive compensation based on the performance of, or procuring of, engagement with the bank to provide any products or services other than audit, review or attestation services?			
24. Did the audit firm, before filing the audit report with the OCC or SEC, report the following: a. All critical accounting policies and practices to be used? b. All alternative treatments of financial information within GAAP that have been discussed with bank management, including i. ramifications of the use of alternative disclosures and treatments, and ii. the treatment preferred by the audit firm? c. Other material written communications between the audit firm and bank management, such as any management letter or schedule of unadjusted differences?			
Summary			
25. Based on responses to the above questions, does the IPA act or appear to act in a capacity equivalent to that of the bank's management?			If yes, explain.
26. Are there any other factors that indicate the IPA does not comply with provisions of the independence standards?			If yes, explain.

Appendix G: Board or Audit Committee Oversight Worksheet

The following worksheet is designed to help examiners assess the quality and extent of the bank's audit committee (or board, if there is no audit committee) duties and responsibilities and the qualifications of committee members. Examiners may want to use the worksheet, or share it with the bank board or audit committee, as a tool or facilitate general discussions with banks about audit committee (or board, if there is no audit committee) responsibilities. The worksheet can be used for banks subject to 12 CFR 363 or for banks with securities registered with the OCC (i.e., subject to the periodic filing and reporting requirements of 12 CFR 11). It can also be used for banks that are not subject to the statutory requirements (i.e., most community banks). When using the worksheet for banks that are not subject to the statutory requirements, however, examiners need to be cognizant of the bank's size, complexity, operations, and risk profile and temper such discussions accordingly. Use of this worksheet is not mandatory. (Updated version 1.1)

Note: A response in a shaded answer block generally indicates an area examiners should discuss with the bank board or its audit committee and, as appropriate, reach agreement on corrective measures. Examiners should explain any mitigating circumstances, particularly for smaller community banks, in the Comments column.

Worksheet: Board or Audit Committee Oversight				
	Yes	**No**	**NA**	**Comments**
General Responsibilities				
1. Does the bank board or its audit committee do the following: a. Review and approve audit strategies, policies, programs (including Bank Secrecy Act compliance programs), and organizational structure? b. Review and approve selection or termination of third-party external auditors and internal auditors? c. Meet regularly with internal and external auditors and third-party internal audit? d. Ensure that internal and external auditors and third-party internal auditors are independent and objective? e. Ensure that comprehensive audit coverage is in place to meet risks and demands posed by current and planned activities? f. Have significant input into hiring senior internal audit personnel, setting their compensation, and evaluating their performance? g. Review and approve annual audit plans and schedules, and any changes thereto, for both internal and external audits? h. Retain internal and external auditors and third parties qualified to audit the activities in which the bank is engaged?				

Worksheet: Board or Audit Committee Oversight				
	Yes	**No**	**NA**	**Comments**
i. Monitor and track significant control weaknesses and management's progress toward corrective action? j. Meet with examiners at least once each supervisory cycle to discuss audit review findings? k. Establish and maintain procedures for bank employees to confidentially submit anonymous concerns to the committee about questionable accounting, internal controls, or auditing matters?				
2. Is the committee responsible for risk management issues? **Note:** The bank board may assign these to another committee or individual designated as responsible for overseeing the bank's overall risk management functions. If so, does it do the following: a. Communicate risk management concerns to the full board? b. Ensure that risk management evaluation functions are independent? c. Review risk management reports and information?				
Audit Committee				
3. Does the bank have an audit committee? (Required for banks subject to 12 CFR 363 or OCC-registered banks.)				
4. Does the committee maintain minutes and other relevant records of their meetings and decisions? (Required for banks subject to 12 CFR 363.)				
5. Has the committee adopted and the board approved a written charter for the audit committee? (Required for OCC-registered banks.) If so, does the charter address the following: a. The committee's responsibilities and how they carry out those responsibilities (including structure, processes, and membership requirements)? b. The committee's review and discussion with IPAs of any relationships or services that may affect the IPA's independence or objectivity? (The SEC's revised independence rule and PCAOB's independence rules require OCC-registered bank audit committees to pre-approve all audit, review, attest, and non-prohibited non-audit services.) c. The IPA's accountability to the board and committee, and the board or committee's authority and responsibility to select, evaluate, and (where appropriate) replace the IPA?				

Worksheet: Board or Audit Committee Oversight				
	Yes	**No**	**NA**	**Comments**
6. Are the majority of committee members independent of management for banks that have between $500 million and $1 billion of total assets (as of the beginning of the year)? (Required for banks subject to 12 CFR 363 and OCC-registered banks.)				
7. Are committee members independent of management for banks that have $1 billion or more of total assets (as of the beginning of the year)? (Required for banks subject to 12 CFR 363 and OCC-registered banks.) (Updated version 1.1)				
8. For banks with $3 billion or more of total assets (as of the beginning of the year), is the audit committee comprised of members with banking or related financial management expertise, have access to its own outside counsel, and not include any large customers of the bank? (Required for banks subject to 12 CFR 363.) (Updated version 1.1)				
9. Is the committee made up entirely of outside directors? (Required for banks subject to 12 CFR 363 and OCC-registered banks.)				
10. Does the bank board annually make a determination of committee member independence? (Required for banks subject to 12 CFR 363 and OCC-registered banks.)				
If so, does the board's determination consider whether				
a. members serve or have served as the bank's or its affiliates' consultant, advisor, promoter, underwriter, legal counsel, or trustee? b. members hold or control, or did not hold or control within the preceding year, either directly or indirectly, a financial interest of 10 percent or more in the bank or its affiliates? c. any committee member is a large customer of the bank?				
d. any member has been, within the last three years, an employee, or whether any member's immediate family member has been, within the last three years, an executive officer? e. the director or an immediate family member of the director, is, or has been within the last three years, employed as an executive officer of another entity where any of the present executive officers of the bank or any of its affiliates at the same time serves or served on that entity's compensation committee? f. the director is a current employee, or an immediate family member is a current executive officer, of an entity that has made payments to, or received payments from, the institution or any of its affiliates for property or services in an amount which, in any of the last three fiscal years, exceeds the greater of $200,000, or 5 percent of such entity's consolidated gross revenues? This would include payments made by the institution or any of its affiliates to not-				

Worksheet: Board or Audit Committee Oversight				
	Yes	**No**	**NA**	**Comments**
for-profit entities where the director is an executive officer or where an immediate family member of the director is an executive officer. g. any member has participated in the preparation of the financial statements? h. any member has received, or has an immediate family member who has received, during any 12-month period within the last three years, more than $100,000 in direct and indirect compensation from the institution, its subsidiaries, and its affiliates for consulting, advisory, or other services? i. any member, or a member's immediate family member, is a current partner of a firm that performs internal or external auditing services for the institution or any of its affiliates; the director is a current employee of such a firm; the director has an immediate family member who is a current employee of such a firm and who participates in the firm's audit, assurance, or tax compliance practice; or the director or an immediate family member was within the last three years (but no longer is) a partner or employee of such a firm and personally worked on the audit of the insured depository institution or any of its affiliates within that time?				
11. Does the committee, for banks with total assets greater than $3 billion as of the beginning of the fiscal year, have access to its own counsel at its own discretion and without prior approval of the board or management? (Required for banks subject to 12 CFR 363 and OCC-registered banks.)				
12. Does the committee perform all duties as determined by the board, including reviewing the following, as applicable, with management and the IPA (required for banks subject to 12 CFR 363 and OCC-registered banks): a. Approve engagement letter and any associated scope of servicers' documents for external auditor? b. The basis of reports required under 12 CFR 363? **Note:** The required reports are: (1) management's report and assertion on internal controls over financial reporting and compliance with designated laws, (2) IPA's audit and report on the bank's financial statements, and (3) IPA's attestation report on management's control assertion. c. Significant accounting policies? d. Audit conclusions regarding significant management estimates? e. Disagreements between the IPA and management? f. Assessments of internal control adequacy and resolution of identified material internal control weaknesses and reportable conditions?				

Worksheet: Board or Audit Committee Oversight				
	Yes	**No**	**NA**	**Comments**
g. The bank's compliance with laws and regulations?				
13. Does the committee oversee the internal audit function? (Required for banks subject to 12 CFR 363.)				
14. Does the audit committee pre-approve all audit and permitted non-audit services provided by the IPA? (Required for OCC-registered banks.)				
15. Does the committee do the following on an annual basis: (Required for OCC-registered banks.) a. Receive and review written disclosures from the IPA disclosing all relationships between the IPA and its related entities and the bank and its related entities that, in the IPA's judgment, may reasonably bear on independence? b. Review the above letter to ensure that the IPA confirms they are independent of the bank? c. Discuss the IPA's independence with the IPA?				
16. Does the committee recommend to the bank board that the audited financial statements be included in the bank's annual report? (Required for OCC-registered banks.)				
17. Does the committee review the aggregate fees billed by the IPA for the following: (Required for OCC-registered banks.) a. The annual financial statement audit? b. Other audit-related services? c. Tax services? d. All other products and services provided by the IPA for the most recent fiscal year?				
18. Does the committee review the hours spent on the bank's financial audit by persons other than the IPA's full-time permanent employees? (Required for OCC-registered banks.)				

Appendix H: OCC Acknowledgment of External Audit Work Paper Request Letter

When examiners request access to external audit work papers, the external auditor may submit a "work paper access" letter to the examiner or the supervisory office along with a request to acknowledge its receipt. Examiners may use the following template as a written acknowledgment and response if presented with such a letter. They should attach the OCC acknowledgment to the external auditor's original letter and return both to the external auditor. Examiners should also retain a copy of the external auditor's letter and the OCC acknowledgment letter.

[Date]

[Name of firm]

We are in receipt of your letter dated [insert date] regarding providing us access to or copies of work papers associated with your [insert date of audit] audit of [insert bank or company name] (see copy attached).

This letter serves as our acknowledgment to confirm receipt of your letter, but does not constitute agreement to any terms specified in your letter that limit our ability to supervise the bank.

We also acknowledge your request for confidential treatment under the Freedom of Information Act or other applicable law. Any request by a third party for disclosure of the information for which you have requested such treatment will be processed pursuant to our regulations governing such requests, which are promulgated at 12 CFR 4.

Office of the Comptroller of the Currency

By: _____ Date: _____

Appendix I: Glossary

Entries marked with an asterisk (*) are as defined in 12 CFR 30, appendix D.

Chain banking group. A group that controls several banks, albeit not through a holding company structure.

Chief auditor. The bank employee assigned responsibility for the internal audit function.

Continuous audit system. A continuous audit system, used in the context of auditing fiduciary activities as set forth in 12 CFR 9.9, "Audit of Fiduciary Activities," and 12 CFR 150.440-480, "Audit Requirements," refers to an alternative to the required annual fiduciary audit. Under a continuous audit system, a bank may arrange for a discrete audit of each significant fiduciary activity at an interval commensurate with the nature and risk of the activity.

Continuous auditing. Continuous auditing is a set of processes or a methodology that enables independent auditors to provide written assurance on a subject matter. Continuous auditing promotes issuance of assurance reports simultaneously with or a short period after the occurrence of monitored events.[183] Technology plays a key role in continuous audit activities by helping to automate the identification of exceptions or anomalies, analyze patterns within the digits of key numeric fields, review trends, and test controls, among other activities.

Continuous monitoring. Continuous monitoring is a set of processes that management puts in place to ensure that the policies, procedures, and business processes are operating effectively. Continuous monitoring typically addresses management's responsibility to assess the adequacy and effectiveness of controls. Continuous monitoring in the internal audit area is limited to its own operations.

Co-sourcing. Also known as partial outsourcing, co-sourcing occurs when the outsourced internal audit services are performed in concert with bank employees. (Glossary term added version 1.1)

External audit function. The external audit function represents the development and implementation of the bank's external audit program. The external audit program provides the bank board with information about the bank's financial reporting risk areas, e.g., the bank's internal controls over financial reporting, accuracy of its recording of transactions, and completeness of its financial reports in accordance with applicable accounting standards. Through its external audit program, the bank board or its audit committee engages an independent auditor or audit firm, commonly known as the "external auditor," for planning and execution of the external audit plan. (Glossary term added version 1.1)

Financial management expertise. Per 12 CFR 363, appendix A.32, the board designates an audit committee member(s) as a banking or related financial management expert (financial

[183] The Canadian Institute of Charter Accountants and the AICPA developed this widely known definition.

expert). This person must have significant executive, professional, educational, or regulatory experience in financial, auditing, accounting, or banking matters. The board determines the relevant banking matters. Significant experience as an officer or member of the board or audit committee of a financial services company would satisfy 12 CFR 363, appendix A.32. A person who has attributes of an "audit committee financial expert" as set forth in the SEC's rules would also satisfy these criteria.

Frontline unit:* Any organizational unit or function thereof in a bank covered under 12 CFR 30, appendix D, that is accountable for a risk in paragraph II.B and that (1) engages in activities designed to generate revenue or reduce expenses for the parent company or covered bank; (2) provides operational support or servicing to any organizational unit or function within the covered bank for the delivery of products or services to customers; or (3) provides technology services to any organizational unit or function covered by these guidelines. A frontline unit does not ordinarily include an organizational unit or function thereof within a covered bank that provides legal services to the covered bank.

Independent public accountants. IPAs are accountants who are independent of the institutions they audit. IPAs are registered or licensed by state boards of accountancy to practice public accounting, hold themselves out as certified public accountants, public accountants, and are in good standing under the laws of the state or other political subdivision of the United States in which they are licensed to practice.

Independent risk management.* Any organizational unit within a covered bank that has responsibility for identifying, measuring, monitoring, or controlling aggregate risks. Such units maintain independence from frontline units through the following reporting structure: (a) The board or the board's risk committee reviews and approves the risk governance framework; (b) each chief risk executive has unrestricted access to the board and its committees to address risks and issues identified through independent risk management's activities; (c) the board or its risk committee approves all decisions regarding the appointment or removal of the chief risk executive(s) and approves the annual compensation and salary adjustment of the chief risk executive(s); and (d) no frontline unit executive oversees any independent risk management unit.

Inherent risk. The risk to an entity in the absence of any actions management might take to alter either the risk's likelihood or impact.[184]

Internal audit function. The internal audit function is the third line of defense. The internal audit function's primary role is to independently and objectively review and evaluate bank activities. This role helps to maintain and improve the efficiency and effectiveness of the bank's risk management system, internal controls systems,[185] and corporate governance. The internal audit function monitors the bank's internal control systems. (Glossary term added version 1.1)

[184] COSO developed this widely known definition.

[185] According to 12 CFR 30, appendix A, II.A, internal control systems include internal controls and information systems.

Large customer. Per 12 CFR 363, appendix A.33, a large customer is any individual or entity (including a controlling person of any such entity) which, in the determination of the bank's board, has such a significant direct or indirect credit or relationship with the institution that its termination would likely have a material and adverse effect on the institution's financial condition or results of its operations.

New activities. Per OCC Bulletin 2017-43, new, modified, or expanded bank products and services are collectively referred to as new activities. (Glossary term added version 1.1)

Outsourced internal audit. This is an arrangement in which the bank engages a third party to conduct internal audit activities. These types of arrangements are referred to as "internal audit outsourcing," "internal audit assistance," "audit integration," "audit co-sourcing," or "extended audit services" (collectively, outsourcing). (Glossary term added version 1.1)

Residual risk. The risk that remains after controls are taken into account (the net risk or risk after controls).[186]

System of internal controls. A system of internal controls is made up of both internal controls and information systems. Internal control is the systems, policies, procedures, and processes, effected by the bank board, management, and other personnel, designed to safeguard bank assets, limit or control risks, and achieve the bank's objectives.[187] These objectives address effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations. The system of internal controls varies with the bank's size and complexity and the nature and scope of the bank's activities.

Third-party relationship. Per OCC Bulletin 2013-29, a third-party relationship is any business arrangement between the bank and another entity, by contract or otherwise. Third-party relationships include activities that involve outsourced products and services, use of independent consultants, networking arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, joint ventures, and other business arrangements where the bank has an ongoing relationship or may have responsibility for the associated records.

[186] Ibid.

[187] Refer to the "Internal Controls" booklet of the *Comptroller's Handbook* (national banks) and *OTS Examination Handbook* section 340 (FSAs) for more information on systems of internal controls.

Appendix J: Abbreviations

(Section updated version 1.1)

ADC	assistant deputy comptroller
AICPA	American Institute of Certified Public Accountants
ASB	Auditing Standards Board
BCBS	Basel Committee on Banking Supervision
CAAT	computer-assisted auditing technique or computer-aided audit tool
CAMELS	capital adequacy, asset quality, management, earnings, liquidity, sensitivity to market risk
CEO	chief executive officer
CFR	Code of Federal Regulations
CIF	collective investment funds
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CPA	Certified Public Accountant
EIC	examiner-in-charge
FBO	foreign banking organization
FDI Act	Federal Deposit Insurance Act
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FSA	federal savings association
GAAP	generally accepted accounting principles
GAAS	generally accepted auditing standards
GLBA	Gramm–Leach–Bliley Act of 1999
IIA	Institute of Internal Auditors
IPA	independent public accountant
IT	information technology
MIS	management information systems
OCC	Office of the Comptroller of the Currency
OTS	Office of Thrift Supervision
PCAOB	Public Company Accounting Oversight Board
ROCA	risk management, operational controls, compliance, and asset quality
ROE	report of examination
SAS	Statement on Auditing Standards
SEC	U.S. Securities and Exchange Commission
SOC	service organization control
SOX	Sarbanes–Oxley Act of 2002
SSAE	Statement on Standards for Attestation Engagements
UBPR	Uniform Bank Performance Reports
UITRS	Uniform Interagency Trust Rating System
URSIT	Uniform Rating System for Information Technology
USC	U.S. Code

References

(Section updated version 1.1)

Listed references apply to national banks and FSAs unless otherwise noted.

Laws

12 USC 1831m, "Early Identification of Needed Improvements in Financial Management"
12 USC 1831p-1, "Standards for Safety and Soundness"
15 USC 78j-1, "Audit Requirements"
15 USC 1681s, "Administrative Enforcement"
15 USC 1681w, "Disposal of Records"
15 USC 6801, "Protection of Nonpublic Personal Information"
15 USC 6805, "Enforcement"
Pub. L. 107-204, 116 Stat. 745 (2002), Sarbanes–Oxley Act of 2002

Regulations

12 CFR 4, "Organization and Functions, Availability and Release of Information, Contracting Outreach Program, Post-Employment Restrictions for Senior Examiners"
12 CFR 9.9, "Audit of Fiduciary Activities" (national banks)
12 CFR 9.18, "Collective Investment Funds" (national banks and FSAs)[188]
12 CFR 11, "Securities Exchange Act Disclosure Rules"
12 CFR 16, "Securities Offering Disclosure Rules"
12 CFR 19, "Rules of Practice and Procedure"
12 CFR 21.21, "Procedures for Monitoring Bank Secrecy Act Compliance"
12 CFR 30, "Safety and Soundness Standards"
12 CFR 150.260, "How May I Invest Funds of a Fiduciary Account?" (FSAs)
12 CFR 150.440-480, "Audit Requirements" (FSAs)
12 CFR 363, "Annual Independent Audits and Reporting Requirements"
17 CFR 210, "Form and Content of And Requirements For Financial Statements, Securities Act of 1933, Securities Exchange Act of 1934, Investment Company Act of 1940, Investment Advisers Act of 1940, and Energy Policy and Conservation Act of 1975"
17 CFR 240, "General Rules and Regulations, Securities Exchange Act of 1934"

Federal Register

73 Fed. Reg. 22215
79 Fed. Reg. 54518, at 54527

[188] Applies to FSAs pursuant to 12 CFR 150.260(b).

Comptroller's Handbook

"Bank Supervision Process"
"Collective Investment Funds"
"Community Bank Supervision"
"Compliance Management Systems"
"Federal Branches and Agencies Supervision"
"Foreword"
"Internal Control" (national banks)
"Large Bank Supervision"
"Related Organizations" (national banks)
"Sampling Methodologies" (national banks)

Comptroller's Licensing Manual

"Charters"

OTS Examination Manual (FSAs)

Section 209, "Sampling"
Section 340, "Internal Control"
Section 730, "Related Organizations"

OCC Issuances

Banking Bulletin 1992-42, "Interagency Policy Statement: External Auditors"
OCC Bulletin 1999-37, "Interagency Policy Statement on External Auditing Programs: External Audit"
OCC Bulletin 2003-12, "Interagency Policy Statement on Internal Audit and Internal Audit Outsourcing: Revised Guidance on Internal Audit and Its Outsourcing"
OCC Bulletin 2006-7, "Interagency Advisory on the Unsafe and Unsound Use of Limitation of Liability Provisions in External Audit Engagement Letters"
OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance"
OCC Bulletin 2016-2, "Interagency Advisory on External Audits of Internationally Active U.S. Financial Institutions"
OCC Bulletin 2017-7, "Third-Party Relationships: Supplemental Examination Procedures"
OCC Bulletin 2017-21, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29"
OCC Bulletin 2017-43, "New, Modified, or Expanded Bank Products and Services: Risk Management Principles"
The Director's Book: Role of Directors for National Banks and Federal Savings Associations

American Institute of Certified Public Accountants

AICPA Audit and Accounting Guide, "Depository and Lending Institutions: Banks and Savings Institutions, Credit Unions, Finance Companies, and Mortgage Companies"

AICPA Standards for Performing and Reporting on Peer Reviews
AICPA Code of Professional Conduct
AICPA Statement on Standards for Attestation Engagement No. 10, "Agreed-Upon Procedures Engagements"
AICPA Statement on Standards for Attestation Engagement No. 18, "Concepts Common to All Attestation Engagements"
AU-C Section 210, "Terms of Engagement"
AU-C Section 230, "Audit Documentation"
AU-C Section 260, "The Auditor's Communication With Those Charged With Governance"
AU-C Section 265, "Communicating Internal Control Related Matters Identified in an Audit"
AU-C Section 300, "Planning an Audit"
AU-C section 610, "Using the Work of Internal Auditors"
AU-C Section 700, "Forming an Opinion and Reporting on Financial Statements"
AU-C Section 705, "Modifications to the Opinion in the Independent Auditor's Report"
AU-C Section 940, "An Audit of Internal Control Over Financial Reporting That Is Integrated With an Audit of Financial Statements"

International Auditing and Assurance Standards Board

International Standard on Assurance Engagements No. 3402

International Standards on Auditing

ISA 705, "Modifications to the Opinion in the Independent Auditor's Report"

NACHA Standards

NACHA 1.2.1, "Audits of Rules of Compliance"

PCAOB Auditing Standards (AS) and Rules

AS 1201, "Supervision of the Audit Engagement"
AS 1301, "Communications with Audit Committees"
AS 1305, "Communications About Control Deficiencies in an Audit of Financial Statements"
AS 2101, "Audit Planning"
AS 2201, "An Audit of Internal Control Over Financial Reporting That Is Integrated With an Audit of Financial Statements"
AS 2605, "Consideration of the Internal Audit Function"
AS 3101, "The Auditor's Report on an Audit of Financial Statements When the Auditor Expresses an Unqualified Opinion"
AS 3105, "Departures from Unqualified Opinions and Other Reporting Circumstances"
Rule 3526, "Communications with Audit Committees Concerning Independence"

Other Publications

Basel Committee on Banking Supervision, "The Internal Audit Function in Banks"
Committee of Sponsoring Organizations of the Treadway Commission, *Internal Control—Integrated Framework*
FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual
FFIEC IT Examination Handbook
Institute of Internal Auditors, *International Standards for the Professional Practice of Internal Auditing*
Institute of Internal Auditors, "Principles Guiding the Performance of Consulting Activities of Internal Auditors"

Table of Updates Since Publication

Refer to the "Foreword" booklet of the *Comptroller's Handbook* for more information regarding the OCC's process for updating *Comptroller's Handbook* booklets.

Version 1.0: Published December 30, 2016			
Version number	**Date**	**Reason**	**Affected pages**
1.1	July 25, 2019	Clarified applicability to federal branches and agencies	1
		Clarified applicability to national banks or FSAs	1, 29, 110
		Clarifications regarding the role of the bank's board or management	2, 12, 13, 80, 93
		Clarifications regarding supervisory guidance, sound risk management practices, or legal language	2–3, 5–9, 15–16, 19–21, 25–26, 33, 35–36, 41, 45, 53–54, 71, 80, 95, 108, 113, 115, 127
		Added reference or cross-reference	2, 5, 7–12, 14, 19–20, 22, 35, 37, 40, 43, 45, 47–49, 53–55, 57–58, 66, 70, 110, 115–116, 132, 146
		Edited for clarity	3–5, 7, 9–11, 14–15, 17, 33, 35–36, 38, 58, 60, 62–63, 69, 72, 80, 89, 94, 106, 108–110, 113, 116–118, 141
		Updated for consistency with booklets in the *Examination Process* series of the *Comptroller's Handbook*	4, 6, 58, 60–62, 64, 67–68, 71–72, 108
		Added risk definition summaries	4–6
		Reflect issuance of OCC Bulletin 2017-43 and rescission of OCC Bulletin 2004-20 and *OTS Examination Handbook* section 760	8, 37, 117
		Changes to AICPA Auditing Standards	31, 43, 73, 116
		Repeal of 12 CFR 16.20 (refer to 73 Fed. Reg. 22215)	45, 135, 139
		Updated for consistency with Uniform Interagency Consumer Compliance Rating System	70
		Updated for consistency with UITRS	71
		Added terms to appendix I, "Glossary"	146–147
		Updated appendix J, "Abbreviations," for consistency with the content of the booklet	148
		Updated "References" section for consistency with the content of the booklet	149–152