Supplemental Examination Procedures

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

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

Planning the Audit Review

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

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

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

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

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

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

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

   - How management supervises audit activities.

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

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

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

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

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

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

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

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

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

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

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

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

Board and Committee Oversight

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

   - Contains management's assessments of:

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

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

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

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

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

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

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

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

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

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

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

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

Internal Audit

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- Control assessments.
- Audit report findings.

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

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

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

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

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

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

   - Quality assurance is conducted in the following manner:

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

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

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

- Quality assurance reviews are conducted regularly.

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

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

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

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

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

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

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

1. Obtain the following:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

   - Time frames

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

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

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

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

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

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

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

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

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

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

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

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

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

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

   - Any of the following issues exist:

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

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

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

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

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

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

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

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

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

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

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

1. Obtain and review the following documents:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

   - Costs and benefits of vendor services to be provided.

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

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

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

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

   - Reference checks.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

External Audit

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

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

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

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

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

   - The results of any vote taken regarding external audit.

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

   - Discussion of the external auditor's independence.

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

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

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

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

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

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

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

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

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

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

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

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

5. Determine the type of external audit performed:

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

6. Obtain copies of:

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

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

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

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

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

- Current examination and external audit results or significant findings.

- Upcoming external audit and examination activities.

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

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

- Any other pertinent information.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

    - Recalcitrant external audit firm or staff.

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

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

    - Work was adequately planned and supervised.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- The professional reputation of the auditors.

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

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

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

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

- Significant banking industry audit experience, including specialized areas.

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

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

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

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

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

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

Overall Conclusions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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