INTERNAL AUDITS

FIL-21-2003
March 17, 2003

TO:
CHIEF EXECUTIVE OFFICER (also of interest to the Internal Audit Manager and Members of the Board)
SUBJECT:
Interagency Policy Statement on the Internal Audit Function and Its Outsourcing
Summary:
The federal banking agencies have revised their 1997 internal audit policy statement to update guidance (in light of the Sarbanes-Oxley Act) on the independence of an accountant who provides both external audit and internal audit services to an institution. Other parts of the 1997 policy statement also have been revised.

The Federal Deposit Insurance Corporation (FDIC) and the other federal banking agencies have issued the attached Interagency Policy Statement on the Internal Audit Function and Its Outsourcing. The policy statement, which replaces a policy issued in 1997 (see FIL 133 97, dated December 22, 1997), updates the agencies' guidance on the independence of an accountant who provides both external and internal audit services to an institution as a result of the auditor independence provisions of the Sarbanes-Oxley Act of 2002. The updated policy statement also reflects the agencies' experience with the 1997 policy and incorporates recent developments in internal auditing.

The Sarbanes-Oxley Act and recently adopted Securities and Exchange Commission (SEC) rules prohibit an accounting firm from acting as the external auditor of a public company during the same period that the firm provides internal audit outsourcing and certain other non-audit services to the company. In addition, if a public company's external auditor will be performing auditing and permitted non-audit services, its audit committee must pre-approve each of these services. These SEC rules generally become effective on May 6, 2003, although a one-year transition period is provided for contractual arrangements in place as of that date. The revised policy statement separately discusses the applicability of these requirements to:

- Institutions that are public companies;
- Insured depository institutions with $500 million or more in assets, which are subject to the annual audit and reporting requirements of Section 36 of the Federal Deposit Insurance Act; and
- Non-public institutions that are not subject to Section 36.

For institutions subject to Section 36, whether or not they are public companies, the FDIC's existing guidelines provide for their external auditors to comply with the SEC's auditor independence requirements that are in effect during the period covered by the audit. These requirements include the non-audit service prohibitions and audit committee pre-approval requirements.
The policy statement encourages non-public institutions not subject to Section 36, which includes non-public banks with less than $500 million in assets, to follow the Sarbanes-Oxley Act's internal audit outsourcing prohibition. However, if such an institution decides to use the same firm for both internal and external audit work, the audit committee should document both that it has pre approved the internal audit outsourcing to its external auditor and has considered the independence issues associated with this arrangement.
In addition to changes related to the Sarbanes-Oxley Act, the agencies revised the 1997 policy statement's discussion of the responsibilities of the board of directors and senior management with respect to the internal audit function and its placement within an organization, its management and staffing, and the communication of concerns and weaknesses in accounting and internal control. Expanded guidance has been provided on the use of independent reviews of significant internal controls

by small institutions that do not have a formal internal audit manager or staff. The policy statement also includes guidance for examiners on addressing concerns about the adequacy of the internal audit function.

This Financial Institution Letter (FIL) replaces FIL-133-97, dated December 22, 1997.

For further information, please contact Robert F. Storch, Chief Accountant (202 898 8906), in the Division of Supervision and Consumer Protection.

For your reference, FDIC Financial Institution Letters may be accessed on the FDIC's Web site at www.fdic.gov/news/news/financial/2003/index.html. To learn how to automatically receive FDIC Financial Institution Letters through e-mail, please visit www.fdic.gov/news/news/announcements/index.html.

Michael J. Zamorski

Director

Attachment

Distribution: FDIC-Supervised Banks (Commercial and Savings)

NOTE: Paper copies of FDIC financial institution letters may be obtained through the FDIC's Public Information Center, 801 17th Street, NW, Room 100, Washington, DC 20434 (1-877-275-3342, option 5, or 202-416-6940).

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
FEDERAL DEPOSIT INSURANCE CORPORATION
OFFICE OF THE COMPTROLLER OF THE CURRENCY
OFFICE OF THRIFT SUPERVISION

INTERAGENCY POLICY STATEMENT ON THE INTERNAL AUDIT FUNCTION AND ITS OUTSOURCING

March 17, 2003

INTRODUCTION

Effective internal control[1] is a foundation for the safe and sound operation of a financial institution (institution).[2] The board of directors and senior management of an institution are responsible for ensuring that the system of internal control operates effectively. Their responsibility cannot be delegated to others within the institution or to outside parties. An important element in assessing the effectiveness of the internal control system is an internal audit function. When properly structured and conducted, internal audit provides directors and senior management with vital information about weaknesses in the system of internal control so that management can take prompt, remedial action. The federal banking agencies' [3] (agencies) long standing examination policies call for examiners to review an institution's internal audit function and recommend improvements, if needed. In addition, pursuant to Section 39 of the Federal Deposit Insurance Act (FDI Act) (12 U.S.C. 1831p-1), the agencies have adopted Interagency Guidelines Establishing Standards for Safety and Soundness that apply to insured depository institutions.[4] Under these guidelines and policies, each institution should have an internal audit function that is appropriate to its size and the nature and scope of its activities.

In addressing various quality and resource issues, many institutions have been engaging independent public accounting firms and other outside professionals (outsourcing vendors) in recent years to perform work that traditionally has been done by internal auditors. These arrangements are often called "internal audit outsourcing," "internal audit assistance," "audit co sourcing," and "extended audit services" (hereafter collectively referred to as outsourcing). Typical outsourcing arrangements are more fully illustrated in Part II below.

Outsourcing may be beneficial to an institution if it is properly structured, carefully conducted, and prudently managed. However, the agencies have concerns that the structure, scope, and management of some internal audit outsourcing arrangements do not contribute to the institution's safety and soundness. Furthermore, the agencies want to ensure that these arrangements with outsourcing vendors do not leave directors and senior management with the erroneous impression that they have been relieved of their responsibility for maintaining an effective system of internal control and for overseeing the internal audit function.

This policy statement sets forth key characteristics of the internal audit function in Part I. Sound practices concerning the use of outsourcing vendors are discussed in Part II. Part III discusses the effect outsourcing arrangements have on the independence of an external auditor who also provides internal audit services to an institution. Part III also discusses the prohibition on internal audit outsourcing to a public company's external auditor under the Sarbanes-Oxley Act of 2002,[5] the effect of this prohibition on insured depository institutions subject to the annual audit and reporting requirements of Section 36 of the

FDI Act (12 U.S.C. 1831m), and the agencies' views on compliance with this provision of the Sarbanes-Oxley Act by institutions not subject to Section 36 (including smaller depository institutions) that are not publicly-held. Finally, Part IV of this statement provides guidance to examiners concerning their reviews of internal audit functions and related matters.

PART I - THE INTERNAL AUDIT FUNCTION

Board and Senior Management Responsibilities

The board of directors and senior management are responsible for having an effective system of internal control and an effective internal audit function in place at their institution. They are also responsible for ensuring that the importance of internal control is understood and respected throughout the institution. This overall responsibility *cannot* be delegated to anyone else. They may, however, delegate the design, implementation and monitoring of specific internal controls to lower-level management and the testing and assessment of internal controls to others. Accordingly, directors and senior management should have reasonable assurance that the system of internal control prevents or detects significant inaccurate, incomplete, or unauthorized transactions; deficiencies in the safeguarding of assets; unreliable financial reporting (which includes regulatory reporting); and deviations from laws, regulations, and the institution's policies.[6]

Some institutions have chosen to rely on so-called "management self-assessments" or "control self-assessments," wherein 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 impartial. Directors and members of senior management who rely too much on these reviews may not learn of control weaknesses until they have become costly problems, particularly if directors are not intimately familiar with the institution's operations. Therefore, institutions generally should also have their internal controls tested and evaluated by units without business-line responsibilities, such as internal audit groups.

Directors should be confident that the internal audit function addresses the risks and meets the demands posed by the institution's current and planned activities. To accomplish this objective, directors should consider whether their institution's internal audit activities are conducted in accordance with professional standards, such as the Institute of Internal Auditors' (IIA) *Standards for the Professional Practice of Internal Auditing*. These standards address independence, professional proficiency, scope of work, performance of audit work, management of internal audit, and quality assurance reviews. Furthermore, directors and senior management should ensure that the following matters are reflected in their institution's internal audit function.

Structure. Careful thought should be given to the placement of the audit function in the institution's management structure. The internal audit function should be positioned so that the board has confidence that the internal audit function will perform its duties with impartiality and not be unduly influenced by managers of day-to-day operations. The audit committee,[7] using objective criteria it has established, should oversee the internal audit function and evaluate its performance.[8] The audit committee should assign responsibility for the internal audit function to a member of management (hereafter referred to as the manager of internal audit or internal audit manager) who understands the function and has no responsibility for operating the system of internal control. The ideal organizational arrangement is for this manager to report directly and solely to the audit committee regarding both audit issues and administrative matters, e.g., resources, budget, appraisals, and compensation. Institutions are encouraged to consider the IIA's *Practice Advisory 2060-2: Relationship with the Audit Committee*, which provides more guidance on the roles and relationships between the audit committee and the internal audit manager.

Many institutions place the manager of internal audit under a dual reporting arrangement: functionally accountable to the audit committee on issues discovered by the internal audit function, while reporting to

another senior manager on administrative matters. Under a dual reporting relationship, the board should consider the potential for diminished objectivity on the part of the internal audit manager with respect to audits concerning the executive to whom he or she reports. For example, a manager of internal audit who reports to the chief financial officer (CFO) for performance appraisal, salary, and approval of department budgets may approach audits of the accounting and treasury operations controlled by the CFO with less objectivity than if the manager were to report to the chief executive officer. Thus, the chief financial officer, controller, or other similar officer should ideally be excluded from overseeing the internal audit activities even in a dual role. The objectivity and organizational stature of the internal audit function are best served under such a dual arrangement if the internal audit manager reports administratively to the CEO.

Some institutions 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 utilize available resources, and enhance the institution's ability to comprehensively manage risk. Such an administrative reporting relationship should be designed so as to not interfere with or hinder the manager of internal audit's functional reporting to and ability to directly communicate with the institution's audit committee. In addition, the audit committee should ensure that efforts to coordinate these monitoring functions do not result in the manager of internal audit conducting control activities nor diminish his or her independence with respect to the other risk monitoring functions. Furthermore, the internal audit manager should have the ability to independently audit these other monitoring functions.

In structuring the reporting hierarchy, the board should weigh the risk of diminished independence against the benefit of reduced administrative burden in adopting a dual reporting organizational structure. The audit committee should document its consideration of this risk and mitigating controls. The IIA's *Practice Advisory 1110-2: Chief Audit Executive Reporting Lines* provides additional guidance regarding functional and administrative reporting lines.

Management, staffing, and audit quality. In managing the internal audit function, the manager of internal audit is responsible for control risk assessments, audit plans, audit programs, and audit reports.

- A control risk assessment (or risk assessment methodology) documents the internal auditor's understanding of the institution's significant business activities and their associated risks. These assessments typically analyze the risks inherent in a given business line, the mitigating control processes, and the resulting residual risk exposure of the institution. They should be updated regularly to reflect changes to the system of internal control or work processes, and to incorporate new lines of business.

- An internal audit plan is based on the control risk assessment and typically includes a summary of key internal controls within each significant business activity, the timing and frequency of planned internal audit work, and a resource budget.

- An internal audit program describes the objectives of the audit work and lists the procedures that will be performed during each internal audit review.

- An audit report generally presents the purpose, scope, and results of the audit, including findings, conclusions, and recommendations. Workpapers that document the work performed and support the audit report should be maintained.

Ideally, the internal audit function's only role should be to independently and objectively evaluate and report on the effectiveness of an institution's risk management, control, and governance processes. Internal auditors increasingly have taken a consulting role within institutions on new products and services and on mergers, acquisitions, and other corporate reorganizations. This role typically includes

helping design controls and participating in the implementation of changes to the institution's control activities. The audit committee, in its oversight of the internal audit staff, should ensure that the function's consulting activities do not interfere or conflict with the objectivity it should have with respect to monitoring the institution's system of internal control. In order to maintain its independence, the internal audit function should not assume a business-line management role over control activities, such as approving or implementing operating policies or procedures, including those it has helped design in connection with its consulting activities. The agencies encourage internal auditors to follow the IIA's standards, including guidance related to the internal audit function acting in an advisory capacity.

The internal audit function should be competently supervised and staffed by people with sufficient expertise and resources to identify the risks inherent in the institution's operations and assess whether internal controls are effective. The manager of internal audit should oversee the staff assigned to perform the internal audit work and 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 institution. Many policies and procedures may be communicated informally in small internal audit departments, while larger departments would normally require more formal and comprehensive written guidance.

Scope. The frequency and extent of internal audit review and testing should be consistent with the nature, complexity, and risk of the institution's on- and off-balance-sheet activities. At least annually, the audit committee should review and approve internal audit's control risk assessment and the scope of the audit plan, including how much the manager relies on the work of an outsourcing vendor. It should also periodically review internal audit's adherence to the audit plan. The audit committee should consider requests for expansion of basic internal audit work when significant issues arise or when significant changes occur in the institution's environment, structure, activities, risk exposures, or systems.[9]

Communication. To properly carry out their responsibility for internal control, directors and senior management should foster forthright communications and critical examination of issues to better understand the importance and severity of internal control weaknesses identified by the internal auditor and operating management's solutions to these weaknesses. Internal auditors should report internal control deficiencies to the appropriate level of management as soon as they are identified. Significant matters should be promptly reported directly to the board of directors (or its audit committee) and senior management. In periodic meetings with management and the manager of internal audit, the audit committee should assess whether management is expeditiously resolving internal control weaknesses and other exceptions. Moreover, the audit committee should give the manager of internal audit the opportunity to discuss his or her findings without management being present.

Furthermore, each audit committee should establish and maintain procedures for employees of their institution to submit confidentially and anonymously concerns to the committee about questionable accounting, internal accounting control, or auditing matters.[10] In addition, the audit committee should set up procedures for the timely investigation of complaints received and the retention for a reasonable time period of documentation concerning the complaint and its subsequent resolution.

Contingency Planning. As with any other function, the institution should have a contingency plan to mitigate any significant discontinuity in audit coverage, particularly for high-risk areas. Lack of contingency planning for continuing internal audit coverage may increase the institution's level of operational risk.

Small Institutions

An effective system of internal control and an independent internal audit function form the foundation for safe and sound operations, regardless of an institution's size. As noted in the Introduction, each institution should have an internal audit function that is appropriate to its size and the nature and scope of its activities. The procedures assigned to this function should include adequate testing and review of internal controls and information systems.

It is the responsibility of the audit committee and management to carefully consider the extent of auditing that will effectively monitor the internal control system after taking into account the internal audit function's costs and benefits. For institutions that are large or have complex operations, the benefits derived from a full-time manager of internal audit or an auditing staff likely outweigh the cost. For small institutions with few employees and less complex operations, however, these costs may outweigh the benefits.

Nevertheless, a small institution without an internal auditor can ensure that it maintains an objective internal audit function by implementing a comprehensive set of independent reviews of significant internal controls. The key characteristic of such reviews is that the person(s) directing and/or performing the

review of internal controls is **not** also responsible for managing or operating those controls. A person who is competent in evaluating a system of internal control should design the review procedures and arrange for their implementation. The person responsible for reviewing the system of internal control should report findings directly to the audit committee. The audit committee should evaluate the findings and ensure that senior management has or will take appropriate action to correct the control deficiencies.

U.S. Operations of Foreign Banking Organizations

The internal audit function of a foreign banking organization (FBO) should cover its U.S. operations in its risk assessments, audit plans, and audit programs. Its U.S. domiciled audit function, head-office internal audit staff, or some combination thereof normally performs the internal audit of the U.S. operations. Internal audit findings (including internal control deficiencies) should be reported to the senior management of the U.S. operations of the FBO and the audit department of the head office. Significant adverse findings also should be reported to the head office's senior management and the board of directors or its audit committee.

PART II - INTERNAL AUDIT OUTSOURCING ARRANGEMENTS

Examples of Arrangements

An outsourcing arrangement is a contract between an institution and an outsourcing vendor to provide internal audit services. Outsourcing arrangements take many forms and are used by institutions of all sizes. Some institutions consider entering into these arrangements to enhance the quality of their control environment by obtaining the services of a vendor with the knowledge and skills to critically assess, and recommend improvements to, their internal control systems.

The internal audit services under contract can be limited to helping internal audit staff in an assignment for which they lack expertise. Such an arrangement is typically under the control of the institution's manager of internal audit, and the outsourcing vendor reports to him or her. Institutions often use outsourcing vendors for audits of areas requiring more technical expertise, such as electronic data processing and capital markets activities. Such uses are often referred to as "internal audit assistance" or "audit co-sourcing."

Some outsourcing arrangements are structured so that an outsourcing vendor performs virtually all the procedures or tests of the system of internal control. Under such an arrangement, a designated manager of internal audit oversees the activities of the outsourcing vendor and typically is supported by internal audit staff. The outsourcing vendor may assist the audit staff in determining risks to be reviewed and may recommend testing procedures, but the internal audit manager is responsible for approving the audit scope, plan, and procedures to be performed. Furthermore, the internal audit manager is responsible for the results of the outsourced audit work, including findings, conclusions, and recommendations. The outsourcing vendor may report these results jointly with the internal audit manager to the audit committee.

Additional Considerations for Internal Audit Outsourcing Arrangements

Even when outsourcing vendors provide internal audit services, the board of directors and senior management of an institution are responsible for ensuring that both the system of internal control and the internal audit function operate effectively. In any outsourced internal audit arrangement, the institution's board of directors and senior management must maintain ownership of the internal audit function and provide active oversight of outsourced activities. When negotiating the outsourcing arrangement with an outsourcing vendor, an institution should carefully consider its current and anticipated business risks in setting each party's internal audit responsibilities. The outsourcing arrangement should not increase the risk that a breakdown of internal control will go undetected.

To clearly distinguish its duties from those of the outsourcing vendor, the institution should have a written contract, often taking the form of an engagement letter.[11] Contracts between the institution and the vendor typically include provisions that:

- Define the expectations and responsibilities under the contract for both parties;
- Set the scope and frequency of, and the fees to be paid for, the work to be performed by the vendor;
- Set the responsibilities for providing and receiving information, such as the type and frequency of reporting to senior management and directors about the status of contract work;

- Establish the process for changing the terms of the service contract, especially for expansion of audit work if significant issues are found, and stipulations for default and termination of the contract;

- State that internal audit reports are the property of the institution, that the institution will be provided with any copies of the related workpapers it deems necessary, and that employees authorized by the institution will have reasonable and timely access to the workpapers prepared by the outsourcing vendor;

- Specify the locations of internal audit reports and the related workpapers;[12]

- Specify the period of time (for example, seven years) that vendors must maintain the workpapers;

- State that outsourced internal audit services provided by the vendor are subject to regulatory review and that examiners will be granted full and timely access to the internal audit reports and related workpapers prepared by the outsourcing vendor;

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

- State that the outsourcing vendor will 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 and, if applicable, will comply with AICPA, U.S. Securities and Exchange Commission (SEC), Public Company Accounting Oversight Board (PCAOB), or regulatory independence guidance.

Vendor Competence. Before entering an outsourcing arrangement, the institution should perform due diligence to satisfy itself that the outsourcing vendor has sufficient staff qualified to perform the contracted work. The staff's qualifications may be demonstrated, for example, through prior experience with financial institutions. Because the outsourcing arrangement is a personal-services contract, the institution's internal audit manager should have confidence in the competence of the staff assigned by the outsourcing vendor and receive timely notice of key staffing changes. Throughout the outsourcing arrangement, management should ensure that the outsourcing vendor maintains sufficient expertise to effectively perform its contractual obligations.

Management. Directors and senior management should ensure that the outsourced internal audit function is competently managed. For example, larger institutions should employ sufficient competent staff members in the internal audit department to assist the manager of internal audit in overseeing the outsourcing vendor. Small institutions that do not employ a full-time audit manager should appoint a competent employee who ideally has no managerial responsibility for the areas being audited to oversee the outsourcing vendor's performance under the contract. This person should report directly to the audit committee for purposes of communicating internal audit issues.

Communication. Communication between the internal audit function and the audit committee and senior management should not diminish because the institution engages an outsourcing vendor. All work by the outsourcing vendor should be well documented and all findings of control weaknesses should be promptly reported to the institution's manager of internal audit. Decisions not to report the outsourcing vendor's findings to directors and senior management should be the mutual decision of the internal audit manager and the outsourcing vendor. In deciding what issues should be brought to the board's attention, the concept of "materiality," as the term is used in financial statement audits, is generally not a good indicator of which control weakness to report. For example, when evaluating an institution's compliance with laws and regulations, any exception may be important.

Contingency Planning. When an institution enters into an outsourcing arrangement (or significantly changes the mix of internal and external resources used by internal audit), it may increase its operational risk. Because the arrangement may be terminated suddenly, the institution should have a contingency plan to mitigate any significant discontinuity in audit coverage, particularly for high-risk areas.

PART III - INDEPENDENCE OF THE INDEPENDENT PUBLIC ACCOUNTANT

This part of the policy statement relates only to an outsourcing vendor who is a public accountant and is considering providing both external audit and internal audit services to an institution.

When one accounting firm performs both the external audit and the outsourced internal audit function, the firm risks compromising its independence. These concerns arise because, rather than having two separate functions, this outsourcing arrangement places the independent public accounting firm in the position of appearing to audit, or actually auditing, its own work. For example, in auditing an institution's financial statements, the accounting firm will consider the extent to which it may rely on the internal control system, including the internal audit function, in designing audit procedures.

The next three sections outline the applicability of the SEC's auditor independence requirements to public companies, insured depository institutions subject to Section 36 of the FDI Act, and non-public institutions that are not subject to Section 36. They are followed by information on the AICPA's independence guidance.

Institutions that are Public Companies

To strengthen auditor independence, Congress passed the Sarbanes-Oxley Act of 2002. Title II of this act applies to any company that has a class of securities registered with the SEC or the appropriate federal banking agency under Section 12 of the Securities Exchange Act of 1934 or that is required to file reports with the SEC under Section 15(d) of that act,[13] i.e., a public company. Within Title II, Section 201(a) prohibits an accounting firm from acting as the external auditor of a public company during the same period that the firm provides internal audit outsourcing services to the company.[14] In addition, if a public company's external auditor will be providing auditing services and non-audit services, such as tax services, that are not otherwise prohibited by Section 201(a) of the Sarbanes-Oxley Act, Title II also provides that the company's audit committee must pre-approve each of these services.

The SEC adopted final rules implementing the non-audit service prohibitions and audit committee pre-approval requirements of Title II on January 22, 2003.[15] According to these rules, an accountant is not independent if, at any point during the audit and professional engagement period, the accountant provides internal audit outsourcing or other prohibited non-audit services to a public company audit client. These rules generally become effective on May 6, 2003, although a one-year transition period is provided for contractual arrangements in place as of that date. Under this transition rule, an external auditor's independence will not be deemed to be impaired until May 6, 2004, if the auditor is performing internal audit outsourcing and other prohibited non-audit services for a public company audit client pursuant to a contract in existence on May 6, 2003. However, the services being provided must not have impaired the auditor's independence under the pre-existing independence requirements of the SEC, the Independence Standards Board, and the AICPA.

The SEC's pre-existing auditor independence requirements are contained in regulations that were adopted in November 2000 and became fully effective in August 2002.[16] Although the SEC's November 2000 regulations do not prohibit the outsourcing of internal audit services to a public company's independent public accountant, they place conditions and limitations on internal audit outsourcing.

Depository Institutions Subject to the Annual Audit and Reporting Requirements of Section 36 of the FDI Act

Under Section 36 as implemented by Part 363 of the FDIC's regulations, each FDIC-insured depository institution with total assets of $500 million or more is required to have an annual audit performed by an independent public accountant.[17] The Part 363 guidelines address the qualifications of an independent public accountant engaged by such an institution by stating that "[t]he independent public accountant should also be in compliance with the AICPA's *Code of Professional Conduct* and meet the independence requirements and interpretations of the SEC and its staff."[18]

Thus, the guidelines provide for each FDIC-insured depository institution with $500 million or more in total assets, whether or not it is a public company, and its external auditor to comply with the SEC's auditor independence requirements that are in effect during the period covered by the audit. These requirements include the non-audit service prohibitions and audit committee pre-approval requirements implemented by the SEC's January 2003 auditor independence rules once they take effect May 6, 2003, subject to the transition rule for internal audit outsourcing and other contracts in existence on that date described in the preceding section. That transition rule provides that such outsourcing arrangements will not impair an auditor's independence until May 6, 2004, provided certain conditions are met.[19]

Institutions Not Subject to Section 36 of the FDI Act that are Neither Public Companies nor Subsidiaries of Public Companies

The agencies have long encouraged each institution not subject to Section 36 of the FDI Act[20] that is neither a public company nor a subsidiary of a public company to have its financial statements audited by an independent public accountant.[21] The agencies also encourage each such non-public institution to follow the internal audit outsourcing prohibition in Section 201(a) of the Sarbanes-Oxley Act when the SEC's January 2003 regulations implementing this prohibition take effect, as discussed above for institutions that are public companies.

As previously mentioned, some institutions seek to enhance the quality of their control environment by obtaining the services of an outsourcing vendor who can critically assess their internal control system and recommend improvements. The agencies believe that a small non-public institution with less complex operations and limited staff can, in certain circumstances, use the same accounting firm to perform both an external audit and some or all of the institution's internal audit activities. These circumstances include, but are not limited to, situations where:

- Splitting the audit activities poses significant costs or burden;
- Persons with the appropriate specialized knowledge and skills are difficult to locate and obtain;
- The institution is closely held and investors are not solely reliant on the audited financial statements to understand the financial position and performance of the institution; and
- The outsourced internal audit services are limited in either scope or frequency.

In circumstances such as these, the agencies view an internal audit outsourcing arrangement between a small non-public institution and its external auditor as not being inconsistent with their safety and soundness objectives for the institution.

When a small non-public institution decides to hire the same firm to perform internal and external audit work, the audit committee and the external auditor should pay particular attention to preserving the independence of both the internal and external audit functions. Furthermore, the audit committee should document both that it has pre-approved the internal audit outsourcing to its external auditor and has considered the independence issues associated with this arrangement.[22] In this regard, the audit committee should consider the independence standards described in Parts I and II of this policy statement, the AICPA guidance discussed in the following section, and the broad principles that the auditor should not perform management functions or serve in an advocacy role for the client.

Accordingly, the agencies will not consider an auditor who performs internal audit outsourcing services for a small non-public audit client to be independent unless the institution and its auditor have adequately addressed the associated independence issues. In addition, the institution's board of directors and management must retain ownership of and accountability for the internal audit function and provide active oversight of the outsourced internal audit relationship.

A small non-public institution may be required by another law or regulation, an order, or another supervisory action to have its financial statements audited by an independent public accountant. In this situation, if warranted for safety and soundness reasons, the institution's primary federal regulator may require that the institution and its independent public accountant comply with the auditor independence requirements of Section 201(a) of the Sarbanes-Oxley Act.[23]

AICPA Guidance

As noted above, the independent public accountant for a depository institution subject to Section 36 of the FDI Act also should be in compliance with the AICPA's *Code of Professional Conduct*. This code includes professional ethics standards, rules, and interpretations that are binding on all certified public accountants (CPAs) who are members of the AICPA in order for the member to remain in good standing. Therefore, this code applies to each member CPA who provides audit services to an institution, regardless of whether the institution is subject to Section 36 or is a public company.

The AICPA has issued guidance indicating that a member CPA would be deemed not independent of his or her client when the CPA acts or appears to act in a capacity equivalent to a member of the client's management or as a client employee. The AICPA's guidance includes illustrations of activities that would be considered to compromise a CPA's independence. Among these are activities that involve the CPA authorizing, executing, or consummating transactions or otherwise exercising authority on behalf of the

client. For additional details, refer to Interpretation 101-3 - *Performance of Other Services* and Interpretation 101-13 - *Extended Audit Services* in the AICPA's *Code of Professional Conduct*.

PART IV - EXAMINATION GUIDANCE

Review of the Internal Audit Function and Outsourcing Arrangements

Examiners should have full and timely access to an institution's internal audit resources, including personnel, workpapers, risk assessments, work plans, programs, reports, and budgets. A delay may require examiners to widen the scope of their examination work and may subject the institution to follow-up supervisory actions.

Examiners will assess the quality and scope of an institution's internal audit function, regardless of whether it is performed by the institution's employees or by an outsourcing vendor. Specifically, examiners will consider whether:

- The internal audit function's control risk assessment, audit plans, and audit programs are appropriate for the institution's activities;
- The internal audit activities have been adjusted for significant changes in the institution's environment, structure, activities, risk exposures, or systems;
- The internal audit activities are consistent with the long-range goals and strategic direction of the institution and are responsive to its internal control needs;
- The audit committee promotes the internal audit manager's impartiality and independence by having him or her directly report audit findings to it;
- The internal audit manager is placed in the management structure in such a way that the independence of the function is not impaired;
- The institution has promptly responded to significant identified internal control weaknesses;
- The internal audit function is adequately managed to ensure that audit plans are met, programs are carried out, and results of audits are promptly communicated to senior management and members of the audit committee and board of directors;
- Workpapers adequately document the internal audit work performed and support the audit reports;
- Management and the board of directors use reasonable standards, such as the IIA's *Standards for the Professional Practice of Internal Auditing*, when assessing the performance of internal audit; and
- The audit function provides high-quality advice and counsel to management and the board of directors on current developments in risk management, internal control, and regulatory compliance.

The examiner should assess the competence of the institution's internal audit staff and management by considering the education, professional background, and experience of the principal internal auditors. In addition, when reviewing outsourcing arrangements, examiners should determine whether:

- The arrangement maintains or improves the quality of the internal audit function and the institution's internal control;
- Key employees of the institution and the outsourcing vendor clearly understand the lines of communication and how any internal control problems or other matters noted by the outsourcing vendor are to be addressed;

- The scope of the outsourced work is revised appropriately when the institution's environment, structure, activities, risk exposures, or systems change significantly;

- The directors have ensured that the outsourced internal audit activities are effectively managed by the institution;

- The arrangement with the outsourcing vendor satisfies the independence standards described in this policy statement and thereby preserves the independence of the internal audit function, whether or not the vendor is also the institution's independent public accountant; and

- The institution has performed sufficient due diligence to satisfy itself of the vendor's competence before entering into the outsourcing arrangement and has adequate procedures for ensuring that the vendor maintains sufficient expertise to perform effectively throughout the arrangement.

Concerns about the Adequacy of the Internal Audit Function

If the examiner concludes that the institution's internal audit function, whether or not it is outsourced, does not sufficiently meet the institution's internal audit needs, does not satisfy the Interagency Guidelines Establishing Standards for Safety and Soundness, if applicable,[24] or is otherwise inadequate, he or she should consider adjusting the scope of the examination. The examiner should also discuss his or her concerns with the internal audit manager or other person responsible for reviewing the system of internal control. If these discussions do not resolve the examiner's concerns, he or she should bring these matters to the attention of senior management and the board of directors or audit committee. Should the examiner find material weaknesses in the internal audit function or the internal control system, he or she should discuss them with appropriate agency staff in order to determine the appropriate actions the agency should take to ensure that the institution corrects the deficiencies. These actions may include formal and informal enforcement actions.

The institution's management and composite ratings should reflect the examiner's conclusions regarding the institution's internal audit function. The report of examination should contain comments concerning the adequacy of this function, significant issues or concerns, and recommended corrective actions.

Concerns about the Independence of the Outsourcing Vendor

An examiner's initial review of an internal audit outsourcing arrangement, including the actions of the outsourcing vendor, may raise questions about the institution's and its vendor's adherence to the independence standards described in Parts I and II of this policy statement, whether or not the vendor is an accounting firm, and in Part III if the vendor provides both external and internal audit services to the institution. In such cases, the examiner first should ask the institution and the outsourcing vendor how the audit committee determined that the vendor was independent. If the vendor is an accounting firm, the audit committee should be asked to demonstrate how it assessed that the arrangement has not compromised applicable SEC, PCAOB, AICPA, or other regulatory standards concerning auditor independence. If the examiner's concerns are not adequately addressed, the examiner should discuss the matter with appropriate agency staff prior to taking any further action.

If the agency staff concurs that the independence of the external auditor or other vendor appears to be compromised, the examiner will discuss his or her findings and the actions the agency may take with the institution's senior management, board of directors (or audit committee), and the external auditor or other vendor. In addition, the agency may refer the external auditor to the state board of accountancy, the AICPA, the SEC, the PCAOB, or other authorities for possible violations of applicable independence standards. Moreover, the agency may conclude that the institution's external auditing program is inadequate and that it does not comply with auditing and reporting requirements, including Sections 36 and 39 of the FDI Act and related guidance and regulations, if applicable.

---

[1] In summary, internal control is a process designed to provide reasonable assurance that the institution will achieve the following internal control objectives: efficient and effective operations, including safeguarding of assets; reliable financial reporting; and, compliance with applicable laws and regulations. Internal control consists of five components that are a part of the management process: control environment, risk assessment, control activities, information and communication, and monitoring activities. The effective functioning of these components, which is brought about by an institution's board

of directors, management, and other personnel, is essential to achieving the internal control objectives. This description of internal control is consistent with the Committee of Sponsoring Organizations of the Treadway Commission (COSO) report Internal Control-Integrated Framework. In addition, under the COSO framework, financial reporting is defined in terms of published financial statements, which, for purposes of this policy statement, encompasses both financial statements prepared in accordance with generally accepted accounting principles and regulatory reports (such as the Reports of Condition and Income and the Thrift Financial Report). Institutions are encouraged to evaluate their internal control against the COSO framework if they are not already doing so.

[2] The term "institution" includes depository institutions insured by the Federal Deposit Insurance Corporation (FDIC), U.S. financial holding companies and bank holding companies supervised by the Federal Reserve System, thrift holding companies supervised by the Office of Thrift Supervision (OTS), and the U.S. operations of foreign banking organizations.

[3] Board of Governors of the Federal Reserve System, FDIC, Office of the Comptroller of the Currency, and OTS.

[4] For national banks, Appendix A to Part 30; for state member banks, Appendix D-1 to Part 208; for insured state nonmember banks and insured state-licensed branches of foreign banks, Appendix A to Part 364; for savings associations, Appendix A to Part 570.

[5] Pub. L. 107-204, 116 Stat. 745 (2002).

[6] Under Section 36 of the FDI Act, as implemented by Part 363 of the FDIC's regulations (12 CFR 363), FDIC insured depository institutions with total assets of $500 million or more must submit an annual management report signed by the chief executive officer (CEO) and chief accounting or chief financial officer. This report must discuss management's responsibility for financial reporting controls and assess the effectiveness of those controls as well as the institution's compliance with designated laws and regulations.

[7] Depository institutions subject to Section 36 of the FDI Act and Part 363 of the FDIC's regulations must maintain independent audit committees (i.e., comprised of directors who are not members of management). Consistent with the 1999 Interagency Policy Statement on External Auditing Programs of Banks and Savings Associations, the agencies also encourage the board of directors of each depository institution that is not otherwise required to do so to establish an audit committee consisting entirely of outside directors. Where the term "audit committee" is used in this policy statement, the board of directors may fulfill the audit committee responsibilities if the institution is not subject to an audit committee requirement.

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

[9] Major changes in an institution's environment and conditions may compel changes to the internal control system and also warrant additional internal audit work. These include: (a) new management; (b) areas or activities experiencing rapid growth or rapid decline; (c) new lines of business, products, or technologies or disposals thereof; (d) corporate restructurings, mergers, and acquisitions; and (e) expansion or acquisition of foreign operations (including the impact of changes in the related economic and regulatory environments).

[10] Where the board of directors fulfills the audit committee responsibilities, the procedures should provide for the submission of employee concerns to an outside director.

[11] The engagement letter provisions described are comparable to those outlined by the American Institute of Certified Public Accountants (AICPA) for financial statement audits (see AICPA Professional Standards, AU section 310). These provisions are consistent with the provisions customarily included in contracts for other outsourcing arrangements, such as those involving data processing and information technology. Therefore, the federal banking agencies consider these provisions to be usual and customary business practices.

[12] If the workpapers are in electronic format, contracts often call for the vendor to maintain proprietary software that enables the bank and examiners to access the electronic workpapers for a specified time period.

[13] 15 U.S.C. 78l and 78o(d).

[14] In addition to prohibiting internal audit outsourcing, Section 201(a) of the Sarbanes-Oxley Act also identifies other non-audit services that an external auditor is prohibited from providing to a public company whose financial statements it audits. The legislative history of Section 201(a) indicates that three broad principles should be considered when determining whether an auditor should be prohibited

from providing a non-audit service to an audit client. These principles are that an auditor should not (1) audit his or her own work, (2) perform management functions for the client, or (3) serve in an advocacy role for the client. To do so would impair the auditor's independence. Based on these three broad principles, the other non-audit services that Section 201(a) prohibits an auditor from providing for a public company audit client include bookkeeping or other services related to the client's accounting records or financial statements; financial information systems design and implementation; appraisal or valuation services, fairness opinions, or contribution-in-kind reports; actuarial services; management functions or human resources; broker or dealer, investment adviser, or investment banking services; legal services and expert services unrelated to the audit; and any other service determined to be impermissible by the PCAOB.

[15] 68 Fed. Reg. 6006, February 5, 2003

[16] 65 Fed. Reg. 76007, December 5, 2000.

[17] 12 CFR 363.3(a).

[18] *Appendix A to Part 363-Guidelines and Interpretations, Paragraph 14. Independence.*

[19] If a depository institution subject to Section 36 and Part 363 satisfies the annual independent audit requirement by relying on the independent audit of its parent holding company, once the SEC's January 2003 regulations prohibiting an external auditor from performing internal audit outsourcing services for an audit client take effect May 6, 2003, or May 6, 2004, depending on the circumstances, the holding company's external auditor cannot perform internal audit outsourcing work for that holding company or the subsidiary institution.

[20] FDIC-insured depository institutions with less than $500 million in total assets are not subject to Section 36 of the FDI Act. Section 36 does not apply directly to holding companies, but it provides that, for an insured depository institution that is a subsidiary of a holding company, its audited financial statements requirement and certain of its other requirements may be satisfied by the holding company.

[21] See, for example, the 1999 Interagency Policy Statement on External Auditing Programs of Banks and Savings Institutions

[22] If a small non-public institution is considering having its external auditor perform other non-audit services (see footnote 14 for examples of such services), its audit committee may wish to discuss the implications of the performance of these services on the auditor's independence.

[23] For OTS-required audits under 12 CFR 562.4, independent public accountants performing such audits must meet the independence requirements and interpretations of the SEC and its staff.

[24] See footnote 4.