Attachment 1:

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

December 22, 1997

INTRODUCTION

Effective internal control[1] is a foundation for the safe and sound operation of a banking institution or savings association (hereafter referred to as institution). The board of Directors and senior managers 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 of an effective 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 agencies' long-standing examination policies call for examiners to review an institution's internal audit function and recommend improvements if needed. In addition, more recently, the agencies adopted Interagency Guidelines Establishing Standards for Safety and Soundness, pursuant to Section 39 of the Federal Deposit Insurance Act (FDI Act).[2] Under these guidelines, 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 (hereafter referred to as outsourcing vendors) to perform work that has been traditionally done by internal auditors. These arrange-ments are often called "internal audit outsourcing," "internal audit assistance," "audit co-sourcing," and "extended audit services" (hereafter, collectively referred to as outsourcing).

Such outsourcing may be beneficial to an institution if it is properly structured, carefully conducted, and prudently managed. However, the federal banking agencies have concerns that the structure, scope, and management of some internal audit outsourcing arrangements may 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 managers with the 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 some characteristics of sound practices for the internal audit function and the use of outsourcing vendors for audit activities. In addition, it provides guidance on how these outsourcing arrangements may affect an examiner's assessment of internal control. It also discusses the effect these arrangements may have on the independence of an external auditor who also is providing internal audit services to an institution. Finally, this statement provides guidance to examiners concerning their reviews of internal audit functions and related matters. This policy statement applies to bank holding companies and their

subsidiaries, FDIC-insured banks and savings associations, and U.S. operations of foreign banking organizations.

THE INTERNAL AUDIT FUNCTION

Director and Senior Management Responsibilities

The board of Directors and senior management are responsible for having an effective system of internal control - including an effective internal audit function - and 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. In discharging their responsibilities, Directors and senior management should have reasonable assurance that the system of internal control prevents or detects inaccurate, incomplete or unauthorized transactions; deficiencies in the safeguarding of assets; unreliable financial and regulatory reporting; and deviations from laws, regulations, and the institution's policies.

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 senior managers 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 assessed by units without business-line responsibilities, such as internal audit groups.

Directors should be confident that the internal audit function meets the demands posed by the institution's current and planned activities. Directors and senior managers should ensure that the following matters are reflected in their internal audit function.

Structure. Careful thought should be given to placement of the audit function in the institution's management structure. The function should be positioned so that Directors have confidence that the internal audit function will perform its duties with impartiality and not be unduly influenced by managers of day-to-day operations. Accordingly, the manager of internal audit should report directly to the board of Directors or its audit committee, which should oversee the internal audit function.[3] The board or its audit committee should develop objective performance criteria to evaluate the work of the internal audit function.[4]

Management, staffing, and audit quality. The Directors 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 responsibilities for operating the business. The manager of internal audit should be 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 and potential risk due to control deficiencies. They should be updated as needed to reflect changes to the system of internal control or work processes, and to incorporate new lines of business.

- The audit plan is based on the control risk assessment and 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 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 should be maintained that adequately document the work performed and support the audit report.

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.[5] 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. Institutions should consider conducting their internal audit activities in accordance with professional standards, such as the Institute for Internal Auditors' (IIA) *Standards for the Professional Practice of Internal Auditing*. These standards address the independence, professional proficiency, scope of work, performance of audit work, and management of internal audit.

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 the internal audit manager'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.[6]

Communication. To properly discharge their responsibility for internal control, Directors and senior management should foster forthright communications and critical examination of issues so that they will have knowledge of the internal auditor's findings and operating management's solutions to identified internal control 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 internal control weaknesses or other exceptions are being resolved expeditiously by management. Moreover, the audit committee should give the manager of internal audit the opportunity to discuss his or her findings without management being present.

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. The internal audit of the U.S. operations normally is performed by its U.S. domiciled audit function, head-office internal audit staff, or some combination thereof. 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.

Small Financial Institutions

An effective system of internal control, including an independent internal audit function, is a foundation for safe and sound operations, regardless of an institution's size. As discussed previously in this policy statement, Section 39 of the FDI Act requires each institution to 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 management's responsibility to carefully consider the level of auditing that will effectively monitor the internal control system after taking into account the audit function's costs and benefits. For many institutions that have reached a certain size or complexity of operations, the benefits derived from a full-time manager of internal audit or auditing staff more than outweigh its costs. However, for certain smaller institutions with few employees and less complex operations, 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 system of independent reviews of key internal controls. The employee conducting the review of a particular function should be independent of the function and able to report findings directly to the board or audit committee.

INTERNAL AUDIT OUTSOURCING ARRANGEMENTS[7]

Examples of Arrangements

An outsourcing arrangement is a contract between the institution and an outsourcing vendor to provide internal audit services. Outsourcing arrangements take many forms and are used by institutions of all sizes. The 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 those of electronic data processing and capital markets activities. Such uses are often referred to as "internal audit assistance" or "audit co-sourcing."

Some outsourcing arrangements may require an outsourcing vendor to perform virtually all internal audit work. Under such an arrangement, the institution may maintain a manager of internal audit and a very small internal audit staff. The outsourcing vendor assists staff in determining risks to be reviewed, recommends and performs audit procedures as approved by the internal audit manager, and reports its findings jointly with the internal audit manager to either the full board or its audit committee.

Additional Considerations for Internal Audit Outsourcing Arrangements

Even when outsourcing vendors provide internal audit services, the board of Directors and senior managers of an institution are responsible for ensuring that the system of internal control (including the internal audit function) operates effectively. 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 can occur.

To clearly set forth its duties from those of the outsourcing vendor, the institution should have a written contract, often referred to as an engagement letter. At a minimum, the contract should:

- Set the scope and frequency of work to be performed by the vendor;

- Set the manner and frequency of reporting to senior management and Directors about the status of contract work;

- Establish the protocol for changing the terms of the service contract, especially for expansion of audit work if significant issues are found;

- 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;

- State that examiners will be granted immediate and full access to the internal audit reports and related workpapers prepared by the outsourcing vendor;

- Prescribe the method for determining who bears the cost of consequential damages arising from errors, omissions and negligence; and

- State that outsourcing vendors that are subject to the independence guidance below will not perform management functions, make management decisions, or act or appear to act in a capacity equivalent to that of an employee.

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.

Communication. Communication between the internal audit function and Directors and senior management should not diminish because the bank 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 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.

Vendor Competence. Before entering an outsourcing arrangement the institution should perform enough due diligence to satisfy itself that the outsourcing vendor has sufficient staff qualified to perform the contracted work. 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 prior notice of staffing changes. Throughout the outsourcing arrangement, management should ensure that the outsourcing vendor maintains sufficient expertise to perform effectively its contractual obligations.

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 increases its operating risk. Because the arrangement might be suddenly terminated, the institution should have a contingency plan to mitigate any significant discontinuity in audit coverage, particularly for high risk areas. Planning for a successor to the prospective outsourcing vendor should be part of negotiating the latter's service contract.

Independence of the External Auditor

This section of the policy statement applies only to an outsourcing vendor who is a certified public accountant (CPA) and who performs a financial statement audit or some other service for the institution that requires independence under AICPA rules.[8]

Many institutions engage certified public accounting firms to audit their financial statements and furnish other attestation services requiring independence. A certified public accounting firm that provides other services for its client (such as consulting, benefits administration or acting as an outsourcing vendor) risks compromising the independence necessary to perform attestation services. The professional ethics committee of the American Institute of Certified Public Accountants (AICPA) has issued rulings and interpretations specifically addressing whether a certified public accountant that furnishes both audit outsourcing and external audit or other attestation services to a client can still be considered independent.[9]

Section 36 of the FDI Act and associated regulations require management of every insured depository institution with total assets of at least Ï500 million to obtain an annual audit of its financial statements by an independent public accountant, report to the banking agencies on the effectiveness of the institution's internal controls over financial reporting and on the institution's compliance with designated laws and regulations (management report), and obtain a report from an external auditor attesting to management's assertion about these internal controls (internal control attestation report). In order to satisfy these requirements, the institution's board of Directors must select an external auditor that will satisfy the independence requirements established by the AICPA, and relevant requirements and interpretations of the Securities and Exchange Commission.

Questions have been raised about whether external auditors who perform an audit of the institution's financial statements or provide any other service that requires independence can also perform internal audit services and still be considered independent. The federal banking agencies are concerned that outsourcing arrangements may involve activities that compromise, in fact or appearance, the independence of an external auditor.

The AICPA has issued guidance to CPAs (Interpretation 101-13 and related rulings) on independence that addresses these issues. Under Interpretation 101-13, the CPA's performance of services required by the outsourcing arrangement "would not be considered to impair independence with respect to [an institution] for which the [CPA] also performs a service requiring independence, provided that [the CPA or the CPA's firm] does not act or appear to act in a capacity equivalent to a member of [the institution's] management or as an employee." The interpretation lists activities that would be considered to compromise a CPA's independence. Included are activities that involve the CPA "authorizing, executing, or consummating transactions or otherwise exercising authority on behalf of the client." [10]

Also, the AICPA's Ruling No.103 sets forth three criteria for evaluating the independence of a CPA who concurrently provides internal audit outsourcing services and the internal control attestation report under Section 36 of the FDI Act. One criterion requires that management "does not rely on [the CPA's] work as the primary basis for its assertion and accordingly has (a) evaluated the results of its ongoing monitoring procedures built into the normal recurring activities of the entity (including regular management and supervisory activities) and (b) evaluated the findings and results of the [CPA's] work and other separate evaluations of controls, if any." Accordingly, a CPA's independence would be impaired if the CPA provides

the *primary* support for management's assertion on the effectiveness of internal control over financial reporting. A copy of the interpretation and rulings is attached to this policy statement. *Agencies' Views on Independence.* The agencies believe that other actions compromise independence in addition to those in Interpretation 101-13. Such actions include:[11]

- Contributing in a decision-making capacity or otherwise actively participating (e.g., advocating positions or actions rather than merely advising) in committees, task forces, and meetings that determine the institution's strategic direction; and

- Contributing in a decision-making capacity to the design, implementation, and evaluation of new products, services, internal controls or software that are significant to the institution's business activities.

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 the internal audit work, regardless of whether it is performed by the institution's employees or by an outsourcing vendor. Specifically, examiners will consider whether:

- The board of Directors (or 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 function's risk assessment, plans and programs are appropriate for the institution's activities;

- 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 interested managers and Directors;

- The institution has promptly responded to identified internal control weaknesses;

- Management and the board of Directors use reasonable standards when assessing the performance of internal audit;

- The internal audit plan and program have been adjusted for significant changes in the institution's environment, structure, activities, risk exposures or systems;

- The activities of internal audit are consistent with the long-range goals of the institution and are responsive to its internal control needs; 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.2

The examiner should assess the competence of the institution's internal audit staff and management by considering the education and professional background of the principal internal auditors.

Additional Aspects of the Examiner's Review of Outsourcing Arrangements. Examiners should also 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 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 function is effectively managed by the institution;
- The arrangement with the outsourcing vendor compromises its role as external auditor; 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.

If the examiner's evaluation of the outsourcing arrangement indicates that the outsourcing arrangement has diminished the quality of the institution's internal audit function, the examiner should consider adjusting the scope of the examination. The examiner also should bring that matter to the attention of senior management and the board of Directors and consider it in the institution's management and composite ratings.

Concerns about Auditor Independence

When an examiner's initial review of an outsourcing arrangement raises doubts about the external auditor's independence, the examiner first should ask the institution and the external auditor to demonstrate that the arrangement has not compromised the auditor's independence. If the examiner's concerns are not adequately addressed, the examiner should discuss the matter with appropriate agency staff.

If the agency's staff concurs that the independence of the external auditor 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. These actions may include referring the external auditor to the state board of accountancy and the AICPA for possible ethics violations, and barring the external auditor from engagements with regulated institutions. Moreover, the agency may conclude that the organization's external auditing program is inadequate and that it does not comply with auditing and reporting requirements, including Section 36 of the FDI Act and related guidance and regulations.

---

[1]In summary, internal control is a process, brought about by an institution's board of Directors, management and other personnel, 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 is essential to achieving the internal control objectives.

[2]For national banks, Appendix A to Part 30; for state member banks, Appendix D to Part 208; for state nonmember banks, Appendix A to Part 364; for savings associations, Appendix A to Part 570.

[3]Institutions subject to Section 36 of the FDI Act must maintain independent audit committees (i.e., comprised of Directors that are not members of management). For institutions not subject to an audit committee requirement, the board of Directors can fulfill the audit committee responsibilities discussed in this policy statement.

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

[5]The form and content of 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 many larger departments require more formal and comprehensive written guidance.

[6]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 (c) new lines of business, products or technologies; (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).

[7]The guidance in the preceding section of this policy statement ("The Internal Audit Function") also applies to internal audit outsourcing arrangements.

[8]Although outsourcing arrangements involving CPAs who are not performing external audit or attestation services for a client are not subject to this independence guidance, they are subject to the other sections of this policy statement.

[9]In May 1997, the AICPA and the Securities and Exchange Commission announced the formation of the Independence Standards Board (ISB), a private-sector body intended to establish independence standards for auditors of public companies. Any future standards established by the ISB should be considered in initiating or evaluating outsourcing arrangements with CPAs.

[10]Other examples of outsourcing activities that would compromise a CPA's independence that are listed in Interpretation 101-13 include:

- Performing ongoing monitoring activities or control activities (i.e., reviewing loan originations as part of the client's approval process or reviewing customer credit information as part of the customer's sales authorization process) that affect the execution of transactions or ensure that transactions are properly executed, accounted for, or both and performing routine activities in connection with the client's operating or production processes that are equivalent to those of an ongoing compliance or quality control function;

- Reporting to the board of Directors or audit committee on behalf of management or the individual responsible for the internal audit function;

- Preparing source documents on transactions;

- Having custody of assets;

- Approving or being responsible for the overall internal audit work plan, including the determination of the internal audit risk and scope, project priorities, and frequency of performance of audit procedures;

- Being connected with the client in any capacity equivalent to a member of client management or as an employee (for example, being listed as an employee in client Directories or other client publications, permitting himself or herself to be referred to by title or description as supervising or being in charge of the client's internal audit function, or using the client's letterhead or internal correspondence forms in communications).

[11]The agencies believe that this guidance is consistent with the AICPA interpretation.