The Institute of Internal Auditors

INTERNAL AUDITING'S ROLE IN SECTIONS 302 AND 404 OF THE U.S. SARBANES-OXLEY ACT OF 2002

May 26, 2004

Internal Auditing's Role in Sections 302 and 404 of the Sarbanes-Oxley Act

Table of Contents

Internal Auditing's Role in Sections 302 and 404 of the Sarbanes-Oxley Act

Executive Overview

As companies have begun the process of implementing compliance with the reporting requirements of Sections 302 and 404 of the U.S. Sarbanes-Oxley Act of 2002 (Act), internal auditors have been confronted with a range of questions and issues related to their role and involvement in these initiatives. Section 404 of Sarbanes-Oxley requires management's development and monitoring of procedures and controls for making their required assertion about the adequacy of internal controls over financial reporting, as well as the required attestation by an external auditor of management's assertion. Section 302 requires management's quarterly certification of not only financial reporting controls, but also disclosure controls and procedures.

It is management's responsibility to ensure the organization is in compliance with the requirements of Sections 302 and 404 and other requirements of the Act, and this responsibility cannot be delegated or abdicated. Support for management in the discharge of these responsibilities is a legitimate role for internal auditors. The internal auditors' role in their organization's Sarbanes-Oxley project can be significant, but also must be compatible with the overall mission and charter of the internal audit function. Regardless of the level and type of involvement selected, it should not impair the objectivity and capabilities of the internal audit function for covering the major risk areas of their organization. Internal auditors are frequently pressured to be extensively involved in the full compendium of Sarbanes-Oxley project efforts as the work is within the natural domain of expertise of internal auditing.

The Institute of Internal Auditors' (IIA) definition of internal auditing is: "Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes." The IIA's *International Standards for the Professional Practice of Internal Auditing* (*Standards)* specifies that the chief audit executive (CAE) establish risk-based plans to determine the priorities of the internal audit activity, consistent with the organization's goals. Internal auditors should consider Sarbanes-Oxley noncompliance as a risk to the organization, along with all other risks, in their risk assessment process for determining internal audit plans and focus of their efforts. This audit risk assessment should also be reevaluated each year and audit's assessment results should be disclosed to and discussed with the audit committee.

The CAE should ensure that the audit committee is kept up to date on the role and activities of internal audit in the company's efforts to comply with Section 404. Instances where independence or objectivity will be impaired by the role that internal audit activity assumes should be discussed with the audit committee prior to assuming this role. In addition, the implications, as well as any impact on both current and future audit plans because of devoting resources to assisting in Section 404 compliance efforts, should be discussed with the audit committee. Where the internal audit activity's

objectivity is impaired, the CAE and the board should consider how this impairment affects the ability to perform future internal audit engagements.

An organization with an established internal audit function operating in full compliance with the definition of internal auditing and its accompanying standards is already well equipped to meet the challenge of good governance and transparency of internal control effectiveness and efficiency. This delicate but essential balance between management's responsibility regarding internal control monitoring and disclosure and the internal audit mission and its efforts has been successfully experienced for many years in industries and countries worldwide where similar regulations have been in place for some time.

Sarbanes-Oxley promotes risk management and governance processes within an organization over which, according to the *Standards*, internal audit should be in a position to provide assurance and consulting without impairing objectivity and independence. Management is responsible for developing the processes needed to ensure the company is in compliance with Sarbanes-Oxley. Internal audit's role should ideally be one of support through consulting and assurance.

Purpose

Internal auditors have been confronted with a range of questions and issues related to their role and involvement in Sections 302 and 404 initiatives. These questions include both short-term issues during the implementation phase of reporting processes, as well as longer-term questions on the role and responsibilities of internal audit in this process. The purpose of this paper is to provide CAEs with relevant guidance to assist them in responding to these questions in a manner that is most helpful to their organizations while maintaining the ultimate objectivity and independence that is required by the *Standards.*

The IIA recognizes that various organizations will respond differently to the reporting requirements and that the internal audit activity will play various roles, especially in the short-term. However, this paper strives to describe an *ideal role* for the internal audit activity that best fits with the *Standards*. The intent of this paper is to present practical guidance and compliance is not required under the *Standards.*

Background

Section 404 of Sarbanes-Oxley requires management's development and monitoring of procedures and controls for making their required assertion regarding the adequacy of internal controls over financial reporting, as well as the required attestation by an external auditor, regarding management's assertion. Section 302 deals with management's quarterly certification of not only financial reporting controls, but also disclosure controls and procedures. The requirements of Sarbanes-Oxley place responsibilities on both management and independent accountants.

The *Standards* require that the internal audit activity evaluate and contribute to the improvement of the organization's risk management, control, and governance processes through consulting and assurance activities. The process utilized by an internal audit activity should be designed to provide reasonable assurance regarding the organization's

reliability and integrity of financial and operational information, effectiveness and efficiency of operations, safeguarding of assets, and compliance with laws, regulations, and contracts. Consequently, the role of internal auditing activity should be one of support through consulting and assurance activities as outlined in the *Standards* as well as the Practice Advisories.

While this guidance only addresses the role of the internal audit activity with regard to Sections 302 and 404 of Sarbanes-Oxley, the CAE should ensure that the internal audit activity's assessment of organizational risk extends beyond financial reporting and disclosure processes. If CAEs are to provide audit committees and senior management with an independent evaluation of risks and controls and contribution to risk management, control, and governance as outlined in the *Standards*, then the internal audit activity must maintain and effectively utilize those resources necessary to execute work in addition to that which is required for purposes of assisting management in the fulfillment of its responsibilities with respect to the financial reporting and disclosure processes.

Summary of Phases, Activities, and Lead Responsibilities for Section 404 Efforts

To achieve the objectives of the Sarbanes-Oxley Section 404, generally a major corporate initiative consisting of several phases and specific key activities within each phase is organized. Specific accountabilities for each activity also must be assigned. The following table presents the typical phases, activities, and person(s) responsible. It also summarizes the recommended roles for internal auditors.

Phase/Activity	**Lead Responsibility**	**Recommended Internal Auditor Roles**
Planning		
Plan	Project Sponsor	Provide advice and recommendations. Participate in project team planning.
Scope	Project Team	Provide advice and recommendations. Participate in project team planning.
Execution		
Document	Line Managers; &/or Project Team; &/or Specialists	Advise management regarding processes to be used. Perform quality assurance reviews.
Evaluation & Testing	Line Managers; Project Team; Specialists	Independent assessor of management's documentation and testing. Perform effectiveness testing (for highest reliance by external auditors).
Issues	Project Team and Line Managers	Identify control gaps. Facilitate management discussions.
Corrective Action	Line Managers	Perform follow-up reviews.
Monitoring Systems	Senior Management	Perform follow-up reviews.

Phase/Activity	Lead Responsibility	Recommended Internal Auditor Roles
Reporting		
Management Reporting	Senior Management and Line Managers	Facilitate determinations (to report). Provide advice.
External Audit Reporting	External Auditor	Act as a coordinator between management and the external auditor.
Monitoring		
Ongoing Monitoring	Senior Management	Perform follow-up services.
Periodic Assessment	Project Team &/or Line Managers	Perform periodic audits.

Summary of Roles of Audit Committees, Management, and External Auditors

Sarbanes-Oxley specifies the various roles of management, the audit committee, and the external auditors; however, the Act does not specifically address the role of internal auditors.

Audit Committee

Although Sections 302 and 404 of the Sarbanes-Oxley Act of 2002 do not assign specific responsibilities to audit committees, Sections 301 and 407 establish broad standards for and disclosures regarding audit committees.

Section 301 establishes certain general standards with which audit committee members are required to comply. These standards are:

- Except for board of director fees, audit committee members may not accept consulting, advisory, or other compensatory fees from the issuer and its subsidiaries. Audit committee members must also not be an affiliated person of the issuer and its subsidiaries.
- Audit committees must be directly responsible for the appointment, compensation, retention, and oversight of all registered public accounting firms that prepare or issue audit reports or perform other audit, review, or attest services for the issuer.
- Audit committees must establish procedures for receiving, retaining, and addressing complaints received by the issuer related to accounting, internal controls, and auditing.
- Audit committees must have the authority to engage independent counsel, as they deem necessary.
- Issuers must provide the audit committee with appropriate funding to enable it to fulfill its responsibilities.

Section 407 requires an issuer to disclose in its annual report whether it has at least one "audit committee financial expert" serving on its audit committee, and if so, whether the expert is independent of management. An issuer that does not have an audit committee financial expert must disclose this fact and explain why.

Management

Section 302 requires management to evaluate and report on the effectiveness of disclosure controls and procedures with respect to the quarterly and annual reports. The principal executive and financial officers must certify that:

- They have reviewed the report, believe that the report does not contain untrue statements or omit material facts, and the financial statements and other financial information are fairly presented.
- They (1) are responsible for establishing and maintaining disclosure controls and procedures; (2) have designed such disclosure controls and procedures to ensure that they are aware of material information; (3) have evaluated the effectiveness of the company's disclosure controls and procedures; and (4) have presented in the report their conclusions about the effectiveness of the disclosure controls and procedures.
- They have disclosed to the auditors and audit committee (1) "all significant deficiencies in the design or operation of internal controls which could adversely affect the issuer's ability to record, process, summarize, and report financial data and have identified for the issuer's auditors any material weaknesses in internal controls;" and (2) "any fraud, whether or not material, that involves management or other employees who have a significant role in the company's internal controls."
- They have indicated whether there have been "significant changes in internal controls over financial reporting or in other factors that could significantly affect internal controls subsequent to the date of their evaluation, including any corrective actions with regard to significant deficiencies and material weaknesses."

Section 404 of Sarbanes-Oxley requires management to document and evaluate the design and operation, and report on the effectiveness, of its internal control over financial reporting. The internal control report must be incorporated into the annual reports and must include the following components:

- Management's recognition of its responsibility for establishing and maintaining adequate internal controls and procedures for financial reporting.
- The framework used by management in its evaluation.
- Management's assessment of the effectiveness of the company's internal control over financial reporting. The assessment must include disclosure of any "material weaknesses" in the company's internal control over financial reporting identified by management.
- A statement indicating that the issuer's external auditors have issued an attestation report on management's assessment of effectiveness of internal control over financial reporting.
- The issuer must also include in its annual report the attestation report of the external auditors.

External Auditors

Section 404 of Sarbanes-Oxley requires an issuer's external auditors to evaluate management's assessment of internal controls and to issue a report thereon. In addition, Title 2 of Sarbanes-Oxley establishes certain independence requirements for external auditors.

- Section 201 makes it unlawful for an issuer's external auditor to provide certain types of non-audit services to an issuer concurrent with the audit.
- Section 203 requires the external auditor to rotate every five years the lead audit or coordinating partner and the reviewing partner on the engagement.
- Section 204 requires the external auditor to report to the audit committee: "(1) all critical accounting policies and practices to be used; (2) all alternative treatments of financial information within generally accepted accounting principles that have been discussed with management officials of the issuer, ramifications of the use of such alternative disclosures and treatments, and the treatment preferred by the registered public accounting firm; and (3) other material written communications between the registered public accounting firm and the management of the issuer, such as any management letter or schedule of unadjusted differences."

Recommended Role of Internal Audit

The services that can be performed by the internal audit activity in meeting the requirements of Sections 302 and 404 should not interfere with the requirement of the *Standards* for the internal auditor's independence and objectivity. The *Standards* provide the framework for an effective internal audit activity, and the recommended role of the internal audit activity in aiding a company in meeting its Sections 302 and 404 obligations should be consistent with the *Standards*. This section describes the internal audit activities that are considered to be consistent with the objectives of the *Standards*.

Activities that are included in the internal auditor's recommended role in supporting the organization in meeting the requirements of Sections 302 and 404 include:

- Project Oversight
- Consulting and Project Support
- Ongoing Monitoring and Testing
- Project Audit

Management is responsible for implementing the processes necessary to meet the regulatory requirements of Sarbanes-Oxley. The role of the internal auditor should support management in carrying out its responsibilities.

<u>Project Oversight</u>

- Participate on project steering committee providing advice and recommendations to the project team and monitoring progress and direction of the project.
- Act as facilitator between external auditor and management.

Consulting and Project Support

- Provide existing internal audit documentation for processes under scope.
- Advise on best practices — documentation standards, tools, and test strategies.
- Support management and process owner training on project and risk and control awareness.
- Perform quality assurance review of process documentation and key controls prior to handoff to the external auditor.

Ongoing Monitoring and Testing

- Advise management regarding the design, scope, and frequency of tests to be performed.
- Independent assessor of management testing and assessment processes.
- Perform tests of management's basis for assertions.
- Perform effectiveness testing (for highest reliance by external auditors).
- Aid in identifying control gaps and review management plans for correcting control gaps.
- Perform follow-up reviews to ascertain whether control gaps have been adequately addressed.
- Act as coordinator between management and the external auditor as to discussions of scope and testing plans.
- Participate in disclosure committee to ensure that results of ongoing internal audit activities and other examination activities, such as external regulatory examinations, are brought to the committee for disclosure consideration.

Additionally, residual benefits to the organization derived from internal audit's recommended role above include enhanced management awareness of risks and controls, stronger control environment, and potential reduction in external audit fees.

Internal audit may fulfill a traditional assurance role for senior management, the audit committee, the board of directors, and other stakeholders, i.e., that of completing a project audit.

Project Audit

- Assist in ensuring that corporate initiatives are well managed and have a positive impact on an organization. Their assurance role supports senior management, the audit committee, the board of directors, and other stakeholders.
- Use a risk-based approach in planning the many possible activities regarding project audits. Audit best practices suggest internal auditors should be involved throughout a project's life cycle — not just in post-implementation audits.

Practical Considerations

It is not always possible or practical for the internal audit activity to achieve the ideal role in the areas of assisting management with compliance with Sarbanes-Oxley. Each organization will have its own set of circumstances relating to internal controls and its own set of resource constraints, such as personnel, time, information technology, and geographic dispersion.

Different situations and different resource constraints may result in a number of roles for the internal audit activity. In considering which role(s) are appropriate for the internal audit activity, the following general factors should be considered:

- Having responsibility for specific operations results is a presumption of impairment of objectivity regarding that operation (Attribute Standard 1130.A1). Whether an internal auditor has taken on responsibility for specific operations will depend on the situation. In general, internal auditors who actively participate in making or directing key management decisions will have impaired objectivity.
- An internal auditor's objectivity is not impaired when the internal auditor recommends standards of control for systems or review procedures before they are implemented. The auditor's objectivity is considered to be impaired if the internal auditor designs, installs, drafts procedures for, or operates such systems. (Practice Advisory A1130.A1-1)
- Consulting on internal control matters is a normal role for internal auditors and does not impair independence or objectivity. However, making key management decisions impairs the internal auditor's independence or objectivity. (Practice Advisory 1000.C1-1)
- Devoting significant amounts of effort to a non-assurance activity may not impair independence; however, the CAE should consider the impact (including risk) of performing non-assurance activities on completing the otherwise planned assurance engagements.

The remainder of this section discusses the potential services the internal audit activity may be requested to provide and the implication of providing those services.

A. Internal Auditing Activity as a Source of Consultants

Internal auditors acting in a consulting role may be asked to assist the organization in identifying, evaluating, and implementing risk and control assessment methodologies as well as recommending controls to address related risks. However, decisions to adopt or implement recommendations made as a result of an internal audit advisory service should be made by management.

An internal auditor may be asked to participate in the design and implementation of a new process for management to assess their internal controls over financial reporting. If the internal auditor's activities are limited to evaluating the new processes and defining a reference guide on recommended controls addressing related risks, the internal auditor's objectivity is not likely impaired. Additionally, if the internal auditor is a member of the project team which selects the assessment methodology and tools, and/or defines the documentation standards management is going to use, objectivity is not likely considered impaired. On the other hand, if the internal auditor implements new processes to remediate control gaps, the internal auditor's objectivity may be considered impaired.

B. Internal Audit Activity as a Source of Resources for Documentation and/or Testing

If management has not documented their control environment and does not have adequate resources needed to do so within the time period required, then internal auditors may be requested to aid management in documenting their internal controls. If the internal auditor is working closely with management in documenting internal controls and slides into more of a decision making role (e.g., implementing internal controls during the documentation process), then objectivity will be impaired.

Section 404 rules require management to test the design and operating effectiveness of its internal controls over financial reporting, and reach an opinion as to whether they are effective to support the assertion they are required to provide under the law. Ideally, management should design the test of controls to validate the effectiveness of such controls, and testing should be performed by someone objective or other than the owners or operators. The internal audit activity may aid management in the design or execution of tests for control effectiveness. The degree to which the internal audit activities constitute management's testing of controls should be clearly specified and agreed to by management, internal audit, and the audit committee. In all cases, management should make the final decision on control design and operating effectiveness, whether and what to remediate, and the sufficiency of information produced from which their assertions are to be made.

C. Internal Audit Activity as the Source for the Lead Project Manager

Internal auditors frequently are skilled at managing large or complicated projects, ensuring key deliverables are produced on time. The internal auditor may be asked to take on the role of lead project manager for all or part of the efforts related to complying with Section 404. A project manager may generally be responsible for monitoring progress of a project, arranging for appropriate communication of project results during the project, and monitoring adherence to the established timetable. If the internal auditor's role is restricted to these administrative tasks, objectivity would not likely be impaired. However, if the project manager role extends to being the primary decision maker as to acceptability of work product, approving successful completion of stages of the project, authorizing redirection of resources within the project team, or other similar management activities, the internal auditor's objectivity is impaired.

D. Internal Audit Activity as a Source of Training or Information about Controls

Internal auditors may provide training and/or information on internal control identification and assessment, risk assessment, and test plan development without impairment to objectivity. As the organization's control experts, this would be a natural role.

E. Internal Audit Activity as a Source for Control Self-assessment

The internal audit activity is often the source for expertise regarding control self-assessment (CSA) and for skilled facilitators. CSA may be used as an effective and efficient means for management to document and/or assess controls. If an internal auditor provides information, training, and/or facilitates a CSA, objectivity is not likely to be impaired. However, if during the CSA the internal auditor owns the assessment or is the main source of the documentation, then objectivity is impaired.

F. Internal Audit activity as a Certifier in the Disclosure Process

The internal audit activity may be asked to complete some type of certification or to issue an opinion on financial controls as part of management's Sections 302 and 404 processes. The CAE should ensure that any certification or opinion is supported by adequate, appropriate audit evidence as required by the *Standards* to support the certification and/or opinion.

Additionally, under the requirements of Section 404, the external auditor will perform tests of management's assertion that key financial controls have been identified, designed appropriately, and management has a sufficient basis to know that the key controls are functioning. External auditors would likely perform extensive testing to attest that management's assertions are appropriate. According to the Public Company Accounting Oversight Board's Auditing Standard, in order for the external auditor to use testing results performed by others to alter the nature, timing, and extent of the tests of controls, he/she should assess the degree of objectivity and competence of the individuals performing the test of controls. If an internal audit activity maintains its independence and objectivity, the external auditor could use their work to the greatest extent an auditor could use the work of others; therefore, reducing the extent of testing, which may otherwise be performed by the external auditor. In this situation, the organization's external auditor fees may be reduced.

Managing Impairment

The CAE should ensure that the audit committee is kept up to date on the role and activities of internal audit in the organization's efforts to comply with Section 404. Instances where objectivity will be impaired by the role the internal audit activity assumes should be discussed with the audit committee prior to assuming this role. In addition, the implications as well as any impact to both current and future audit plans because of devoting resources to assisting in Section 404 compliance efforts should be discussed with the audit committee.

Where the internal audit activity's objectivity is impaired, the CAE and the board need to consider how this impairment affects the ability to perform future internal audit engagements.

******

Sarbanes-Oxley promotes risk management and governance processes within an organization over which, according to the *Standards*, internal audit should be in a position to provide assurance and consulting without impairing objectivity and independence. Management is responsible for developing the processes needed to ensure the company is in compliance with Sarbanes-Oxley. The internal auditing activity's role should ideally be one of support through consulting and assurance.