The Institute of Internal Auditors

June 29, 2005

David A. Richards, CIA
President

Tel: +1 407 937 1200
drichards@theiia.org

John Stevenson, Secretary
Ontario Securities Commission
20 Queen Street West
Suite 1900, Box 55
Toronto, Ontario M5H 3S8
Fax: (416) 593-2318 - E-mail: jstevenson@osc.gov.on.ca

Anne-Marie Beaudoin, Directrice du secretariat
Autorité des marchés financiers
Tour de la Bourse
800, square Victoria
C.P. 246, 22e étage
Montréal, Québec, H4Z 1G3
Fax: (514) 864-6381 - E-mail: consultation-en-cours@lautorite.com

Re: Comments on Proposed Instruments 52-109 and 52-111

Dear Mr. Stevenson and Ms. Anne-Marie Beaudoin:

The Institute of Internal Auditors (IIA) applauds the efforts of the Ontario Securities Commission (OSC) and other securities regulatory authorities involved (the Participating Jurisdictions) to promote effective corporate governance in Canada. The IIA has long advocated that good governance and accurate financial reporting emanate from the balanced interaction of board members, executives, external auditors, and internal auditors.

Clearly, the first year's implementation of Sarbanes-Oxley in the U.S. has provided many lessons learned. A recent report issued by The IIA's Research Foundation concluded through a comprehensive survey that there have been many control improvements as a result of implementing Sarbanes-Oxley. Most notable are a more engaged control environment, with active participation by the board, audit committee and management, and a broader understanding of controls by personnel and management throughout the organization. (See copy of research report in Attachment C.)

Representing more than 108,000 members worldwide – approximately 5,000 of whom are in 11 chapters located across Canada – The IIA is the global voice, acknowledged leader, and recognized authority of the internal audit profession. The IIA maintains the *International Standards for the Professional Practice of Internal Auditing (Standards)*, which are recognized throughout the world.

Global Headquarters
247 Maitland Avenue
Altamonte Springs, FL
32701-4201 U.S.A.
Tel: +1-407-937-1100
Fax: +1-407-937-1101
www.theiia.org

Internal Auditing's Role in Corporate Governance
We believe that internal auditors play a vital role in improving corporate governance, risk management, and control processes because of their unique position within their organizations. The IIA's definition of internal auditing acknowledges this role in corporate governance:

"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."

Since the adoption of this definition in 1999, The IIA has intensified its efforts to contribute to the reform of governance practices of public companies around the world. IIA leaders in Canada and staff at global headquarters contributed to the development of this response.

IIA's Recommendations (further comments are provided in Attachment A)

1. Consider the importance of enterprise-wide risk management and controls other than those limited to financial reporting. Good governance is an enterprise wide effort and since other jurisdictions have adopted a much wider view, the Participating Jurisdictions should consider what guidance should be provided to management to ensure all aspects of strong governance are considered and addressed by publicly-traded organizations.

2. In the U.S. the lack of detailed guidance by the SEC to management on what is expected of them regarding the control assessment process has caused management in many cases to turn to their external audit to obtain guidance on what is acceptable. This has resulted in the PCAOB setting the standard for management on what is required to perform a control assessment – rather than management setting the standard based on the guidance from the SEC. In Canada, the Participating Jurisdictions should consider the regulatory efforts in the UK with their Combined Code and the approach of "comply or explain", i.e. in the UK, fairly detailed guidelines are provided to management.

3. The external auditor's reliance on the use of work of a competent and independent internal audit function should be encouraged. The IIA believes an organization with an established internal audit function operating in accordance with The IIA's *International Standards for the Professional Practice of Internal Auditing* is well equipped to meet the challenge of good governance. Using the work of internal auditors, where appropriate, would increase efficiencies in testing and reduce costs. Where internal audit has done testing or performed walkthroughs that fall within the scope of the financial reporting controls, external audit should rely on their work.

Internal Auditing's Role in Sections 302 and 404 of the U.S. Sarbanes-Oxley Act of 2002
We have enclosed The IIA's position paper "*Internal Auditing's Role in Sections 302 and 404 of the U.S. Sarbanes-Oxley Act of 2002"* (Attachment B). The IIA strongly believes that internal auditing can contribute significantly to the organization's efforts to improve internal controls and financial reporting. Management is responsible for implementing the processes necessary to meet the regulatory requirements of Sarbanes-Oxley. The internal auditor should support management in carrying out its responsibilities but not take on management's responsibilities for documenting controls or implementing systems of internal controls. In Canada, we believe the internal audit function can perform a similar role as in the U.S. and will be issuing a similar position paper adopted for the Canadian environment – once the Participating Jurisdictions rules are finalized and become operational.

Other Information
The IIA has recently responded to the SEC regarding the first year's lessons learned and recommendations for enhancement and we include this paper in Attachment D for your consideration. Also, we have enclosed our most recent position paper entitled, "Practical Considerations Regarding Internal Auditing Expressing an Opinion on Internal Control" which was issued to our members (Attachment E).

We appreciate the opportunity to express our views on these important matters and welcome the opportunity to discuss any and all issues with you, at any time.

Best regards,

David A. Richards, CIA

Attachments

A - Additional comments by The IIA

B - *Internal Auditing's Role in Sections 302 and 404 of the U.S. Sarbanes-Oxley Act of 2002* – An Institute of Internal Auditors' position paper.

C - *Sarbanes-Oxley Section 404 Work - Looking at the Benefits* – An Institute of Internal Auditors Research Foundation report.

D - *IIA's submission to the SEC – March 31, 2005*.

E - Practical Considerations Regarding Internal Auditing Expressing an Opinion on Internal Control - An Institute of Internal Auditors' position paper.

IIA Affiliated Canadian Chapters:
Alberta: Calgary and Edmonton
Manitoba: Winnipeg
Nova Scotia: Maritime (Canada)
Quebec: Montreal and Quebec City
British Columbia: Vancouver
Newfoundland: Newfoundland & Labrador
Ontario: Ottawa and Toronto
Saskatchewan (Regina): Saskatchewan

THE INSTITUTE OF INTERNAL AUDITORS

Attachment A

Additional comments and answers to specific questions raised in 52-111

General Support

The Institute of Internal Auditors (IIA) is supportive of the Participating Jurisdictions proposals and the recommendations contained in the various instruments. The proposed rules will help those charged with governance responsibilities and increase the confidence of stakeholders. A strong and comprehensive plan of action for implementing the final rules will be vital in obtaining buy-in from the business community. Opportunities exist, however, for changes and additions to enhance the proposal. Our suggestions and answers to several questions posed in the *Requests for Comment* follow.

The IIA believes that promulgating a strong, uniform code for corporate governance and requiring board reporting on the extent of compliance with this code are vital steps toward strengthening corporate governance, improving transparency, and restoring investor confidence. Generally accepted governance principles would be of significant value as benchmarks against which to measure and report on the fulfillment of fiduciary duties by all parties in the governance process. A uniform code of corporate governance would also help foster the high levels of integrity expected of officials of all public companies.

The IIA's response to specific 52-111 questions follows.

1. Do you agree that the Proposed Internal Control Instrument should apply to all reporting issuers other than investment funds and venture issuers? If not, which issuers do you believe should be subject to the Proposed Internal Control Instrument?

No. The Proposed Internal Control Instrument should apply to all reporting issuers including investment funds and venture issuers.

2. Do you believe that venture issuers should be subject to different requirements relating to internal control over financial reporting beyond what is required by the Revised Certification Materials? If so, what should be the nature of any different requirements?

No, venture issuers should be required to comply with the same rules as other listed companies as these entities can be higher risk and public money is still involved.

3. Should the term "management" be formally defined? If so, what would be an appropriate definition?

No need to further define management.

4. If "management" is not defined, is the guidance in the Proposed Internal Control Policy adequate and appropriate?

Yes.

Response to the 52-111 questions (cont'd).

5. Is the guidance set out in the Proposed Internal Control Policy with respect to the scope of the evaluation of internal control over financial reporting in relation to each of the circumstances set out above adequate and appropriate?

More definition required for "key controls" and " materiality".

6. Are there any other control frameworks that should be identified in the Proposed Internal Control Policy as satisfying the criteria for a suitable control framework?

No need to define other control frameworks.

7. Are there any specific aspects of the identified control frameworks on which additional guidance is required to assist in their application by issuers that have limited formal structures for internal control over financial reporting?

Yes. COSO has a small business task force which is currently developing guidance for smaller companies with an expected exposure draft being available during July, 2005.

8. Is the guidance in the Proposed Internal Control Policy regarding the content of the evidence adequate and appropriate?

Yes.

9. Are the requirements in the Proposed Internal Control Instrument regarding the manner in which the evidence must be maintained adequate and appropriate? Is the guidance in the Proposed Internal Control Policy regarding the manner in which the evidence may be maintained adequate and appropriate?

Yes

10. Is the requirement in the Proposed Internal Control Instrument on the period of time during which the evidence must be maintained adequate and appropriate?

Yes

11. Is it appropriate to require disclosure of any limitations in management's assessment of the effectiveness of an issuer's internal control over financial reporting extending into a joint venture, VIE or acquired business? If not, are there alternative ways of providing transparency with respect to any limitations in management's assessment?

Yes

12. Are there any other circumstances under which management may reasonably limit its assessment? Should disclosure of these circumstances be required?

No examples were identified but if it does occur disclosure should be required.

Response to the 52-111 questions (cont'd).

13. Are the exemptions from the Proposed Internal Control Instrument appropriate?

Yes, except that it should apply to all reporting issuers including investment funds and venture issuers.

14. Are there any other classes of issuers that should be exempt from the Proposed Internal Control Instrument?

No

15. Is the phased-in implementation of the Proposed Internal Control Instrument appropriate?

Yes, however, four categories may be too many different deadlines, i.e. consideration should be given to one for large (≥$250,000,000) and one for small (<$250,000,000). We also believe the initial deadline is too soon and should be moved back to June 30, 2007.

16. Does the phased-in implementation adequately address the concerns regarding the cost and limited availability of appropriate expertise within reporting issuers and among external advisors and auditors? If not, how can these concerns be addressed?

Yes, the recommended solution is to extend the deadline. Resources are in short supply currently and this will continue in the short term.

17. Are there any costs or benefits associated with the Proposed Internal Control Materials that have not been identified in the Internal Control CBA? If so, what are they?

Hidden costs may include staff hiring requirements, increased salary levels required, management focus on internal controls rather then strategic management of the organization, and external audit firms staffing challenges.

18. Do you believe that the benefits (both quantifiable and unquantifiable) justify the costs of compliance (both quantifiable and unquantifiable) for:

(a) issuers with a market capitalization of less than $75 million?

(b) issuers with a market capitalization of $75 million or more but less than $250 million?

(c) issuers with a market capitalization of $250 million or more but less than $500 million?

(d) issuers with a market capitalization of greater than $500 million?

(e) all issuers? (Why?)

Long term benefits will probably justify the costs involved. Short term the cost benefit will be much more challenging. Also refer to the recent IIA research report on cost benefits regarding the implementation of Sarbanes requirements in the U.S. (Appendix C).

Response to the 52-111 questions (cont'd).

19. Do you agree with our assessment of the identified alternatives?

More commentary should be provided for Alternatives 2 and 4, i.e. the focus of management and the external auditors need to be more risk-based and less checklist. This point should be clearly articulated and focus on those areas where inherent and residual risk are highest. Note: the recent PCAOB and SEC clarifying statement on May 16th provide an excellent overview of this specific issue.

20. What other alternatives, if any, would achieve the objectives identified above?

No new alternatives suggested, see reply to #19 re suggested enhancements to alternatives provided.

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.

Sarbanes-Oxley Section 404 Work

Looking at the Benefits

by

Larry E. Rittenberg, Ph.D., CIA, CPA
Ernst & Young Professor of Accounting
University of Wisconsin

and

Patricia K. Miller, CIA, CPA, CISA
Partner, Deloitte & Touche LLP
Vice-Chairman, Professional Practices, IIA

January 2005

The IIA Research Foundation

Disclosure

The IIARF publishes this document for informational and educational purposes. This document is intended to provide information, but is not a substitute for legal or accounting advice. The IIARF does not provide such advice and makes no warranty as to any legal or accounting results through its publication of this document. When legal or accounting issues arise, professional assistance should be sought and retained.

The Professional Practices Framework for Internal Auditing (PPF) was designed by The IIA Board of Directors' Guidance Task Force to appropriately organize the full range of existing and developing practice guidance for the profession. Based on the definition of internal auditing, the PPF comprises Ethics, *Standards*, Practice Advisories, and Development and Practice Aids, and paves the way to world-class internal auditing.

This guidance fits into the *Professional Practice Framework* under the heading Development and Practice Aids.

TABLE OF CONTENTS

ACKNOWLEDGMENTS

The authors wish to thank Alexandra Lee, graduate student at the University of Wisconsin, and Greg Lax, AERS Regional Controller - NORPAC at Deloitte & Touche LLP, for their assistance in helping us analyze the data. We further want to acknowledge the work of Don Sparks at The Institute of Internal Auditors for all his efforts in automating the survey and preparing data for our analysis.

ABOUT THE AUTHORS

Larry E. Rittenberg, Ph.D., CIA, CPA, formerly the vice president of research and president of The IIA Research Foundation, replaced John J. Flaherty in January 2005 as chairman of The Committee of Sponsoring Organizations of the Treadway Commission (COSO), a voluntary private-sector organization formed in 1985 to improve the quality of financial reporting through business ethics, effective internal controls, and corporate governance. Rittenberg presently teaches coursework and conducts research on auditing and corporate governance at the University of Wisconsin in Madison. He co-authored *Auditing: Concepts for a Changing Environment* and *The Outsourcing Dilemma: What Works Best for Internal Auditing* and has received many accolades from his peers and colleagues throughout his career, including The IIA's Leon R. Radde Educator of the Year Award in 1998, *Internal Auditor* magazine's Outstanding Contributor Award, and the Outstanding Educator distinction from the Wisconsin Institute of Certified Public Accountants. Larry is a past member of the IIA Executive Committee, Board of Regents, and served on the Guidance Planning Committee and Board of Research Advisors.

Patricia K. Miller, CIA, CPA, CISA is an experienced internal audit partner in the Northern California Enterprise Risk Services practice of Deloitte Touche LLP. During her career with Deloitte, she has provided a broad array of internal audit and Sarbanes-Oxley readiness services. Patty joined the Deloitte & Touche ERS practice in 1997, following a 14-year career with Pacific Telesis and Pacific Bell where she held numerous management positions in diverse areas including internal audit, billing systems, financial management and planning, process design and reengineering, project and program management, and merger planning and integration. Patty is a member of the Executive Committee of the Board of Directors for the Institute of Internal Auditors (IIA), serving in the role of Vice Chairman – Professional Practices, and is a member of the North American Committee. She has also previously served on the Standards Board, the Board of Regents, the District and Regional Representative Committees, and she served a term as President of the San Francisco Chapter of the IIA.

ABSTRACT

Companies have struggled in implementing the internal control provisions of the U.S. Sarbanes-Oxley Act of 2002. Costs have been high. However, few studies have systematically looked at the benefits. We survey 171 chief audit executives (CAEs) and internal audit managers to help identify the specific benefits associated with Section 404 work. We identify control improvements that have taken place as a direct result of Section 404 evaluations. We also identify lessons learned that can improve the efficiency and effectiveness of control evaluations in the future.

EXECUTIVE SUMMARY

We surveyed 171 practicing internal auditors about their assessment of costs and benefits associated with Section 404 work. Three major themes emerged in the survey:

First, there are significant benefits associated with the control identification, documentation, and testing process. The evaluation process has led to improvements in basic internal controls such as reconciliations and segregation of duties. There were substantial improvements in the control environment that came about as a direct result of the process. Many companies recognized they have vulnerabilities in the Information Technology (IT) area and will be devoting more resources to improving and evaluating IT controls as they move forward. Companies have more confidence in their control structure and are evaluating accounting risks, which should enable investors to have more confidence in the reliability of unaudited data furnished to the securities market.

Second, the prognosis is that the future costs associated with Section 404 will decrease substantially as we look forward three years. Much of the initial cost came about because controls had not been systematically documented or evaluated prior to the Section 404 requirements. CAEs see the process as becoming more systematized. The authors believe companies will see significant efficiencies as they fully implement the information, communication, and monitoring concepts embedded in COSO's *Internal Control – Integrated Framework.*

Third, there is uncertainty about the future role of internal auditing with respect to Section 404 work. The majority of CAEs want to maintain a strong presence in the risk and control arena, and recognize the need to perform more operational auditing that continues to add value to the organization. The majority of the respondents recognize a need to invest resources in IT auditing. Most CAEs see themselves playing a major role in ongoing monitoring and testing activities associated with Section 404 work.

Overview of the Control Improvements

There were many control improvements and they are described in more detail in the remainder of the report. We have summarized the control improvements into a "Top 10" list that can help companies consider their progress toward improved control processes. The following list is covered more fully in the report:

1. A more engaged control environment — with active participation by the board, the audit committee, and management.

2. More thoughtful analysis of monitoring controls, along with recognition that monitoring is an integral part of the control processes.

3. More structure to the year-end closing process and recording of journal entries, thus recognizing the extent to which these areas have increased in complexity.

4. Implementation of anti-fraud activities with defined processes in place, including responsibility for follow-up by defined parties and resolution approaches.

5. Better understanding of the risks associated with general computer controls, and the need to improve both control and audit procedures to gain assurances that the risks associated with computer systems are mitigated.

6. Improved documentation of controls and control processes that can serve as a basis for training, practical day-to-day guidance, and management evaluation.

7. Improved definition of controls, and the relationship of controls and risk, across the organization.

8. Control concepts becoming embedded into the organization with a broader understanding by operating personnel and management of their responsibility for controls.

9. Improvements in the adequacy of the audit trail as a basis to support operations as well as to support audit assessment of control adequacy and financial reporting.

10. Re-implementation of basic controls, e.g., segregation of duties, periodic reconciliation of accounts, and authorization processes that had been eroded as organizations downsized or consolidated operations.

INTRODUCTION

Much has been written about the costs associated with implementing the internal control provisions of the Sarbanes-Oxley Act [hereinafter referred to as Section 404 work]. Essentially, most studies have indicated that the costs have been very high — much more than what was anticipated by the companies performing the work. There has been a severe resource shortage for the internal control documentation and review, including significant accounting staff and auditors (both internal and external), as well as a shortage of proven methodologies to document internal controls — all of which have added significantly to the costs incurred by companies. This has been compounded by what has been perceived as a combination of (a) lack of clear direction on the nature of the work to be performed; (b) very stringent definitions of materiality and internal control deficiencies in Audit Standard 2 (AS2)[1], and (c) significant time pressures to complete the work. Most of the studies issued to date assert that the costs associated with the internal control work far exceed the benefits.

The studies on costs/benefits associated with Section 404 work are incomplete in three important ways. First, they fail to address the benefits that improved controls and reliability of financial reporting have on the investing public. Second, very few of the studies deal with the learning curve associated with new processes, i.e., they fail to address expected ongoing costs as opposed to one-time start-up costs. Third, they fail to identify specific control improvements that have been made as a result of the mandated internal control work.

The research described in this paper has been designed to specifically address the control benefits that have been found by companies and practicing internal auditors in performing 404 work. The IIA Research Foundation has assisted us in this research to provide timely information of interest to practicing accounting and auditing professionals. The research was designed to address four specific objectives:

- Identify specific control benefits associated with Section 404 work,
- Better understand the costs associated with Section 404 work,
- Develop insights on how to reduce future costs associated with ongoing evaluations of controls to meet the public reporting requirements, and
- Understand how internal audit is likely to evolve to meet the required Section 404 work as well as to add value in traditional areas associated with broader operational controls, risk, and governance.

[1] PCAOB Standard 2, *An Audit of Internal Controls Over Financial Reporting Conducted in Conjunction with an Audit of Financial Statements.*

UNDERSTANDING 404 REQUIREMENTS AND COSTS

Section 404 of the Sarbanes-Oxley Act came about as a direct result of corporate failures of the past decade in which there were significant internal control failures associated with fraudulent financial statements. In the opinion of legislators, it was not sufficient that the external audit profession would be improved; there had to be significant improvement in the governance and control of public registrants. Section 404 was just one part of a more comprehensive set of requirements that included the development of disclosure committees, certification of financial statements by both the CEO and CFO, the development of more financially literate and responsible audit committees, increased independence of the external auditor, and the implementation of fraud risk management processes (like "whistleblower" procedures) that would alert the appropriate levels of governance of potential frauds or illegal acts within the company. Further, the legislation took the setting of auditing standards for the audits of public companies away from the AICPA, a private standard setter, and formed a new body, the Public Company Accounting Oversight Board (PCAOB), to set auditing standards for public companies. The time required to get the PCAOB staffed and in operation led to a delay in the standard-setting process, which contributed to some of the difficulties companies encountered in implementing Section 404.

The control deficiencies at the largest failed companies were extensive and included problems with the "tone at the top" as well as deficiencies in basic processing. For example, within WorldCom, there were material control deficiencies noted in the board of directors report, including issues with (a) the closing process, (b) non-supported journal entries, (c) booking accounting estimates, and (d) recording expenses and fixed assets. These control deficiencies were exacerbated by a lack of integrity at the top of the organization, including both top management and the board of directors.[2] Similar deficiencies were found at other organizations, including HealthSouth, Lucent, and Enron. Early public reports of control deficiencies reinforce the notion that the quality of internal control merits the attention of boards, investors, regulators, management, and internal auditors.

The Public Benefits of Improved Controls

It is important to understand the public perspective in order to form a balanced view on the cost and benefits of internal control certification. Don Nicolaisen, chief accountant at the SEC and a former partner with PricewaterhouseCoopers, describes the importance of the Sarbanes-Oxley Act in motivating him to join the SEC:

> "The Sarbanes Oxley Act required major reform in many areas in response to the financial failures of recent years. The crisis was real, and I believe the Act sets the right perspective and establishes an appropriate foundation upon which to improve financial reporting. This drive to improve financial reporting was one of the main reasons I joined the Commission staff."[3]

Nicolaisen and others, such as the Financial Executives Institute (FEI), have noted the substantial costs associated with Section 404 work. Most of those cost estimates, although high, do not include the cost of the external auditor's extra efforts in performing an integrated audit of internal controls and financial statements. Nicolaisen acknowledges that many question whether the internal control efforts will be worth the costs. He unequivocally answers:

> "I suspect that the costs are not easy to estimate, but I know that it is even tougher to quantify the benefits. However, given the massive financial scandals, decline in market capitalization, and resulting loss of investor confidence in our markets, I believe that, of all of the recent reforms, the internal control requirements have the greatest potential to improve the reliability of financial reporting. Our capital markets run on faith and trust that the vast majority of companies present reliable and complete financial data for investment and policy decision-making. Representing to the world that a company has in place an appropriate control system, free of material weaknesses, that gathers, consolidates, and presents financial information strengthens public confidence in our markets and encourages investment in our nation's industries. If that's the

[2] For a thorough review of the problems, see Beresford, Dennis, Nicholas Katzenbaum, and C. B. Rogers, *Special Investigative Committee of the Board of Directors of WorldCom*, at www.Findlaw.com, March 31, 2003.
[3] Nicolaisen, Donald T., Keynote Speech at 11th Annual Midwestern Financial Reporting Symposium; October 7, 2004. Speech is available at www.sec.gov.

> case, then it's worth it, and it is absolutely critical that we get the internal control requirements right."[4]

Rating agencies have also indicated that internal control information is important. Fitch Ratings, in a recently published special report, stated their views on the importance of internal control reporting as follows:

> "Fitch believes that investors should consider material weaknesses, as well as significant deficiencies, when assessing credit ratings. While auditors can render "clean" opinions on financial statements, investors should consider the analytical implications of certain disclosures on the entity as a whole, as well as the reliability of unaudited data furnished by management." [5]

A substantial part of the costs incurred are related to winning back the public confidence in a financial reporting system that had become unreliable. Given that objective, it is reasonable to assume that there are two costs associated with Section 404 work:

- The cost associated directly with winning back the public confidence, and
- The cost associated with ongoing internal control documentation and testing efforts.

It is reasonable to expect that the future costs of complying with Section 404 will decrease because (a) the initial investment in winning back the public confidence will already have been made, (b) there is a learning curve associated with control evaluation and testing, and (c) control processes, like many other processes, should become more efficient over time as companies implement process improvement methodologies. Some practitioners make similar observations. James Quigley, CEO of Deloitte & Touche, LLP, in testimony before Congress states it this way:

> "My viewpoint, although costly, the internal control management and auditor attestation are valuable, meaningful safeguards, [and] as businesses and auditors gain experience in complying with the requirements, [the audit and control processes] will become more efficient."[6]

These expectations, although reasonable, are speculative and merit further investigation. We wish to understand whether individuals, such as internal auditors, who have been dealing with internal control processes and evaluations on a daily basis, believe that such changes in cost will take place.

Cost Estimates

There is strong evidence that the cost of complying with Section 404 is very expensive. An August 2004 study by the Financial Executives Institute (FEI) of 224 companies showed costs upward of $3 million for the larger companies in its survey. More recently, Yellow Roadway (a trucking firm) indicated that the Section 404 costs represented over 3% of its annual profits.[7] However, most of the cost estimates do not distinguish the costs that are due to initial documentation and testing (start-up) costs versus ongoing costs, and to what extent the costs were due to uncertainty over the required evaluation process. Our research is designed to gather more insight on these issues.

[4] Nicolaisen, Donald T., Keynote Speech at 11th Annual Midwestern Financial Reporting Symposium; October 7, 2004. Speech is available at www.sec.gov.
[5] Fitch Ratings, *Special Report, Sarbanes-Oxley Section 404;* January 2005, New York, New York, p. 3.
[6] Quigley, James T., *Sarbanes-Oxley Implementation in Restoring Public Confidence*, Washington, D.C, House Committee on Financial Services, July 22, 2004; Deloitte, 2004.
[7] Henry, David, and Amy Borrus, "No Escaping Sarbanes-Oxley," *Business Week*, January 6, 2005.

RESEARCH METHODOLOGY

In cooperation with The IIA Research Foundation, we utilized the resources of The IIA's research department and GAIN database to survey chief audit executive (CAE) members of The IIA. Many of the CAEs are with larger companies, so the survey reflects the view of those larger organizations. The survey was completed last fall (2004) after most companies had completed their Section 404 evaluations, but before external auditors had completed their testing. We received 171 responses. The respondents represented diversity in size of companies as shown in Exhibit 1, with almost an equal percentage of responses coming from very large, large, and intermediate-sized companies based on our definition of those terms.

Exhibit 1
Size of Companies Responding

Size	Number	Percentage
Very Large – over $6 billion in sales	54	31.6%
Large – between $1 billion and $6 billion in sales	64	37.4%
Intermediate – between $200 million and $1 billion in sales	42	24.6%
Small – less than $200 million in sales	4	2.3%
Not Reporting	7	4.1%
Total	**171**	**100.0%**

Although almost 70% of our responses are from very large and large companies, we believe the lessons learned are useful for most companies, including smaller companies.

The respondents represent a wide variety of industries. A summary of responses by industry is shown in Exhibit 2. We did subsequent analysis by industry, but the results were quite similar across industries.

Exhibit 2
Industry Background of Respondents

Industry	Number	Percentage
Technology	20	11.7%
Manufacturing	41	24.0%
Distribution	4	2.3%
Retail	10	5.8 %
Insurance	16	9.4%
Financial Institutions, other than Insurance	18	10.5%
Wholesale	3	1.8%
Other	54	31.6%
Not Reporting	5	2.9%
Total	**171**	**100.0%**

RESEARCH FINDINGS

Control Improvements Directly Associated with Section 404 Work

We were most interested in knowing the current view of the specific benefits associated with Section 404 work. For example, the CFO of General Electric (which spent approximately $30 million on Section 404 compliance) states:

> "(GE) had good controls before this, but it [Section 404 work] has added more rigor. . . It certainly gives [CEO Jeff Immelt] and me more confidence when we're signing off on the results."[8]

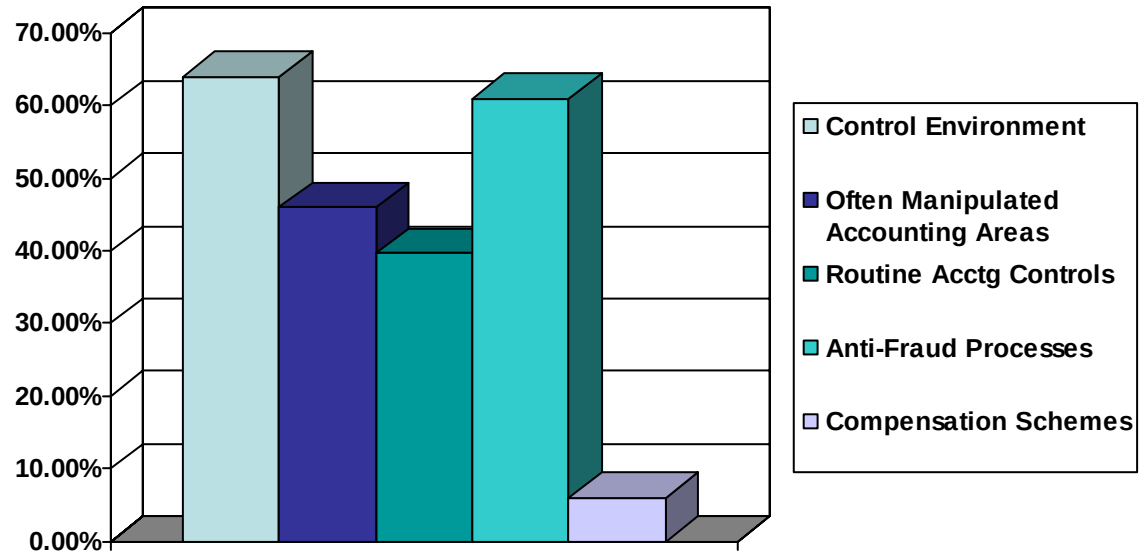
Similar comments are echoed by the CEO of PricewaterhouseCoopers, Sam DiPiazza, who states that "we are finding that the focus on internal controls is uncovering problems at the best of companies."[9] What is the nature of these problems?

We asked the study participants to identify the controls that were improved *directly as a result of 404 work in their organization.* The participants ranked the controls on a 5-point scale, with a 4 indicating agreement with a statement that the controls had improved directly as a result of the work and a 5 indicating strong agreement. We have categorized their responses in four categories:

- The control environment (excluding compensation schemes which we address separately);
- Often-manipulated accounting areas;
- Routine accounting controls; and
- Anti-fraud activities.

The results are shown in Exhibit 3.

Exhibit 3
Agree or Strongly Agree Controls Have Improved Due to Section 404 Work



[8] "No Escaping Sarbanes-Oxley," *Business Week, Online Edition,* January 6, 2005.
[9] Ibid.

The two biggest areas of control improvements are the control environment and the anti-fraud awareness actions taken by the companies. Over 60% of the respondents agreed that there were improvements in these areas that would not have taken place without the Section 404 work. We are not surprised by the emphasis on these two areas because weaknesses in the control environment have often been associated with business failure or financial frauds. Most organizations did not have well-developed anti-fraud programs. Thus, although we are not surprised by the emphasis, we think the percentage of respondents indicating that controls in these areas have improved directly as a result of Section 404 work is significant. Remember, many of the respondents come from very large organizations *and* those organizations have already invested in an internal audit function. In other words, these respondents are saying that the improvements would not have been identified, or taken place, without the systematic review, documentation, testing, and analysis of controls that took place as a direct result of Section 404 work. We analyze each of these areas in greater depth.

Improvements in the Control Environment

There were six control topics under the control environment category:

Exhibit 4
The Control Environment:
Improvements Due to Section 404 Work

Areas of Improvement Due to 404 Work:	Disagree or Strongly Disagree	Neutral	Agree or Strongly Agree
Audit Committee Involvement and Knowledge	9%	20%	71%
Monitoring Controls	11%	18%	71%
Board Knowledge and Role In Controls	10%	24%	66%
Control Environment	16%	22%	62%
Internal Auditing	20%	21%	59%
Greater Acceptance of Codes of Conduct	18%	26%	56%
Mean Response	**14%**	**22%**	**64%**

One of the major objectives of the legislation was to improve governance through more effective audit committees. Over 70% of our respondents identified significant improvements in the knowledge and involvement of the audit committee. In our open-ended responses, the increased knowledge and involvement of the audit committee was cited as one of the five major benefits of the control work. However, the improvements are much broader than the audit committee; all members of the board have developed greater awareness and responsibility for controls over financial reporting. Other areas, such as internal audit activities and greater acceptance of the role an effective code of conduct can play in effective governance, have also improved directly because of the Sarbanes-Oxley legislation and the organization's attention to the "tone at the top" and the control environment.

Controls over Often-manipulated Accounting Areas

Even before the Sarbanes-Oxley Act, many companies had paid increasing attention to the areas that were most often manipulated in financial frauds. These areas include manipulating revenue recognition, inappropriately using accounting estimates (often referred to as "cookie jar reserves") to manage earnings, and using unsupported journal entries to manipulate reported earnings.[10] We were interested in whether companies had already implemented significant control improvements in these areas, or whether there were still more to be performed. An overview of these three areas is shown in Exhibit 5.

[10] For example, WorldCom used journal entries and restructuring estimates to manipulate its reported earnings. Many companies have hundreds of year-end journal entries — many of which are not subject to detailed scrutiny. The SEC has taken action against many companies for inappropriate revenue recognition.

Exhibit 5
Improvements in Often-Manipulated Accounting Areas

Areas of Improvement Due to 404 Work:	Disagree or Strongly Disagree	Neutral	Agree or Strongly Agree
Closing Process and Unusual Journal Entries	14%	24%	62%
Accounting Estimates	19%	35%	46%
Revenue Recognition	28%	42%	30%
Mean Response	**20%**	**34%**	**46%**

The good news is that many companies had implemented better controls over revenue recognition and had developed more concrete criteria for revenue recognition. Still, a full 30% of the respondents indicated significant improvements in controls over revenue that were directly attributable to Section 404 work.

The significant improvement in the closing process strikes us as very significant. Given the typical volume and complexity of the closing process and year-end journal entries, it is likely that this area had not been subjected to detailed control analysis. Historically, accountants and auditors have had a tendency to focus on controls over routine transaction processing, leaving this fundamental processing area systematically overlooked in many organizations. In our conversations with both internal and external auditors, we also have strong anecdotal evidence that neither internal nor external auditors have historically or systematically tested the closing process. For example, auditors have not used audit software to analyze journal entries, summarize the entries, and select entries for support and review. And it is often difficult to trace journal entries back to the underlying support and origination, or the dollar amounts are below the auditor's scope threshold.[11] The control reviews performed on the closing process and unusual journal entries have led to significant control improvements according to almost two-thirds of the study respondents. It is clearly an area that all organizations ought to review.

AUTHOR ANALYSIS

We believe that internal auditors can be a significant help to organizations by using data analysis software that examines journal entries and effectively traces journal entries back to their originating source. The entries should be monitored within the company and periodically evaluated by the internal or external audit function.

The misuse of accounting estimates has received considerable attention, starting with the 1998 speech on the "Numbers Game" by then-SEC Chairman Arthur Levitt.[12] Levitt described situations where companies would make unusually large accruals to liabilities in good times (for example, this was done with restructuring reserves associated with acquisitions at WorldCom) and then use these "cookie jar reserves" to manage earnings in bad times. Almost half of the respondents indicated that they had made significant control improvements in this area — again, as a direct result of the Section 404 work.

Routine Accounting Controls

Historically, routine accounting controls receive attention because they are essential for an organization to operate. A company must be able to track its inventory, receivables, and fixed assets, and record basic transactions to operate its business. Thus, we would not be surprised to learn that the overall controls in these areas were generally good. However, there are still a significant number of companies that made improvements in these areas as a result of their Section 404 work. As an example, Visteon, a major automotive parts supplier, reported that it found major control problems dealing with billing and receivables for an important customer, Ford Motor Company, and had made significant improvements to those controls directly as a result of 404 work.[13] An overview of these three areas is shown in Exhibit 6.

[11] For example, it has been reported on C-Span that HealthSouth covered up much of its fraudulent reporting by making thousands of journal entries well below $5,000 and across many operating entities to keep the threshold below materiality guidelines. For more details on the nature of the fraud, see Securities & Exchange Commission, Plaintiff vs. HealthSouth Corporation and Richard M. Scrushy, Defendants, at www.findlaw.com, Civil Action No. CV-03-J-0615-S.
[12] Arthur Levitt, "The Numbers Game," speech presented at NYU Center for Law and Business, September 28, 1998, available at http://www.sec.gov/news/speech/speecharchive/1998/spch220.txt.
[13] Henry, David, and Amy Borrus, "No Escaping Sarbanes-Oxley," *Business Week*, January 6, 2005, online edition, p. 2.

Exhibit 6
Improvements in Routine Accounting Controls

Areas of Improvement Due to 404 Work:	Disagree or Strongly Disagree	Neutral	Agree or Strongly Agree
Record Retention/Audit Trail	17%	22%	61%
Asset Safeguarding and Property Accounting	27%	39%	34%
Expense Classification and Accounting	30%	46%	24%
Mean Response	**25%**	**35%**	**40%**

The most important control improvement area in this category, with 61% indicating a strong improvement, is in the record retention/audit trail area. It is an often-neglected area, but it is important to answering customer questions, as well as building documented support for accounting entries. On the other hand, there was significantly less reported improvement in the areas of asset safeguarding, property accounting, and expense classification, perhaps because most companies have adequate controls in these areas. Still, there was room for improvement in a significant minority of the companies in the study.

Anti-fraud Activities

Many companies had not established specific anti-fraud control and reporting measures prior to the Sarbanes-Oxley legislation. This does not mean companies did not have any anti-fraud controls, but many did not have specific procedures, including whistleblower. The Sarbanes-Oxley Act required companies to go a step further, if they had not already done so, to establish effective anti-fraud controls. Implementing anti-fraud activities is much more than establishing whistleblowing; it must include effective monitoring of operations, effective internal audit, continuous risk analysis, and follow-up to unusual results. Not surprisingly, a significant percentage of our respondents found that their companies made significant improvement in anti-fraud activities as a direct result of the legislation.

Exhibit 7
Improvements in Anti-fraud Activities

Areas of Improvement Due to 404 Work:	Disagree or Strongly Disagree	Neutral	Agree or Strongly Agree
Anti-fraud Activities	**19%**	**33%**	**48%**

Revised Compensation Schemes

We added a question about compensation schemes because many of the financial frauds point directly to the misuse of compensation practices as a direct motivator of frauds. As shown in Exhibit 8, the companies in our sample do not appear to have made a connection between compensation schemes and controls over financial reporting.

Exhibit 8
Revision of Compensation Schemes

Areas of Improvement Due to 404 Work:	Disagree or Strongly Disagree	Neutral	Agree or Strongly Agree
Revised Compensation Schemes	62%	32%	6%

Only 6% of the respondents felt that there had been improvement, and a clear majority (62%) did not believe there had been an improvement due to Section 404 work.

Most Significant Control Improvements Noted by Study Participants

In addition to responding to the specific control improvements evaluated in the previous section, we asked the study participants to write in the five most significant control improvements they had observed. We were interested in specific observations they had about their organization's activities that we might not have captured in our earlier questions. We received numerous thoughtful responses. We were able to classify most of these open-ended responses into seven broad categories, although some of the responses were difficult to classify. Those categories were:

- Specific improvements in controls or documentation processes,
- Improvements in the control environment of the organization,
- Recognition of the need, and improvements made, over computerized controls,
- Implementation of risk management approaches to better analyze and drive the implementation of controls, with more efficient control structures as controls were linked to risks,
- Increased control awareness by the process owners,
- Management acknowledgment of their responsibility for the effective implementation and monitoring of controls, and
- Other, a wide variety of responses that were unique to each participant.

An overview of the open-ended responses on control improvements is presented in Exhibit 9.

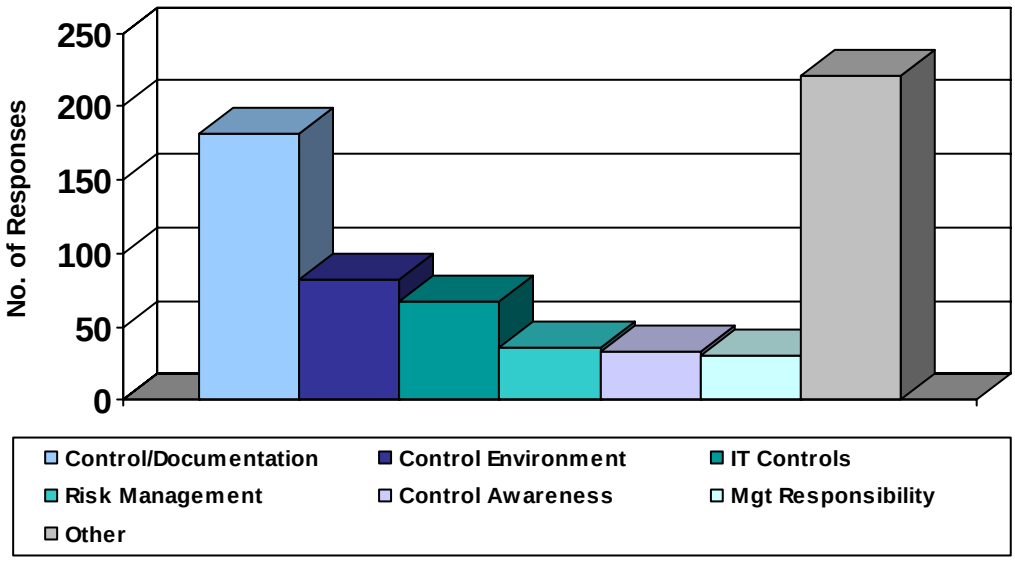
AUTHOR ANALYSIS

The authors believe the lack of attention to compensation plans is a serious omission because compensation is clearly a major motivator of performance. Further, the recent problems with the public accounting profession further demonstrate that a well-established ethical code is not sufficient to overcome dysfunctional compensation schemes.[14] Given the clear linkage between fraud and management incentive plans, compensation plans should be a continuing focus of boards, management, regulators, and legislators.[15] The changes must start at the top of the organization and be carried out consistently throughout the organization. We feel it is a significant omission and should be reconsidered by organizations as they assess the design and effectiveness of internal controls over financial reporting for Section 404.

[14] Our focus here is not on the public accounting firms. However, the example of the large public accounting firms changing their compensation schemes to focus less on "selling" products and other services to a higher emphasis on quality factors is an example of using compensation schemes to motivate desired performance.

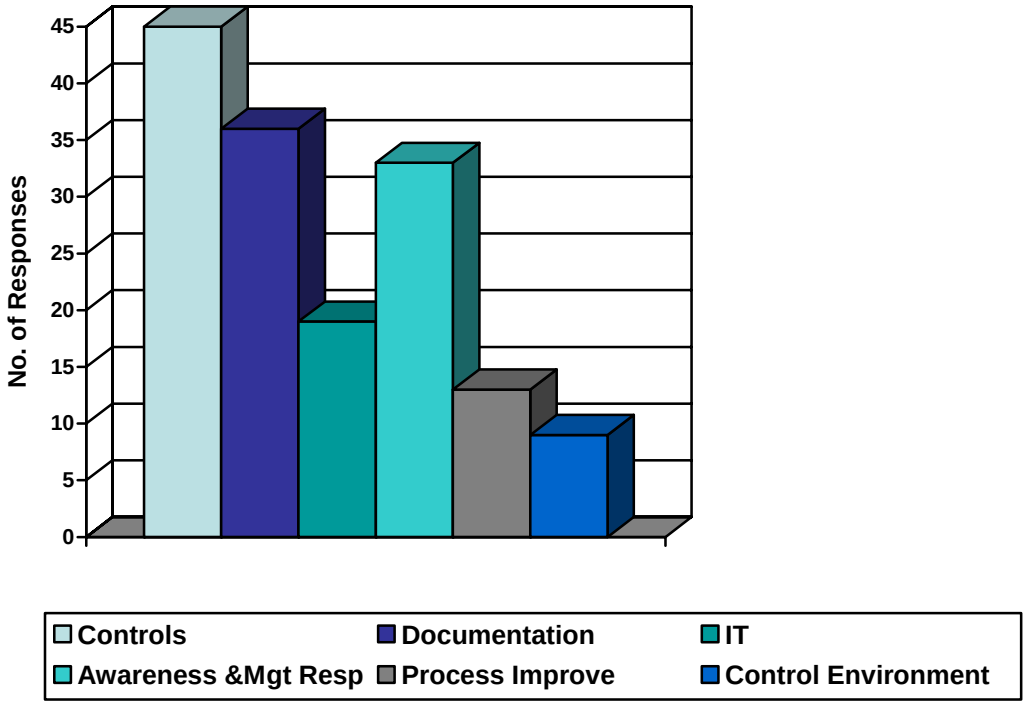
[15] The use of stock options is often cited as an example of a compensation method that has encouraged dysfunctional activities in some organizations. The FASB is, of course, addressing the issue of expensing stock options. Some companies are addressing what they believe may be dysfunctional aspects of stock options through such mechanisms as (a) restricted stock plans, (b) performance objectives that represent a more balanced-scorecard approach, and (c) aligning performance rewards with longer-run results.

Exhibit 9
Most Significant Control Improvements



We further explored the responses by performing a separate analysis of the first item identified by our respondent on the assumption that the first item was most important or had the greatest effect. We present this analysis in Exhibit 10.

Exhibit 10
Most Important Control Improvement



There is a consistency between the overall analysis and the separate analysis of the first item identified. The first item most often mentioned related to the identification of specific, easily identifiable control improvements such as the documentation or improvement of controls. Improvements in the control environment, awareness of the importance of controls across the organization, and management's responsibility for controls also rank highly, and the need for improved information technology controls remains. We discuss the overall findings below.

Management Awareness and Ownership for Controls

Overall, most survey participants believed that their companies have gained valuable awareness throughout all levels of the organization about internal controls and the need for those controls. A large number of survey participants wrote comments supporting their view that management and employees more fully understand how controls affect operations and that management has accepted responsibility for controls.

Many respondents described the embedding of internal control ownership into the culture of the organization as a major benefit. However, based on answers to a subsequent question, there remain a significant number of companies where control ownership (or at least the ownership of Section 404 compliance efforts) does not necessarily reside with management.

Control Benefits: A Summary

It is difficult to summarize the major control benefits because of the diversity of improvements noted by the study participants. Our observation of both the structured questions and the open-ended responses leads to our assessment of a "Top 10" list of control improvements:

1. A more engaged control environment — with active participation by the board, the audit committee, and management.
2. More thoughtful analysis of monitoring controls, along with recognition that monitoring is an integral part of the control processes.
3. More structure to the year-end closing process and recording of journal entries, thus recognizing the extent to which these areas have increased in complexity.
4. Implementation of anti-fraud activities with defined processes in place, including responsibility for follow-up by defined parties and resolution approaches.
5. Better understanding of the risks associated with general computer controls, and the need to improve both control and audit procedures to gain assurances that the risks associated with computer systems are mitigated.
6. Improved documentation of controls and control processes that can serve as a basis for training, practical day-to-day guidance, and management evaluation.
7. Improved definition of controls, and the relationship of controls and risk, across the organization.
8. Control concepts becoming embedded into the organization with a broader understanding by operating personnel and management of their responsibility for controls.
9. Improvements in the adequacy of the audit trail as a basis to support operations as well as to support audit assessment of control adequacy and financial reporting.
10. Re-implementation of basic controls, e.g., segregation of duties, periodic reconciliation of accounts, and authorization processes that had been eroded as organizations had downsized or consolidated operations.

Section 404 Compliance Ownership

To comply with the requirements of Section 404, organizations tried different models for assigning ownership and responsibility. These included:

- Creating a compliance team,
- Assigning responsibility to process owners (generally the heads of operating units),

- Assigning responsibility to the controller, or
- Outsourcing major efforts to a third party with oversight and responsibility by an internal leader.

Others have used some combination of the above alternatives. The wide divergence of practice is evident in the results to our question about responsibility. The following chart summarizes the answers to our question about current responsibility for various aspects of Section 404 compliance:

Exhibit 11
Current Responsibility for Section 404 Effort

	Management	Controller	Internal Audit
Overall Section 404 Ownership	41%	39%	20%
Documentation	59%	20%	21%
Ongoing Testing	28%	7%	65%
Monitoring Process	26%	17%	57%

For our respondents, management (central compliance team and/or process owners) generally had overall ownership and responsibility for documenting controls, but internal audit owned testing and monitoring. It is interesting to note that there is no consistent assignment of overall ownership, and that internal audit is described as the "overall owner" for 20% of the companies responding.

Enhanced Documentation and Control Evidence

There are two components of improved documentation that were mentioned by our respondents:

- Documentation of the processes, workflow, and controls, and
- Documentation of the evidence that the controls are working.

Improving the documentation of controls and processes is not surprising because it has been mandated by regulation and auditing standards. In completing the readiness effort, organizations have better captured not only the process flow and associated controls, but also updated the associated policies, procedures, handbooks, job descriptions, and other pertinent documents. Respondents believed that the development of adequate

AUTHOR ANALYSIS

Our Observations on Control Ownership

We have noted a number of themes regarding control and process ownership. The most common theme is that the "process owner" ought to be the owner of the controls and should be held responsible for the adequacy of the controls. That concept is embodied in the Sarbanes-Oxley requirement that the CEO and CFO certify both the report on internal control over financial reporting and the financial statements. However, the comments received in the open-ended responses from the CAEs indicate that they believe many process owners do not fully understand controls, although they do understand control objectives and the responsibility to see that controls are adequate.

We believe that organizations are going to continue to struggle with control ownership. The process owners are not "control experts," but they are an integral part of the control system. Process owners also have an obligation to ensure that the processes under their control are efficient — and rightly, or wrongly, they often believe that "controls" create unnecessary work and slow down the underlying processes, or at a minimum add unnecessary overhead. Controllers (and auditors) are generally the control experts within the organization. However, they usually do not have the authority to mandate controls, and more important, they are not part of the system that ensures that employees are motivated to comply with control requirements or follow control procedures. That is management's job. Thus we have a dilemma. Either the process owners have to become control experts and controls have to become embedded in the organization's culture, or alternatively, the controller's function must provide sufficient guidelines, training, and selection choices that provide a foundation on which control objectives can be achieved. In the latter alternative, the process owners still have a responsibility to see that control objectives are achieved.

An example might help explain our concerns. Think of a manufacturing process with a number of stamping machines working in serial processing to manufacture goods. The engineers (controllers) set up tolerances in the machines and then develop monitoring controls that tell the plant manager whether any machine is failing to meet the quality objectives, i.e., the machines are producing products outside of tolerance. The plant manager is responsible for monitoring the performance of the process and taking corrective action when the machines are out of tolerance. Who has responsibility for the controls? It seems to us that there is a joint responsibility. The engineers (controllers) are responsible for establishing the control objectives and standardized processes to accomplish the objectives. However, it then becomes part of the owner's responsibility (the plant manager) to monitor the system, identify instances of control deviations, and take timely and effective corrective action. This model is consistent with COSO's *Internal Control – Integrated Framework,* which anticipates that an effective information and communication system, coupled with monitoring and feedback, are essential elements of the control process. We believe that organizations will need to expand their thinking about the COSO model to achieve more responsibility and efficiency in the control process. Ownership and development of the control activities and system may differ from the process owners' responsibility to monitor and signal control failures.

documentation will pay future dividends in areas such as training new employees, enabling backfill and succession planning for key positions, and identifying process improvement opportunities. Many respondents mentioned that the improved documentation is an important control from a global control perspective.

A major finding is that there was little documentation or evidence that existing controls were working. For example, how would an organization determine that there was a proper review of an exception report, or a proper reconciliation, if there was no documentation that the review of the reconciliation was performed? Respondents noted the improvement in documenting the evidence of supervisory reviews and approvals, management committee actions and decisions, and the investigation and resolution of unreconciled or outstanding items. The need to properly and clearly develop evidence of the operation of each key control has become a more common practice.

Stronger Tone at the Top

Several respondents noted the "tone at the top" and control environment are now better understood by company executives and employees. The board is more aware of its control responsibilities and the audit committee has taken leadership in supporting improved controls. The "tone at the top" has extended beyond management and into the governance process. Anti-fraud efforts have been established or strengthened, including the implementation of fraud and ethics hotlines. The audit committee has become more involved in accounting policies and practices, earnings releases, and the evaluation of internal controls.

Strengthened Information Technology Controls

Information technology (IT) controls is perhaps the Achilles' heel of financial reporting controls. Everyone knows that we need improved controls over IT, but the responsibility has often been delegated to the IT staff. Many organizations have recognized the increased need to more actively evaluate IT controls using appropriate resources, such as IT auditors. The five most mentioned enhancements to information system controls were:

- Improved information system security,
- Better understanding and improvement of segregation of duties,
- Improved access controls and access monitoring,
- Improved testing procedures and program change management, and
- Improved processes to document policies, procedures, and controls.

As one respondent stated: "*Without the push from SOX, this [IT control improvement] would not have happened, when it happened*."

Many respondents voiced the opinion that as organizations grow and become more technologically dependent, there is an increased need to "automate" more controls — essentially to build the controls into the business process, much as the engineer builds tolerances into the stamping machines. The audit/control challenge will be to develop an effective information, communication, and monitoring system that will identify when the controls that are built into the system are not working within their prescribed tolerances, and then signal evaluation activities and monitor correction.

AUTHOR ANALYSIS

Many participants indicated the biggest thing that was needed going forward was that a "control culture" become embedded into the organization. The audit committee is clearly giving such direction. However, we would like to see those responsible for the "tone at the top" embrace controls as a more effective way of operating, as opposed to something that must be done to meet a governmental regulation. This applies to both large and small organizations. The authors believe that COSO's *Internal Control – Integrated Framework,* as well as COSO's *Enterprise Risk Management – Integrated Framework,* provide rich frameworks for management and audit committees to use in embedding a risk and control culture within the organization.

Strengthening Other Controls

Improvement of specific controls was the item most often noted. The controls that were improved varied with the nature of the company and the industry. The most often-cited control improvements were:

- The reconciliation process — at all levels within the processing system,
- Specific accounting processes, most often payables and inventory,
- The journal entry and closing process,
- Better segregation of duties, and
- Improved consistency in definition and application of control adequacy across the organization.

AUTHOR ANALYSIS

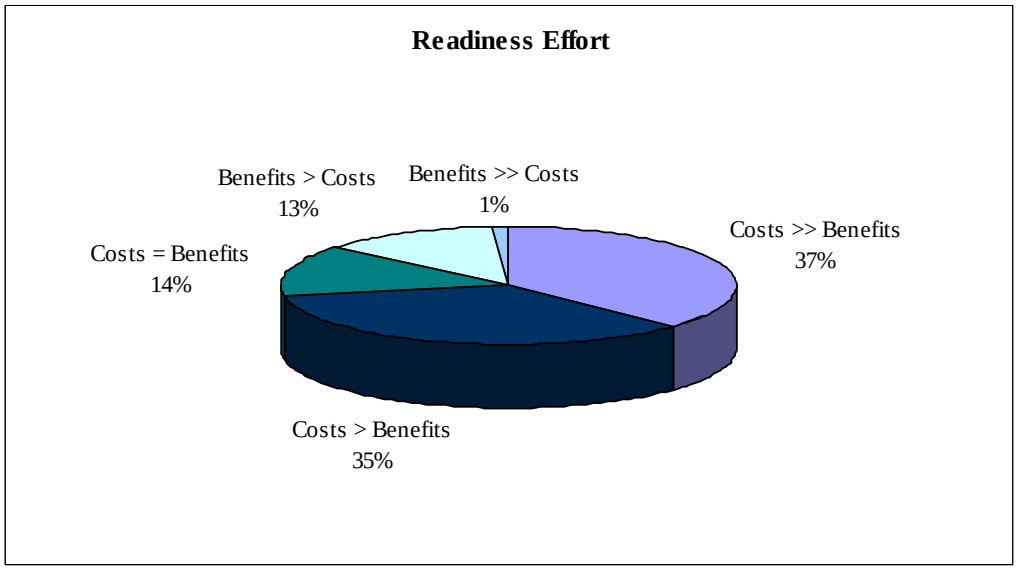
Given (a) the nature of accounting failures in the past decade, and (b) the basic auditing evolution away from testing and relying on controls to more analytic and substantive procedures, we are not surprised that some organizations may have ignored basic internal controls. As organizations grow and become more complex, there is an increasing need for timely and thorough reconciliations — between parent and subsidiary ledgers, and of account balances to the detail. For example, finding weaknesses in reviewing journal entries, the year-end accounting closing process, or performing basic reconciliations is a sign of less control emphasis. Companies are now finding that they have to drive new control philosophies consistently across entities to achieve required control objectives. Many of the respondents indicated a major problem uncovered by Section 404 work was that independent units did not feel they needed to follow corporate policies. The systematic approach to controls assessment, brought on by Section 404, is changing that belief.

Cost-benefit of Section 404 Work

The first year costs to comply with the Sarbanes-Oxley Act were significant, and significantly more than understood or forecast at the beginning of the process. And the total cost of compliance mushroomed — the FEI August 2004 noted that the average expected cost had increased more than 62%, from $1.93 million to $3.14 million, in a period of only six months (January - July 2004). This paralleled the expected increase in employee hours — from 12,265 estimated in January to 25,667 estimated in July.

We asked survey participants for their opinion regarding the relative costs and benefits associated with readiness. When asked about the up-front costs to get ready, 72% of the respondents answered that the costs exceeded (>) or greatly exceeded (>>) the benefits. The breakout by answer is depicted in Exhibit 12; only 14% of the respondents indicating that year one benefits exceeded or greatly exceeded the costs.

Exhibit 12
Relationship of Cost of Readiness Activities and Benefits



There is some differentiation in the results when looking at the cost versus benefit responses by industry. The percentage of respondents by industry who selected costs exceeded or greatly exceeded benefits ranged from 50% (Retail) to 81% (Insurance), with the average 72%. The breakout was:

Average	Financial Institutions	Insurance	Manufacturing	Retail	Technology	Other
72%	61%	81%	80%	50%	75%	70%

The size of organization did not appear to be a factor in the participant's responses – when looked at by company size, the percentage of respondents answering negatively (costs greater than benefits) ranged from 72% to 75%.

In answering this cost/benefit question, many respondents acknowledged the difficulty in quantifying the types of benefits received to date. For example, one participant pondered: *"… how do you quantify the benefit of continuing to be able to access equity markets because you have not had any "Enron" type disaster?"* Even so, the costs were so significant the shared belief seemed to be that they dwarfed the benefits — tangible as well as intangible.

Reasons for the High Costs

To understand the answers above, we also asked participants to provide reasons for their response to the cost question, and to provide recommendations to retain the benefit of internal control assessments while significantly reducing the cost of the assessments. Five clear themes emerged from their answers.

1) Learning Curve

While external auditors and internal auditors have historically assessed (but not necessarily tested) internal controls, a company-wide effort to identify, document, and test all key controls associated with financial reporting has never been undertaken. Financial reporting controls are not limited to what goes on in the accounting department to reconcile accounts, close the books, and produce quarterly and annual financial statements. Companies learned they needed to start at the beginning of the transaction stream, where the sale is contracted, the order entered, the product produced, the loan originated, or the revenue recognition principle applied. Preventive controls were recognized as being just as — if not more than — important as the detective controls. Operational employees, who had limited accounting or auditing knowledge, were, by necessity, involved in the process. So — not only was the entire effort a new undertaking with no tried-and-tested methodology, the individuals performing the work were frequently inexperienced in basic control and accounting concepts.

2) Time Pressure and Fees

The Sarbanes-Oxley Act was signed into law in July 2002, with an original December 2003 due date for complying with Section 404. All affected public companies and their boards wanted to get a clean opinion. The question was how to go about it. Since failure was not a desirable option, companies with December year-ends sought advice from professional service firms (including The Big 4), law firms, and their external auditor to understand the requirements. And due to the relatively short time period to implement and no abundance of spare internal resources, many organizations chose to engage external consultants and contractors to advise them as well as to augment their internal resources. As the demand for the audit and accounting consultants grew, so did the cost of engaging them.

Ultimately the implementation date was postponed. However, the issuance of the independent audit attestation standards (Audit Standard 2) increased the perceived requirements on management as well as the external auditor. So, although it would appear the time pressure had been alleviated, in actuality the work pressure remained because of the perceived increase in the amount of effort required to get a clean opinion. To compound the costs issue, the external auditor's fee estimate to complete the integrated control and financial statement audit was increasing. In the same August 2004 FEI survey noted earlier, the expected external audit fees for the internal control attestation had increased 40% between January 2004 and July 2004.

3) Uncertainty

The Sarbanes-Oxley Act Section 404 required management to acknowledge its responsibility "for establishing and maintaining an adequate internal control structure and procedures for financial reporting"; and to assess the "effectiveness of the internal control structure and procedures of the issuer for financial reporting." In addition, the external auditor was responsible to "attest to, and report on, the assessment made by the management..." The internal control requirement was viewed as a "principles-based" concept, but auditors and management worried that The IIA's *International Standards for the Professional Practice of Internal Auditing (Standards)* required "more" and sought greater guidance to meet the reporting requirements. With tight deadlines, companies had to begin the process of identifying and documenting controls over financial reporting based on the broad concepts in COSO's *Internal Control – Integrated Framework*. Meanwhile, the new regulatory body to oversee the public accounting profession, the PCAOB, was forming. One of the PCAOB's first jobs was to develop the standard by which the auditors would attest to management's internal control certification as required by Section 404. In the absence of final standards, and in order to maintain independence from management's process, the auditors were reluctant to provide guidance to their clients on how much documentation was sufficient, on what constituted sufficient internal controls, and on what exceptions might constitute a material weakness. Ultimately, the final Audit Standard 2 (AS 2) was issued in June 2004, almost two years after the Sarbanes-Oxley Act was signed into law. Associated guidance and clarification continued to be released by the SEC and the PCAOB through December 2004. One respondent summarized the problem as follows:

> *"Accelerated time line, with relatively no guidance from SEC or external audit firms... All issues are treated with the same level of importance."*

During this period of unclear requirements and standards, most companies continued their documentation and testing efforts, believing they were living up to the principles of the legislation. However, in the view of many, the final PCAOB standard "raised the bar" on the attestation requirement above the original expectations and dictated rigorous testing requirements for the auditor. For many companies, the final PCAOB rules led to a higher standard of documentation and control testing by both management and the external auditor. This, in turn, led to significant amounts of rework to their documentation and expanded testing beyond the level originally planned.

Many in our survey believe AS 2 still lacks clarity, particularly in the definitions of significant deficiency and material weakness. Many of those involved in testing controls express concern that there remains too much uncertainty about how to quantify control breakdowns in terms of a dollar misstatement, and how to judge the likelihood that the breakdown could cause a misstatement. This seems especially true with information systems weaknesses — where companies continue to struggle with equating a weakness in an area like operating system access privileges to a dollar misstatement.

4) Attestation Requirement

One of the objectives of Sarbanes-Oxley was to ensure that the chief executive officer and the chief financial officer took personal responsibility for the effectiveness of the internal controls over financial reporting. The Act also requires an independent opinion on the effectiveness of their controls. Many of the respondents to our survey believe that there is excess cost in the system because of the requirement for duplicative detailed testing by the organization and by the external auditor.

For an auditor to opine, there must be clear evidence to review, test, and, ultimately, rely upon. It is not enough for management to assess and certify to the CEO and CFO that the existing controls are effective. The challenge for management is to ensure that sufficient documentation is available for the

AUTHOR ANALYSIS

This is a difficult dilemma for the accounting and auditing profession as a whole. On one hand, the profession and many user groups feel that we would be better served by professional auditors and managers who make decisions based on fundamental concepts of control and economic analysis. In order to get to that point, however, auditors and managers have to feel that every judgment that is made is not second-guessed by standard setters (or worse yet, plaintiff lawyers) by yet-unspecified criteria. Our view is that the profession is better served by professionals who understand the fundamental concepts of controls and the objectives of financial reporting established in the COSO framework. It will take some time to get to the point where everyone is comfortable in making those decisions, and it will come only if the PCAOB and the SEC allow good faith judgments to be made by management and the external auditors.

external auditor to carry out the procedures shown in Exhibit 13.

Exhibit 13

Documentation and Process by Management to Facilitate an External Audit

Management has to maintain sufficient documentation and evidence of their assessment work effort so that the auditor can:

- Confirm the sufficiency of management's risk assessment and scoping process,
- Understand and confirm the sufficiency of the COSO entity level controls,
- Understand the primary business processes and transaction flows and confirm this understanding during an independent walk-through,
- Confirm that all significant classes of transactions are included,
- Confirm that all relevant financial assertions are considered for each significant account and disclosure,
- Reperform to the same conclusion tests of the effectiveness of controls,
- Independently test the effectiveness of selected key controls at selected significant locations.

For many of our respondents, this level of documentation and additional controls evidence was perceived as "overkill."

"In short, most aspects of financial reporting were already well controlled, but informal. We've made tweaks, but spent a lot of time focusing on evidence rather than being satisfied that the control — evidence or not — actually works."

"External auditors will be retesting and reevaluating controls work already done by the companies; in effect charging their time for duplicating work."

5) Compliance, Not Improvement, Effort

The readiness effort for Section 404 certification was fairly quickly recognized to be a major effort. It is important to note that as companies sought to be more cost efficient in their operations over the past few years, they have often downsized, stripping away non-critical positions and leaving the remaining staff stretched to complete business as usual. Control requires resources — and many of those resources had been stripped away, and there was no ready resource "standing by" to meet the sizable demands of Section 404 certification.

"Documentation resources are scarce and therefore costs are high."

AUTHOR ANALYSIS

The PCAOB would likely argue that such a view is misguided because (a) management must establish a mechanism to ensure itself that controls are effective, (b) independent testing of the system by the organization is an appropriate method to gain such assurance, and (c) management must understand its obligation to independently assure the effectiveness of internal controls over financial reporting. The PCAOB takes a firm view that the auditor must attest management's assertion, i.e., management, not the auditor, is responsible for documenting and gaining assurance about the effectiveness of internal controls. The authors believe that future improvements in control processes, particularly with advances in the automation of controls, coupled with better information, communication, and monitoring systems, will allow management to gather sufficient evidence to meet their obligations on attesting to the effectiveness of internal controls by assuring themselves that monitoring and feedback controls are effective. Tests of individual controls can be limited in extent to providing evidence that the overall control process, especially the effectiveness of monitoring controls, is effective. We believe such a change is inevitable because of the need to be cost efficient, and such a change is compatible with the COSO internal control framework. However, the change may require a change in thinking on the roles of three major parties involved: management, auditors, and the PCAOB.

"Company views 404 as a compliance exercise and not an improvement exercise; will only do what it takes to comply but no more."

"To meet the first year of compliance, companies are scrambling to document and test controls along with managing the external auditor. No time to analyze and implement any potential benefits."

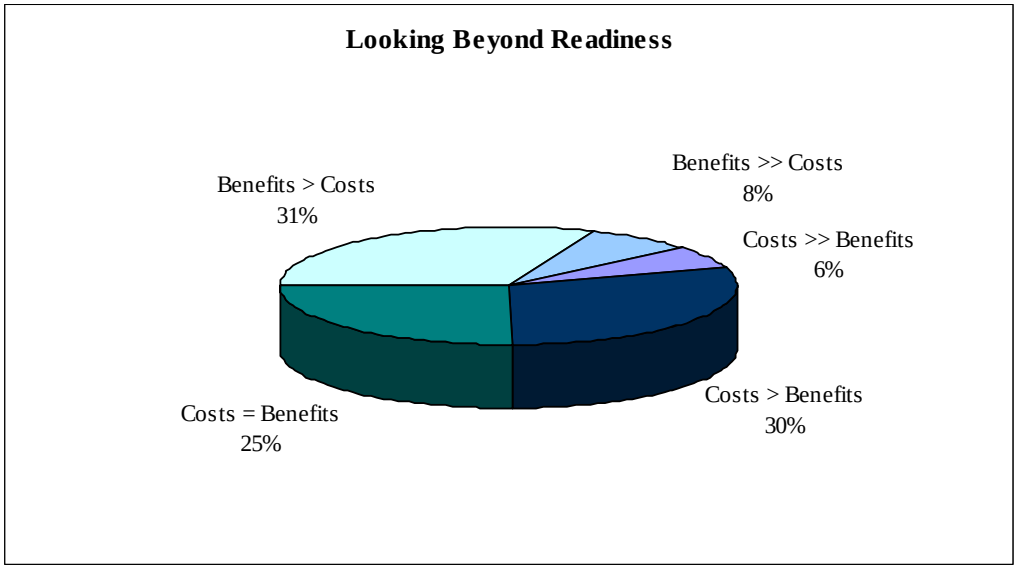
AUTHOR ANALYSIS

Our practical observation is that most organizations began the process with an unstated, but real objective of doing the minimum required to get a clean opinion from the external auditor. In other words, the emphasis was on meeting the literal requirements of the legislation. However, in doing so, the companies often missed opportunities to streamline processes, automate activities, and eliminate redundancies. In the effort to gain base-level compliance only, most organizations have ignored the opportunity to identify inefficiencies, remediate, and reap savings.

Prognosis – Cost/Benefit Tips in Favor of Benefits

When looking beyond the first year readiness costs and learning costs, 4% of the survey respondents felt the long-run benefits from the internal control evaluation processes would at least equal the cost, with over half of those respondents believing the benefits would be greater (>) or significantly greater (>>) than the costs. The results are displayed in Exhibit 14.

Exhibit 14
Relationship of Cost of Readiness Activities and Benefits Considering a Reduced Level of Continuing Costs



Earlier when we looked at only the first year efforts, only 28% of the respondents felt that the benefits were at least equal to the costs when considering the upfront readiness effort. Looking beyond the first-year costs, the view has changed significantly. A comparison of the two views is displayed in Exhibit 15.

Exhibit 15
Relationship of Cost of Readiness Activities and Benefits

	First Year -- Readiness Effort		Looking Forward to Steady State of Control Assessments	
Costs Greatly Exceed Benefits	37%		6%	
Costs Exceed Benefits	35%		30%	
Costs Equal Benefits	14%		25%	
Benefits Exceed Costs	13%	28%	31%	64%
Benefits Greatly Exceed Costs	1%		8%	

During the first year, only 14% of the total respondents felt benefits exceeded costs. When asked to look ahead and ignore the one-time costs, 39% believed benefits would exceed costs, while another 25% perceived that costs and benefits would equal out. We perform more detailed analysis by groups as shown in Exhibit 16. It is interesting to note that 50% of Retail, Distribution, and Technology respondents felt that benefits exceeded or greatly exceeded costs when looking beyond the one-time costs. The least favorable responses to this question came from manufacturing respondents, with only 34% believing benefits exceeded or greatly exceeded costs. A breakout by industry grouping is provided below.

Exhibit 16
Benefits Exceed Costs - Looking Forward
Analysis By Industry

Average	Financial Institutions	Insurance	Manufacturing	Retail	Technology	Other
39%	44%	38%	34%	50%	50%	34%

This overall shift in perspective appeared to be driven both by a belief in increasing benefits over time, as well as an expectation for significant compliance cost savings going forward.

Reaping the Benefits

As noted above, many of the participants believe management will be able to take advantage of the readiness investment to streamline, simplify, and standardize their processes. What they could not accomplish in year 1 due to time and cost constraints they believe they will accomplish in the future.

> *"SOX 404 has been invaluable to improving controls in our business, especially as it provides a 'big stick' when necessary to encourage action by some managers."*
>
> *"Monitoring processes done as a matter of routine rather than add-on work will drive cost efficiency."*
>
> *"Unique processes and systems create a multiplier effect when creating risk/control profiles which increase documentation, testing, and remediation efforts. Greater ownership by management allows them to see such inefficiencies and improve the operating and control environment which they manage."*

Reduced Maintenance Costs

Our respondents did see the narrow focus on compliance changing in future years. When asked to answer the cost/benefit question looking forward, after the significant upfront costs associated with readiness, the perspective of the relative costs and benefits shifted greatly. Respondents believed that costs will significantly decline in the future. When asked "To what extent do you believe costs will decrease in future years as compared to this year?", 43% of the respondents estimated reductions of

50% or greater in year 2, and 54% felt cost savings of at least 40% would be realized. When asked to look into years 3 and 4, increasing reductions were expected. Over half of the respondents felt costs would be reduced another 20% in year 3, and over 75% of the respondents expected another 10% reduction by the end of year 4.

Exhibit 17
Expected Cost Reductions in Future Years for Section 404 Compliance
% of Respondents

	Compliance Costs Savings Equal to or Greater Than:				
	50%	**40%**	**30%**	**20%**	**10%**
In Year 2	43%	54%	70%	93%	99%
In Year 3	12%	17%	25%	52%	87%
In Year 4	12%	18%	21%	29%	77%

As we move into year 2, companies expect to realize cost savings of this magnitude for three primary reasons: the upfront documentation effort is completed, management now understands the process and requirements, and third-party services will be greatly reduced.

However, there was also caution expressed. Will companies be able to embed the needed control awareness and ownership into the fabric of their ongoing business activities, or will it become a once a quarter (or worse, once a year) mad rush to document, test, and remediate? Will monitoring processes be automated, or will management continue to rely on a collection of spreadsheets and narrative documents, with the ongoing challenge of version control and update? In the words of some of the survey participants:

"Need to remember SOX is not a one-time thing and now we can move on to something else. If senior management does not speak positively, nobody else will be supportive of the continuing efforts and benefits."

"It is cheaper to maintain control documentation on a continual basis than having to recreate each quarter or year end. More automated processes improve reliance on controls and decreases costs of manual efforts and related testing."

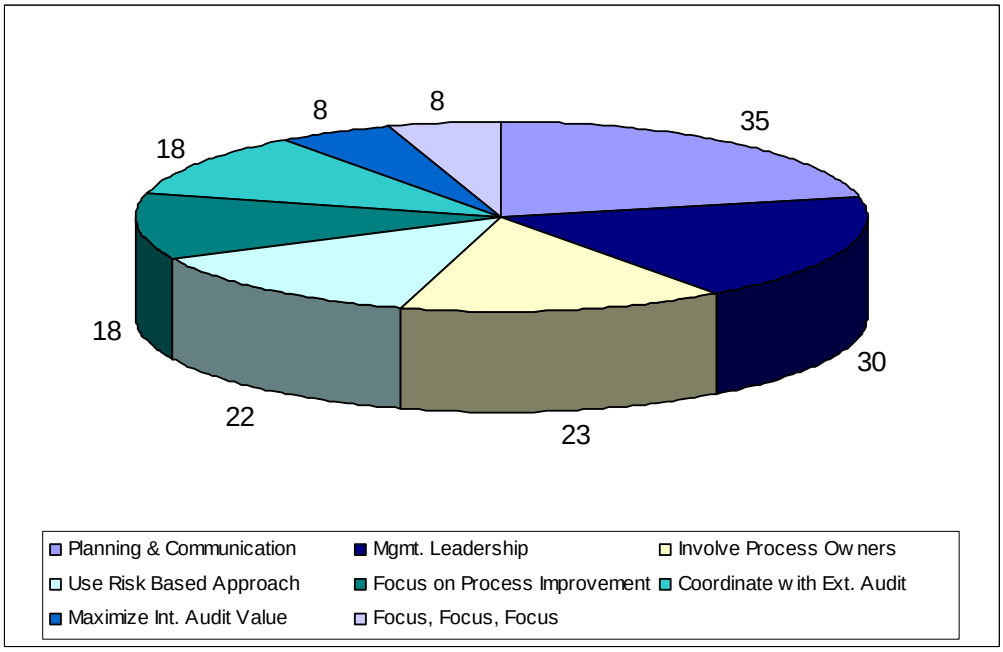
"Two dangers going forward are that management heaves a sigh of relief when compliant and forgets to keep the assessment going. Secondly, they establish their own "testing" people which duplicates work done by internal audit and adds unnecessary cost."

Lessons Learned

It is important that we learn from the efforts made by all those involved in this year's process of meeting the regulatory requirements. The responses are somewhat as expected, e.g., get involved earlier, develop a consistent methodology, automate controls and the documentation process as much as possible, reinvest in the control system (like other processes it needs adequate resources). We probed each of these areas to develop a deeper understanding of the processes.

We have summarized the major comments in Exhibit 18.

Exhibit 18
Lessons Learned for Going Forward
Number of Responses



It is not unusual to significantly underestimate the time it will take to accomplish a particular task. Thus, the number one recommendation is to plan the project early — and in detail with assigned responsibilities and timetables for completion. The plan must include the necessary training of the process owners, as well as developing consistent control and documentation guidelines to be used throughout the organization. Management can play an important role in providing support for the project. Respondents phrased it in various ways, but all essentially followed the tone of the comments below.

Need for Supportive Management

"Audit committee and CEO active support are essential to people taking the process seriously."

"Board and execs must have robust understanding of control systems, and set right tone."

"Senior line management needs to be actively engaged in process — cannot be delegated to a special 404 staff."

We like two comments that really summarize the lessons:

"START NOW"

and

"Anyone can make something complicated, but few can make it simple."

AUTHOR ANALYSIS

The common theme we saw from the respondents is that management must take ownership right away, set the tone for a constructive exercise rather than just meeting regulatory requirements, involve the process owners to help embed the control consciousness in the organization, apply a risk-based approach to determine the areas needing greater focus, do not wait too long to evaluate technology and IT controls, and most important, START NOW! The respondents did not uniformly recommend a software package, and did not uniformly recommend who should own what role. However, they did recommend that the organization develop uniform policies and procedures, and that there are significant advantages (and sometimes cultural difficulties) in communicating to all organizational units the ONE standard for effective controls.

Recommendations to Regulatory Agencies to Improve the Process

Auditors, management, and process owners dealt with significant uncertainty this year as they attempted to address the legislative requirements while waiting for the PCAOB to issue audit standards and guidance. We asked for the CAEs' insights on lessons to be learned from having dealt with the Section 404 control processes for a year. We also asked for their recommendations to regulatory agencies which would continue to achieve the legislative objectives, but would be more practicable and cost effective. A summary of their responses is shown in Exhibit 19.

Exhibit 19
Recommendations to Legislative Agencies

Nature of Recommendations	Number	Percentage
Clearer Direction on Requirements • Material deficiency • Threshold – needs to be more reasonable • Understand integration of accounting & other controls	44	29%
More Detailed Guidance • Industry guidance • Smaller business • Apply definitions in IT environment • Standardized approaches	33	22%
Less Detailed, More Principles-based Guidance • Less detail, more concepts • Keep framework simple • Allow management more flexibility in achieving objectives as long as objectives are achieved	16	11%
More of a Risk-based Approach • Allow risk to differentiate work • Focus more on management, less on transactions	14	9%
More Focus on Control Environment • Too much emphasis on transactions • Include systematic evaluation of compensation schemes	9	6%
Expanded Role for Internal Audit	9	6%
Less Focus on Documentation	6	4%
Other: • Reduced version for smaller companies • Develop lessons learned • Drop independent auditor attestation • Understand control correction is part of the process, i.e., there is no deficiency when errors are identified by the control system for correction	20	13%

Some of the responses were predictable. Auditors want more precise guidance. An interesting question, analogous to the debate in financial accounting standard setting, is whether guidance can be "principles-based" or whether the guidance must be detailed. While it seems that all auditors and accountants endorse a "principles-based" approach to accounting and auditing, they want the certainty of detailed prescriptions.

Some of the other responses are quite insightful:

- Error identification and correction are normal parts of a good control system; thus, if the system identifies and corrects errors as a regular part of the process, there is no control deficiency,
- Encourage auditors to spend more time looking at the "tone at the top" and considering the implications on the overall financial statement assertions,
- Include specific requirements to evaluate the effect of compensation schemes on management motivation and how the schemes may affect the overall control structure,
- Understand that it is difficult to segregate accounting and other controls, and
- Allow the organization to follow a risk-based approach to identifying and evaluating controls.

Future of Internal Auditing

To date, most organizations have focused their Section 404 efforts on achieving first-year compliance, and not on creating an ongoing, repeatable compliance process. In many instances, the organizational responsibilities and structures to support an ongoing assessment process, as well as supporting tools and technologies, have not yet been implemented. As noted earlier in this study, internal audit has played a significant role in most organizations' first-year compliance efforts — ranging from 20% of organizations in our survey who assigned the overall responsibility to internal audit, to the 65% of the organizations where internal audit was responsible for the testing of controls. In this environment, a clear question emerges on the future role of internal audit: How much will internal audit "own" of Section 404 compliance going forward?

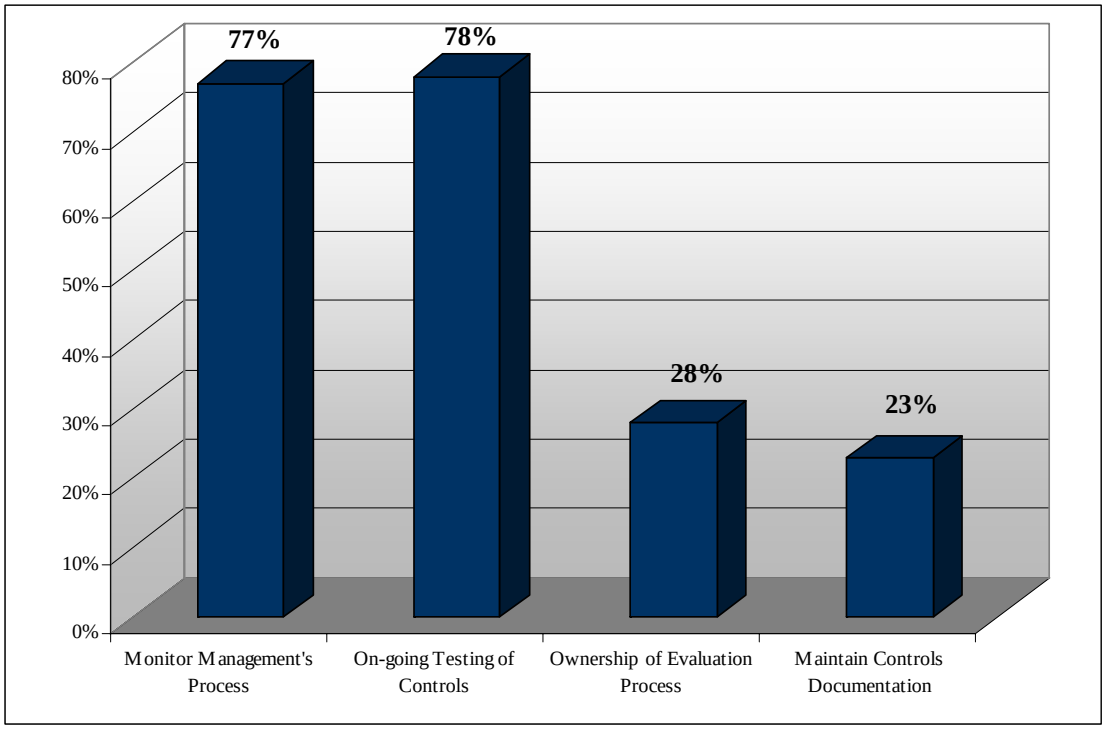
AUTHOR ANALYSIS

The tension between "principles-based" standard setting and detailed guidance is interesting, and applies to control evaluations just as much as it does to financial accounting. The respondents seem to indicate they are capable of making "principles-based" decisions, and perceived PCAOB Audit Standard 2 to be prescriptive rather than principles-based. They also found the definitions of significant and material deficiencies to be somewhat abstract. The most important issue, from our viewpoint, is that if the regulatory agencies want to move to a "principles-based" approach to standard setting, the standards must be conceptual and capable of relative uniform implementation of professionals. It also means that we must wean professional accountants/auditors away from reliance on checklists and detailed guidance and instead require informed decisions based on a solid understanding of the concepts and evidence of control effectiveness. This is an education process that must begin in our universities and must be reinforced by every aspect of practice.

To help answer this question, our survey included two forward-looking questions — one asking participants to describe the role of internal audit regarding 404 work looking ahead, and a second asking participants to describe their expectations for the level of internal audit work in the coming year in a variety of potential audit areas, including Section 404.

The answers to the first question are noted graphically in Exhibit 20 and suggest the heavy ongoing involvement of internal auditing in Section 404 compliance efforts, or at least in the monitoring and testing processes. The vast majority of respondents see internal audit as the responsible function to monitor management's Section 404 compliance processes. Given internal audit's responsibility to help monitor risk management and governance processes in an organization, this is not surprising. Perhaps what is surprising is that 23% of the respondents did NOT see this as internal audit's role!

Exhibit 20
Likely Role of Internal Audit Looking Forward
% of Total Survey Respondents

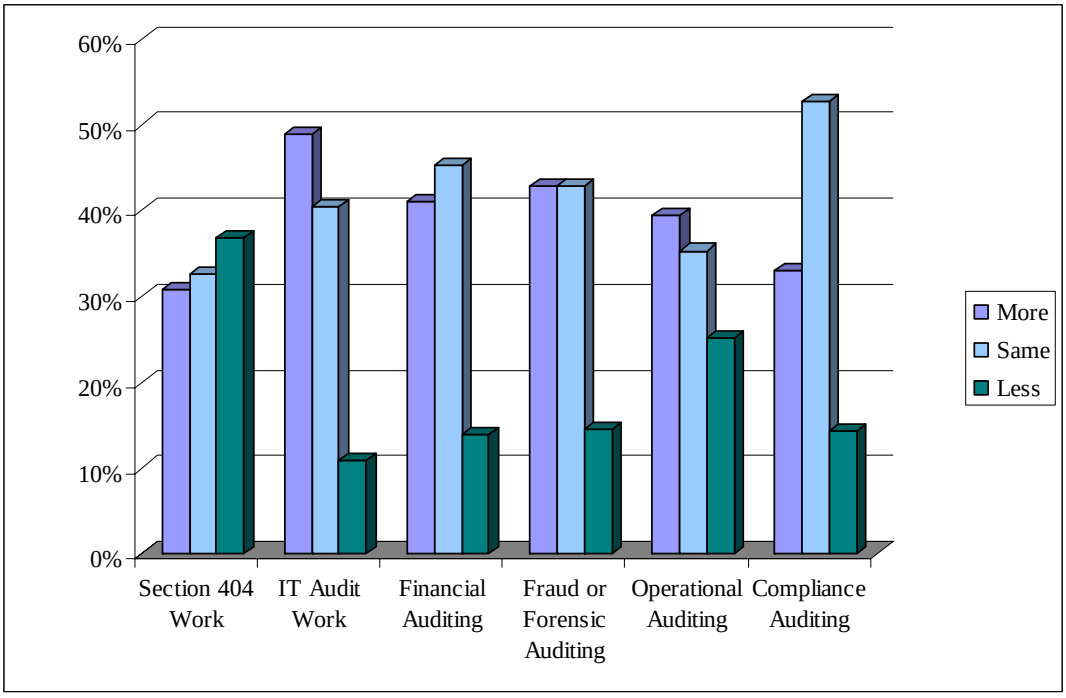


In addition, over 75% of the survey participants believe internal auditing will be responsible to conduct the ongoing testing of control effectiveness to support management's year-end certification. Given that internal audit houses the control expertise for most organizations, this result is, again, not surprising. The internal auditing profession's view, as described in the May 2004 position paper from The IIA titled "Internal Auditing's Role in Sections 302 and 404 of the U.S. Sarbanes-Oxley Act of 2002," is that internal audit should support management's compliance effort, to the extent this support does not impact objectivity or the ability of internal audit to cover major risk areas in the organization. The guidance recognizes that internal audit may be called upon to assist in the design and execution of testing, but reinforces management's responsibility for testing. It appears that most organizations are still choosing to have internal audit take on the total testing responsibility.

What is surprising is the percentage of companies planning to have internal audit responsible for maintaining controls documentation (23%) or for overall ownership of the evaluation process (28%) — areas generally viewed as the clear responsibility of management: the controller, a compliance manager, and/or the business process owners.

We also sought information as to where internal auditing was likely to go in the future, i.e., would they focus on risk management, operational audits, IT audits, or would they become a slave to Section 404 work and management and the audit committee's need to focus on financial reporting controls? An overview of the responses is shown in Exhibit 21.

Exhibit 21
Expectations Regarding Nature of Internal Audit Work in Coming Year



Recall that the expectations in Exhibit 20 are based on the work that internal auditors performed this year, i.e., most internal auditors had devoted a significant portion of their audit resources to Section 404 work. Thus, we wanted to know — starting with this biased base — if internal auditors would be switching back to operational or compliance audits.

The results are mixed: they expect to reduce the amount of 404 work, but do not expect a significant change back to operational and compliance audits. The area of biggest new effort will be IT audits — a common theme among the control findings. Their responses also show a continuing focus on Section 404, thus somewhat limiting the extent of other value-added services internal auditors have been providing in the past decade.

Exhibit 22
Future Work Planned for Internal Audit

Nature of IA Audit Work in the Next Year	Less or Substantially Less	Same	More or Substantially More
IT Audit Work	11%	40%	49%
Fraud or Forensic Auditing	14%	43%	43%
Financial Auditing	14%	45%	41%
Operational Auditing	25%	35%	40%
Compliance Auditing	14%	53%	33%
Section 404 Work	37%	32%	31%

AUTHOR ANALYSIS

From the respondents' answers and our experience to date, it appears that internal auditing is — at least temporarily — being significantly defined by the pressures of the required assessment of internal controls over financial reporting brought on by the Sarbanes-Oxley Act. This is understandable, as internal auditors have proudly built a reputation of being "internal control experts." But with this current focus, there is also a risk that internal auditing may lose some of its past identity – and reduce its potential contribution to the organization — as it minimizes its operational focus in favor of Section 404 compliance.

There have always been more opportunities for internal audit to assess activities and projects than time and resources would allow. A robust internal audit group has looked beyond control assessment to the broader concepts of risk management and governance for several years. The definition of internal auditing promulgated by The Institute of Internal Auditors clearly describes the broad character of the function:

> "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."

One of the CAE's ongoing challenges has been to develop a plan and process, after consideration of these broad areas, which would focus his or her limited resources and provide the most value to the organization. Historically, CAEs have dealt with this challenge by basing their annual audit plan on the results of a rigorous enterprise-wide risk assessment, enabling them with confidence to allocate their resources to topics of highest perceived risk.

In an enterprise-wide risk assessment, all aspects of an organization and key alliances were "fair game" — operating, support, and corporate organizations, as well as contractual partners.

Has this plan development process now changed, or does it need to change? That is, are CAEs now faced with allocating a significant percentage of their available resources to Section 404 compliance activities regardless of the risk profile, with the remaining leftover time, if any, available for risk-based auditing? If so, has the function been relegated to a legal compliance/quality assurance support function for management's assertion? Alternatively, one could conclude that Section 404 compliance, due to the associated legal and regulatory requirements and the potential for harm to the organization's reputation, is defacto a "high risk" activity warranting internal audit's attention.

Our survey does not hold the answers to these questions, and we suspect the answer varies by organization and size of internal audit function. However, we do believe that focusing only on Section 404 compliance without a significant focus on operational processes and controls will lead to a decreased value of internal audit to the organization. Early reviews of the COSO Enterprise Risk Management framework indicate that companies can enhance the effectiveness of their control activities — from a broad operational viewpoint — by embedding risk management activities within the culture of the organization. We believe the chief audit executive needs to be proactive in developing risk-based audit plans and in making the case for the incremental resources to address and reduce the identified risks. In other words, we do not believe that internal audit should sit and wait for the audit committee to initiate a discussion about the breadth of activities because the audit committee, by necessity, has to have a high priority on Section 404 compliance as organizations win back the public trust.

This conversation is significant. Not only does it impact the character of internal audit, it determines the function's ability to provide value to an organization, and it impacts its ability to attract and retain new talent, as well as changing the hiring profile, training needs, and career development opportunities for the professional staff. CAEs should plan to strategically leverage the Section 404 experience — the heightened visibility of internal audit and increased appreciation for the importance of controls, risk management, and governance throughout the business — to further the value internal audit can provide. Our vision includes a continuation of risk-based audit planning, with internal audit fulfilling an important monitoring role over Section 404 compliance without "owning" Section 404 compliance, and, most importantly, internal audit fulfilling an important risk management and governance role.

SUMMARY

We surveyed 171 practicing internal auditors about their assessment of costs and benefits associated with Section 404 work. Three major themes emerged in the survey:

First, there are significant benefits associated with the control identification, documentation, and testing process. The evaluation process has led to improvements in basic internal controls, such as reconciliations. There were substantial improvements in the control environment that came about as a direct result of the process. Many companies recognized they have vulnerabilities in the Information Technology area and will be devoting more resources to improving and evaluating IT controls as they move forward. Companies have more confidence in their control structure and are evaluating accounting risks, which should enable investors to have more confidence in the reliability of unaudited data furnished to the securities market.

Second, the prognosis is that the future costs associated with Section 404 will decrease substantially as we look forward three years. Much of the initial cost came about because controls had not been systematically documented or evaluated prior to the Section 404 requirements. CAEs see the process as becoming more systematized. The authors believe companies will see significant efficiencies as they fully implement the information, communication, and monitoring concepts embedded in COSO's *Internal Control – Integrated Framework.*

Third, there is uncertainty about the future role of internal auditing with respect to Section 404 work. The majority of chief audit executives recognize a need to invest resources in IT auditing. The majority of internal auditors want to maintain a strong presence in the risk and control arena, and recognize the need to perform more operational auditing that continues to add value to the organization. Most CAEs see themselves playing a major role in ongoing monitoring and testing activities associated with Section 404 work. We were a bit surprised that a not-insignificant minority (20%) saw themselves as taking responsibility for Section 404 work. We were surprised because such ownership is inconsistent with both the concept of internal auditing as well as The IIA's *Standards*.

Challenges remain: control evaluation must become more efficient; a culture of risk and control must be embedded in the organization; companies must invest more internal resources in control activities (downsizing had hurt); and companies must invest more resources in the internal audit activity. Our research indicates that the substantial costs in implementing Section 404 work in the first year was necessary because of (a) years of control neglect and downsizing by many companies; and (b) the nature of start-up work necessary to win back investor's confidence. The control processes will become more efficient and effective. We now have some idea about the benefits associated with Section 404 work and our assessment is that the benefits have been underestimated and they are substantial.

About The IIA Research Foundation
The IIA Research Foundation is the global leader in developing, sponsoring, disseminating, and promoting research and knowledge resources to enhance the development and effectiveness of the internal audit profession. Founded by The Institute of Internal Auditors, Inc. in 1976, The Foundation has set the standard for professional achievement in the internal audit profession.

The Foundation's major objective is to support research and education in internal auditing, thereby enhancing the development of the internal auditing profession. The IIARF accomplishes this by:

- Providing timely, relevant information on the roles and responsibilities of internal auditing as well as emerging trends and model practices within the profession.
- Funding, supporting, and disseminating both theoretical and applied research, and educational products.
- Developing ongoing funding of research and educational efforts.
- Helping to improve internal auditing research and education in colleges and universities by encouraging, supporting, and assisting in the implementation of collegiate curricula and programs in internal auditing.
- Building relationships among researchers, authors, practitioners, academics, and others.

The Foundation was declared tax-exempt under Section 501(c)(3) of the U.S. Internal Revenue Code on September 20, 1976. Operating exclusively for research and educational purposes, the Foundation pays no taxes on earnings or contributions received. In turn, when U.S. individuals or organizations contribute to the Foundation, their contributions are deductible under Section 170 of the U.S. Internal Revenue Code.

For further information about The IIA Research Foundation, visit www.theiia.org.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, its member firms, and their respective subsidiaries and affiliates. Deloitte Touche Tohmatsu is an organization of member firms around the world devoted to excellence in providing professional services and advice, focused on client service through a global strategy executed locally in nearly 150 countries. With access to the deep intellectual capital of 120,000 people worldwide, Deloitte delivers services in four professional areas — audit, tax, consulting, and financial advisory services — and serves more than one-half of the world's largest companies, as well as large national enterprises, public institutions, locally important clients, and successful, fast-growing global growth companies. Services are not provided by the Deloitte Touche Tohmatsu Verein, and, for regulatory and other reasons, certain member firms do not provide services in all four professional areas.

As a Swiss Verein (association), neither Deloitte Touche Tohmatsu nor any of its member firms has any liability for each other's acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names "Deloitte," "Deloitte & Touche," "Deloitte Touche Tohmatsu," or other related names.

In the U.S., Deloitte & Touche USA LLP is the member firm of Deloitte Touche Tohmatsu, and services are provided by the subsidiaries of Deloitte & Touche USA LLP (Deloitte & Touche LLP, Deloitte Consulting LLP, Deloitte Tax LLP, and their subsidiaries) and not by Deloitte & Touche USA LLP. The subsidiaries of the U.S. member firm are among the nation's leading professional services firms, providing audit, tax, consulting, and financial advisory services through nearly 30,000 people in more than 80 cities. Known as employers of choice for innovative human resources programs, they are dedicated to helping their clients and their people excel. For more information, please visit the U.S. member firm's website at www.deloitte.com/us.

The Institute of Internal Auditors

March 31, 2005

David A. Richards, CIA
President

Tel: +1 407 937 1200
drichards@theiia.org

Jonathan G. Katz
Secretary
U.S. Securities and Exchange Commission
450 Fifth Street, N.W.
Washington, DC 20549-0609

Re: Implementation of U.S. Sarbanes-Oxley Act Internal Control Provisions

File Number 4-497 - Response to be emailed to: rule-comments@sec.gov

Dear Mr. Katz:

The Institute of Internal Auditors (IIA) welcomes the opportunity to comment on the implementation of the Sarbanes-Oxley Internal Control Provisions and commends the efforts of the SEC to promote effective corporate governance. The IIA has long advocated that good governance and accurate financial reporting emanate from the balanced interaction of board members, executives, external auditors, and internal auditors. The U.S. Public Company Accounting Oversight Board (PCAOB) has worked hard in its efforts to codify the standard governing the implementation of sections 404(b) and 302(a) of the Sarbanes-Oxley Act.

Clearly, the first year's implementation has provided many lessons learned. A recent report issued by The IIA's Research Foundation concluded through survey that there have been many control improvements as a result of implementing Sarbanes-Oxley. Most notable are a more engaged control environment, with active participation by the board, audit committee and management, and a broader understanding of controls by personnel and management throughout the organization. (See copy of research report in Attachment C.)

Representing more than 102,000 members worldwide – approximately 46,000 of whom are in 133 chapters located across the United States – The IIA is the global voice, acknowledged leader, and recognized authority of the internal audit profession. The IIA maintains the *International Standards for the Professional Practice of Internal Auditing (Standards)*, which are recognized throughout the world.

Internal Auditing's Role in Corporate Governance
We believe that internal auditors play a vital role in improving corporate governance, risk management, and control processes because of their unique position within their organizations. The IIA's definition of internal auditing acknowledges this role in corporate governance:

"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."

Global Headquarters
247 Maitland Avenue
Altamonte Springs, FL
32701-4201 U.S.A.
Tel: +1-407-937-1100
Fax: +1-407-937-1101
www.theiia.org

Since the adoption of this definition in 1999, The IIA has intensified its efforts to contribute to the reform of governance practices of public companies around the world. IIA leaders, including prominent chief audit executives (CAEs) from various industries, contributed to the development of this response. We also gathered information from a formal survey of over 1,900 CAE members.

IIA's Recommendations for Change (Detailed Comments in Attachment A)

To the SEC:

1. Consider the importance of enterprise-wide risk management and controls other than those limited to financial reporting. Good governance is an enterprise wide effort and since other jurisdictions have adopted a much wider view, the SEC should consider what guidance should be provided to management to ensure all aspects of strong governance are considered and addressed by publicly-traded organizations.
2. The lack of detailed guidance by the SEC to management on what is expected of them regarding the control assessment process has caused management in many cases to turn to their external audit to obtain guidance on what is acceptable. This has resulted in the PCAOB setting the standard for management on what is required to perform a control assessment – rather than management setting the standard based on the guidance from the SEC.
3. Provide further detailed guidance regarding the quarterly 302 assessment process and the reporting on the status of remediation efforts to handle material weakness disclosures.
4. Provide additional guidance on how to determine "principal evidence". In practice the current guidance has proven to be inadequate, resulting in the external auditor relying on the work of others for much less, we believe, than the guidance would suggest. If there is an overemphasis on routine control activities and not enough time spent on key issues such as top management overrides, then we are defeating the intent of the law to improve governance.
5. Increase the cost effectiveness of Sarbanes-Oxley provisions by eliminating the requirement that each issuer's external auditor attest to the assessment made by management, encouraging greater reliance on the work of internal auditors, clarifying rules, and encouraging communication between the audit committee, external auditors, and management.
6. Finally, The IIA believes in many organizations that the internal audit function contributed to the successful implementation of the Sarbanes-Oxley internal control provisions by shifting some of their work away from other priorities. In the longer term the sustainability of this "redirection" of internal audit coverage should be questioned. The IIA believes the annual internal audit plan needs to be balanced, and reflect all the risks facing the organization, not just the financial reporting related risks.

To the PCAOB:

7. Increase reliance on the work of others related to their assessment of the control environment. The present PCAOB standard #2 describes factors for external auditors to consider when determining the ability to rely on the work of others or to perform the work themselves. Attachment A details several areas that currently require the external auditor to perform the work where relying on the work of others would be more efficient and effective. We also believe that reliance on the work of others is desirable for some of the walkthroughs currently mandated by the standard. By eliminating the external auditor's use of judgment and requiring the extent of testing (principal evidence) and walkthroughs, duplication in work can occur, which leads to implementation time and resource inefficiencies.

8. Increase reliance on the use of work of a competent and independent internal audit function. The IIA believes an organization with an established internal audit function operating in accordance with The IIA's *International Standards for the Professional Practice of Internal Auditing* is well equipped to meet the challenge of good governance. While the PCAOB standard appears to allow the external auditor to rely on the work of internal auditors, year-one implementation has not proven this to be the case in many organizations. Using the work of internal auditors, where appropriate, would increase efficiencies in testing and reduce costs. Where internal audit has done testing or performed walkthroughs that fall within the scope of the financial reporting controls, external audit should rely on their work.
9. Finally, with regard to the extent of testing controls, the external auditor should be able to determine whether partial reliance on the results of testing from prior years is acceptable. Such reliance will more likely be possible when the design and operation of the controls has not changed significantly from the prior year. The external auditor would, however, need to confirm if the risk of an unnoticed change in controls is indeed low when planning on partial reliance on evidence gathered in the prior year.

Internal Auditing's Role in Sections 302 and 404 of the U.S. Sarbanes-Oxley Act of 2002
We also have enclosed The IIA's position paper "*Internal Auditing's Role in Sections 302 and 404 of the U.S. Sarbanes-Oxley Act of 2002"* (Attachment B). The IIA strongly believes that internal auditing can contribute significantly to the organization's efforts to improve internal controls and financial reporting. Management is responsible for implementing the processes necessary to meet the regulatory requirements of Sarbanes-Oxley. The internal auditor should support management in carrying out its responsibilities but not take on management's responsibilities for documenting controls or implementing systems of internal controls.

We appreciate the opportunity to express our views on these important matters and welcome the opportunity to discuss any and all issues with you, at any time.

Best regards,

David A. Richards, CIA

Attachments
A - Detailed comments by The IIA
B - *Internal Auditing's Role in Sections 302 and 404 of the U.S. Sarbanes-Oxley Act of 2002* – An Institute of Internal Auditors' position paper.
C - *Sarbanes-Oxley Section 404 Work - Looking at the Benefits* – An Institute of Internal Auditors Research Foundation report.

THE INSTITUTE OF INTERNAL AUDITORS

Attachment A

Detailed Comments Regarding the Implementation of the

Sarbanes-Oxley (SOX) Internal Control Provisions

The Institute of Internal Auditors (IIA) is supportive of the SEC; however, opportunities exist for changes to enhance the effectiveness of the SOX provisions. In addition, The IIA recognizes that many of the following changes would need to come from the PCAOB and encourages the SEC to work with the PCAOB to effect the recommended changes.

1. Increase Ability of External Auditors to Rely on the Work of Others

Auditing Standard (AS) No. 2 provides the external auditor with specific guidance on when and how they can use the work of others in performing their audit of internal controls over financial reporting. The effectiveness and efficiency of an external auditor's testing of internal controls over financial reporting would be improved with the following changes:

a) Allow the external auditor to selectively rely on the work of others related to their assessment of the control environment

Paragraph 112 of AS No. 2 describes factors for external auditors to consider when determining the ability to rely on the work of others or to perform the work themselves. These factors include the degree of judgment required to evaluate the operating effectiveness of the controls, the level of judgment or estimation required, and the potential for management override. These factors are not reiterated in paragraph 113 where the external auditors are instructed that they can never rely on any work of others in relationship to the elements of the control environment, which has caused additional work. The guidance in paragraph 113 is only consistent with paragraph 112 if every aspect of the control environment is so highly judgmental that reliance on others is unacceptable but this is not typically the case.

For example, the following elements of an effective control environment are not highly judgmental and can be effectively assessed by others:

- Existence of a written code of conduct and consistency of this code with other formal and informal policies, practices and standards of the business
- Methods of interacting with suppliers, customers, creditors, etc. as evidenced by written agreements, policies, and standards
- Formal job descriptions which define tasks that comprise particular jobs
- Frequency and timeliness of board of directors or audit committee meetings
- Sufficiency and timeliness with which the board of directors or audit committee is appraised of sensitive information, investigations or improper acts
- Frequency of interactions between senior management and operating management
- Adequacy of definition of key manager's responsibilities
- Appropriateness of control-related standards and procedures, including job descriptions
- Extent to which policies and procedures for hiring, training, promoting and compensating employees are in place
- Appropriateness of remedial action taken in response to departures from approved policies

— Adequacy of employee candidate background checks

In each of the above areas, the guidance of AS No. 2 has led external auditors to ignore information prepared and analyzed by others. The external auditors believe the guidance of paragraph 113 requires them to perform the entire data gathering, testing of the integrity of that data, and evaluation of the data themselves. For many of these areas, and for many aspects of the evaluation process, relying on the work of others (such as by a competent and independent internal audit function), would be more efficient and effective. The information does not require a high level of complex judgment to gather and evaluate, and the prohibition in paragraph 113 is overly restrictive.

b) Allow the external auditor to rely on the work of others for some walkthroughs

AS No. 2 in paragraph 116 directs the external auditor to perform ALL walkthroughs themselves, regardless of the risk of the area being audited or the ability of others to adequately evaluate and document a walkthrough. A walkthrough can be an extremely useful mechanism for understanding a process and the related internal controls. However, the prohibition on the external auditor to consider relying on the work of others essentially implies that no one other than an external auditor can understand a process and document it through a walkthrough.

The principles behind the guidance in paragraph 126, the fifth bullet point, should be applied to reliance on the work of others for walkthroughs, i.e. there will be instances in which processes involve a low degree of judgment in evaluating operating effectiveness of controls, have a low potential for management override, and/or are simple in their construction. In such situations, the external auditor should be allowed to exercise judgment and elect to rely on the walkthrough work performed by others, i.e. the current prohibition in paragraph 113 is overly restrictive.

c) Provide additional guidance on how to determine "principal evidence"

AS No. 2 paragraph 108 provides some general guidance to the external auditor on how to determine whether their testing provides the principal evidence for their opinion. In practice, this guidance has proven to be inadequate, resulting in the external auditor relying on the work of others for much less than the guidance would suggest. The note at the end of paragraph 108 suggests that not all evidence is of the same importance in determining how much the "principal evidence" is. This nuance has been missed.

In practice, we believe external auditors are not placing any reliance on the work of others for areas like entity-level controls and pervasive controls, and have taken the position that they must personally obtain the majority of the evidence related to all other controls, including low-risk, routine transactions.

The scandals which were a large part of the rationale behind the requirements of section 404 dealt with management override of controls, highly subjective areas, and non-routine transactions. Focusing an external auditor's attention on these areas should provide a large degree of evidence in the areas of risk. However, many, if not most, external auditors continue to treat all individual elements of internal control equally and personally review the majority of the evidence for all elements of control individually, regardless of risk.

The guidance currently stated in AS No. 2 could be enhanced and more explicit guidance on the requirements for obtaining principal evidence is needed to allow a more effective and efficient approach to this work.

2. Improving Guidance Related to Obtaining a High Level of Assurance

AS No. 2 paragraph 104 provides that the testing for each year must stand on its own. During the preparation of AS No. 2, the PCAOB received feedback on the desire of some to allow the concept of "rotation" of audit testing to be used. The PCAOB rejected this suggestion requiring that each year must stand on its own. This approach in the standard results in inconsistencies within the guidance of the standard. In addition, how this has been interpreted in practice has resulted in an audit approach that frequently ignores the concept of risk to make sure everything is tested every year in a comprehensive manner.

Paragraph 105 requires the external auditor to design tests to provide a high level of assurance that the control being tested is operating effectively. The level of assurance required must correspond to the level of risk present in the control. While this concept is alluded to, in the third bullet under paragraph 105, it is not well developed. The following highlight the gaps in the current guidance:

— Audit results from testing in prior years should allow the external auditors to consider a shift in their testing. For example, during annual audits of controls of a transactional system, the external auditors may find that controls are well designed and expertly executed. After years of these findings, the auditors should consider shifting their testing methods from detailed re-performance of transactions to testing of monitoring or other high-level controls. Given the proven low risk of these systems, reliance on these higher level controls would still provide a "high level of assurance" based on the risk of the area being audited. Under the current guidance, external auditors are frequently concluding that an understanding of the risk of an area being audited built up from prior year audits should be ignored and all areas are to be assumed to be high risk. This is ineffective and inefficient.

— Paragraph E120 of AS No. 2 states that absence of fraud in prior periods is not a reasonable indicator of the likelihood of misstatement due to fraud in the future. We agree. However, it is a tenuous bridge from this statement to a conclusion that reliance on work performed in prior years is unacceptable. Absence of fraud may be due to good controls, or due to luck (a fraud wasn't perpetrated in that period). Absence of fraud is not a good predictor of the absence of future frauds, nor is it a good indicator of a good system of internal controls. However, years of evidence of excellence in the design of controls and their operating effectiveness does correlate highly to such attributes in future years. The proven existence of a highly effective system of internal controls is often a good indicator of an effective system of internal controls in future periods, assuming the risk of management override is properly addressed. Addressing this risk of management override requires much less testing than exhaustive testing of all internal controls every year.

— Paragraph 98 of AS No. 2 requires the external auditors to perform tests over a period of time adequate to determine whether the controls are operating effectively as of year-end. The period of time over which the external auditors are to perform their testing varies based on the nature of the control. This principle is neglected when the standard does not allow the external auditors to use the results of any testing performed prior to the beginning of the year. There can be controls, which by their nature, could be tested prior to the beginning of the year and still provide evidence for their operating effectiveness as of year-end. Well-established, mature processes do not become unstable or unpredictable merely because a year-end has passed.

3. Increase the cost effectiveness

Companies have embraced both the spirit and the letter of the Sarbanes-Oxley Act, in spite of the complaints about the cost of compliance. The IIA is surveying companies on the final cost of compliance for 2004, but it is clear from earlier surveys that they far exceeded everyone's initial estimates, and escalated throughout 2004 as companies and external auditors worked through the requirements, some of which were not finalized until late in 2004.

Companies expect to reduce the cost in year-two by leveraging what was done in year-one. However, studies show that management expects it will be year-three and beyond before costs fully stabilize. Recent surveys show that companies hope to realize reductions from year-one costs through improved learning curves, better automation of manual controls, centralization of multiple systems (like payroll or accounts payable), etc.

a) Eliminate the requirement that each issuer's external auditor must attest to the assessment made by the management of the issuer

The Act requires the external auditor to provide three opinions: (1) whether the financial statements are fairly stated, (2) whether internal controls over financial reporting are adequate, and (3) whether management's process for assessing internal controls is adequate. There is minimal value for investors to receive the third opinion. From an investor's viewpoint, having received the opinion of management and the opinion of the external auditor on the adequacy of internal controls over financial reporting, there is very little incremental benefit on the external auditor expressing an opinion on management's assessment process. The adequacy of management's process would likely affect the scope of testing performed by the external auditor, but shouldn't be assessed separately.

b) Allow the external auditor to use more of the work of internal auditors

- PCAOB Standard No. 2 requires external auditors to personally perform a walkthrough for each major class of transaction. We suggest (1) eliminate the requirement for walkthroughs because testing of transactions determines that the same control objectives are achieved (controls are working as designed) or (2) allow external auditors to use internal auditors to perform some of this work.

- Questions were continually raised in year-one about the extent of the external auditors' reliance on the work of others, including the internal auditors. We believe costs could be significantly reduced, without impacting the quality of compliance by greater utilization of internal auditors. The IIA has published a position paper (attached) which describes the various roles that internal auditors can play in Section 302 and 404 efforts.

- The IIA believes an organization with an established internal audit function operating in full compliance with the *Standards* and The IIA definition of internal auditing is already well equipped to meet the challenge of good governance and transparency of internal control effectiveness and efficiency. The *Standards* require the internal audit function to implement a quality assurance and improvement program and have an external quality assurance review a minimum of every five years.

c) Clarify the rules

- The lack of detailed guidance by the SEC to management, on what is expected of them regarding the control assessment process, has caused management, in many cases, to turn to their external audit to obtain guidance on what is acceptable. This has resulted in the PCAOB setting the standard for management on what is required to perform a control assessment – rather than management setting the standard based on the guidance from the SEC.

- Re-emphasize that the objective of the audit is for the external auditor to obtain reasonable assurance that no material weaknesses exist as of the date specified in management's assessment.

- There is need for further detailed guidance regarding the quarterly 302 assessment process and the reporting on the status of remediation efforts to handle material weakness disclosures.

d) Encourage communication

- Encourage the external auditors, the audit committee, and management to discuss and reach agreement on key controls prior to detailed testing to eliminate misunderstandings and unnecessary work, and to keep the focus on the controls over financial reporting.

- The audit committee should also play an important role in internal control oversight. The audit committee can work with management and with the internal and external auditors to ensure the strength of internal controls, and to help in determining the scope of the audit of the internal controls.

The Institute of Internal Auditors

Practical Considerations Regarding Internal Auditing Expressing an Opinion on Internal Control

IIA Web Site – http://www.theiia.org/

Practical Considerations Regarding Internal Auditing Expressing an Opinion on Internal Control

Table of Contents

Practical Considerations Regarding Internal Auditing Expressing an Opinion on Internal Control

Introduction

The chief audit executive (CAE) may be requested to issue an opinion on the adequacy of internal controls within the organization. This request is becoming more common with the advent of new financial reporting legislation and regulation. The *International Standards for the Professional Practice of Internal Auditing* (The *Standards*), specifically Standard 2410.A1 indicates, "Final communication of engagement results, where appropriate, contain the internal auditor's overall opinion and or conclusions." The need for such an opinion, and the ability of a CAE to express such an opinion, depends on individual circumstances. This paper provides guidance in those situations where a CAE does express an opinion on internal controls.

Some internal auditors have not expressed opinions on the adequacy of controls in the past, either on individual audits or for organizations as a whole. Instead, only specific weaknesses in internal control have been reported. This leaves the responsibility up to the reader to interpret the importance of the issues reported and the reader may often assume areas with no issues reported were "perfect." If a CAE issues an opinion, the CAE needs to consider the scope of the audit work, the nature and extent of audit work performed, and evaluate what the evidence from the audit means concerning the adequacy of internal controls. Such an opinion should express clearly:

- The evaluation criteria and structure used.
- The scope over which the opinion applies.
- Who has responsibility for the establishment and maintenance of internal controls.
- The specific type of opinion being expressed by the auditor.

The CAE should be careful that the opinion expressed is consistent with the internal audit activity's charter as approved by the board and supported by sufficient amount of audit evidence. A CAE should resist expressing an opinion related to a subject that is inconsistent with the charter. In addition, a CAE should not express an opinion that is not supported by sufficient audit evidence.

The CAE should also understand fully the reason and proposed use of any opinion that he or she is requested to issue. For example, does management intend to share the opinion with third parties or does management intend to place reliance on the opinion as a basis for any management attestation on controls? The CAE must ensure that any opinion is appropriate for its intended use and audience.

Evaluation Criteria and Structure

An opinion is best expressed when using a defined criteria and evaluation structure. Opinions can be very poorly defined, which leads to misunderstanding of what an opinion is saying. Using a defined evaluation structure allows the reader to better understand the opinion being expressed and helps to ensure the internal auditor is consistent in his or her formulation of an opinion across different audit areas and different time periods.

The *Internal Control–Integrated Framework*, published in 1992 and 1994 by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) is the most common framework for assessing internal controls.

The COSO report defines an internal control structure along five elements (control environment, risk assessment, control activities, information and communication, and monitoring) and three components/objectives (financial

reporting, operations and compliance), with identification of the areas/activities audited (e.g., geographic unit, business unit, process).

Other comprehensive structures have been developed and can be equally as useful. Governing law or other special circumstances should be considered in selecting the evaluation structure to be used.

A defined evaluation structure is especially useful to understand the scope of the audit work. For example, an opinion using the COSO framework can define whether the opinion extends to all three components of internal control and whether the audit work addressed controls along all five elements.

Many organizations have adopted their own criteria and policies on internal controls. Depending on the sophistication and detail of these policies, the CAE may use compliance with internal policies as his or her evaluation criteria. If the CAE uses, or is asked to use, an internal policy as evaluation standards, the CAE should ensure that the policies are sufficiently detailed and appropriate to serve as an evaluation standard.

Scope Description

The scope over which the opinion extends should be communicated clearly in the opinion document. Common elements defining the scope over which the opinion applies are descriptions of the portions of the organization being covered (e.g., specific departments, geographic areas, or subsidiaries) or processes (e.g., financial reporting, purchasing, or IT operations), as well as the control components/objectives covered by the audit (e.g., which financial, operational, or compliance objectives were addressed). The time period over which the opinion is expressed is also a critical element of the scope (e.g., an opinion as of a point in time or an opinion regarding controls operating during a specified time period).

Typical internal audits focus heavily on internal controls related to transactional processes. Care should be taken to define whether the opinion being expressed is limited to these types of transactional controls, or if it extends to broader aspects of internal controls. For example, did the internal audit consider "soft" aspects of the control environment, like tone at the top,

adequacy of training, etc? Also, did the audit consider not only controls related to transactional accuracy, but also compliance with laws over data privacy and regulatory reporting requirements? An opinion with a well defined scope will not leave the reader guessing as to the relevance, focus of the opinion, or time period to which it applies. Many internal audit activities use a risk-based audit plan. In some situations it might be difficult to issue an opinion on internal controls as the audit work performed may not cover a clearly definable portion of the organization.

Defining Responsibility for Internal Controls

Consideration should be given to clarifying within the opinion who has the responsibility for establishing and maintaining the internal controls audited. Internal controls should be the responsibility of process owners. Internal auditors provide assurance on the design and effectiveness of those controls, but are not responsible for them. This separation of responsibility and assurance is an underlying assumption of the definition of internal auditing developed by The Institute.

Types of Audit Opinions

There are two different types of opinions, positive assurance and negative assurance, and each conveys different meanings to the reader and provides different levels of assurance by the auditor. The opinion should describe the scope of work performed and the evaluation criteria and structure used. Expressing an opinion requires gathering sufficient competent supporting evidence, in conformity with the *Standards*. Different opinions likely require different levels of audit evidence. The alternative to expressing an opinion is to formally *disclaim* an opinion. This would be used when the auditor has not gathered, or is unable to gather, sufficient audit evidence to express any form of opinion and decides to clearly state that fact.

Positive assurance is one of the strongest types of audit opinions. In providing positive assurance, the auditor is taking a position on the strength of the

internal controls. Varieties of a positive assurance opinion are:

- Binary – internal controls are or are not appropriate in the situation, for example: internal controls are satisfactory or unsatisfactory, effective or ineffective, meet expectations or don't meet expectations, etc.
- Graded – the effectiveness of internal controls is rated using a grading system, for example: red-yellow-green, 1-2-3-4-5, etc.
- Directional – provides additional information about the direction of the opinion since a previous report, for example "Satisfactory, but diminished since last year."

A positive assurance opinion requires the highest level of evidence as it implies not only whether controls are adequate, but also that sufficient evidence was gathered to be reasonably certain that evidence to the contrary, if it exists, would have been identified. The auditor takes full responsibility for the sufficiency of the audit procedures to find what should have been found. Positive assurance opinions provide the reader a high level of information, which generally brings a higher level of confidence or comfort in the accuracy of the opinion. CAEs typically are requested to provide positive assurance opinions.

The CAE should ensure that a sufficient amount of audit evidence is obtained to express their opinion. For example, work often is performed on a rotation basis across many audit units, with the scope of the work performed based on work in multiple audit units. Giving a positive assurance opinion on each of the individual units may not be possible if the amount of work done in each unit is insufficient.

A grading scale can be useful in providing sufficient information to build a positive assurance opinion. Use of a grading scale would generally require a well-defined evaluation structure. In addition, the more detailed the grading scheme, the more evidence is required to support the grades. Thus, a grading scale can provide more precision in the positive assurance opinion being expressed. For example, an opinion that merely states that internal controls meet a minimum defined criteria would not require the same amount of evidence as an opinion that stated how much better

or worse internal controls are than a defined benchmark. Increased precision in the information provided in an opinion normally increases the amount of evidence needed to support the opinion. Providing a grade as part of a positive assurance opinion may provide useful information to the reader, but sufficient evidence is needed to support that finer level of detail given in the opinion.

Negative assurance is a statement that nothing came to the auditor's attention that would indicate inadequate internal controls. The auditor takes no responsibility for the sufficiency of the audit scope and procedures to find all concerns or issues. Such an opinion is less valuable than a positive assurance opinion as it provides limited assurance that sufficient evidence was gathered to determine whether internal controls were inadequate. A negative assurance opinion merely states that the internal auditor has not seen problems based on the work performed.

An opinion can be *qualified* with specific findings that contradict the overall opinion. Qualified opinions can be useful in situations where there is an exception to the general opinion. For example, the opinion may indicate that controls were, "Satisfactory, with the exception of accounts payable controls, which require significant improvement."

The *Standards* provide guidance for determining the adequacy of evidence and documentation. The CAE must ensure that any opinion expressed can be fully supported with sufficient audit evidence. The CAE should determine the level of audit evidence required to support an opinion on internal controls. This determination relies heavily on the judgment of the CAE based on the scope of the opinion and the risks in the organization being addressed by the internal controls. Some internal audit activities have sufficient resources to gather enough audit evidence to provide very definitive and descriptive opinions. Other internal audit activities do not have sufficient resources to gather enough audit evidence to provide any type of opinion other than negative assurance qualified with a clear explanation of the limited amount of testing performed.

Care must be taken with wording used in any opinion. The CAE must ensure the

wording of an opinion is clear and appropriately defined for the reader. Using general terms such as “satisfactory,” “effective,” or “adequate” alone may not sufficiently define their meaning. For example, the term “effective” usually refers to controls being effective both in design and in operation. It should be clear in the opinion whether both meanings are included. Another example is use of the general term “internal controls” which could be confusing without some definition of the type or extent of controls covered. Finally, in certain jurisdictions words have been assigned specific meanings. For example, in the United Sates, the terms "material weakness" and "significant deficiency" have very specific definitions and ramifications. CAEs should avoid using these defined terms unless they are reporting in accordance with the applicable regulations in that jurisdiction.

Interaction with Section 404 of the U.S. Sarbanes-Oxley Act of 2002

Most organizations who file financial statements with the U.S. Securities and Exchange Commission are required to comply with the requirements of Section 404 of the Sarbanes-Oxley Act of 2002. This section requires management to state its responsibility for establishing and maintaining adequate internal controls over financial reporting and include in the annual report an assessment by management as to the effectiveness of these internal controls.

A number of CAEs have been asked to sign an attestation stating that internal auditing has evaluated the effectiveness of internal control over financial reporting and whether they were found to be effective, or whether there were material weaknesses or significant deficiencies. Often, these attestations are drafted based on the attestation to be signed by the CEO and CFO of the organization for inclusion in the annual filings with the SEC.

CAEs should carefully consider the wording of the attestation before signing it. Signing such an attestation is expressing an opinion and the concerns discussed above come into play. Specific issues to consider include:

— If internal audit work is performed in accordance with an annual audit plan approved by the audit committee, the

objectives and scope of that plan may not provide enough audit evidence specifically related to internal controls over financial reporting to give a positive assurance opinion. By signing the attestation, the CAE is assuming responsibility for the sufficiency of the audit work done to express a positive assurance opinion. A negative assurance opinion, with reference to the scope of the internal audit plan, may be more appropriate if the amount of audit testing in this area is inadequate.

— A statement that there are no material weaknesses assumes that all areas within the organization that could have material weaknesses have been audited thoroughly enough to conclude they do not exist within the organization. If the audit plan did not cover all these areas, the opinion should be limited to the areas audited.

— The attestations drafted for signing by the CAE may refer to the adequacy of internal controls over which the signer has responsibility. Internal auditors have no responsibility for internal controls, but only the monitoring of these controls. Any opinion expressed in support of Section 404 should not imply that the CAE has any management responsibility for internal controls.

— If the internal audit activity has performed work related to the organization's readiness for compliance with Section 404 that impairs the independence and objectivity of the internal audit activity, the impairment should be noted in the opinion expressed. The Institute has published separate guidance concerning internal auditing's role in Section 302 and 404 of the Act that discusses situations where independence and objectivity may be impaired.

Practical Considerations

The following question and answer section applies the concepts described above in various situations.

Q. Why can't I just say that "internal controls are adequate"? This is a short and clear message and I know what it means.

A. The auditor may know what this means, but the reader may not. Such a brief statement, with no explanation of context, leaves the reader to assume a lot. For example: Does this opinion cover all regulatory aspects of the organization? Was the tone of the executive team evaluated as to its impact on internal controls and did the auditor document the evidence collected? Did the auditor test every control that exists in the organization?

Q. How do I express in my opinion that I have sufficient basis to make this opinion?

A. The *Standards* include discussion of the need for sufficient evidential matter to support the conclusions of an internal auditor. If the auditor's opinion states that the auditor complies with the *Standards*, the reader should be able to understand the basis for the auditor's opinion.

Q. I don't know what type of opinion my audience requires (e.g., positive binary, positive with grading scale, or negative). What should I do?

A. The CAE of an internal audit activity must understand the needs of the organization, which includes the needs of the reader of an opinion expressed. If the CAE does not know what type of opinion is required or what the opinion is to be used for, he or she should raise the issue with the key stakeholders, educating them on the different types of opinions possible, the effort required to express these opinions, and their relative value to the stakeholders. The results of that discussion should clarify the opinion needed from the CAE. If the readers of audit reports typically do not understand the

different types of audit opinions, an explanation could be provided as an attachment to the audit report or by reference to policy statements of the internal audit activity.

Q. Why do I need to deal with the bureaucracy of something like the COSO framework? If I audit payroll, everyone knows what I audited.

A. Internal controls can include financial reporting, operational, and compliance objectives and involve a range of elements from detailed control activities to the tone at the top of an organization. The COSO framework was created in part because the context of a discussion regarding internal controls is not always that clear. In the example of a payroll audit, using the COSO framework clarifies whether the audit covered items such as:

- Risk assessment activities, including management's process for assessing the likelihood of the risk of fraudulent employees, errors in pension accounting, loss of confidential data, etc.
- Compliance with regulations regarding data privacy in all jurisdictions.
- Efficiency of handling employee-initiated changes in benefit plans elections.
- Sufficiency of training of payroll clerks.
- Adequacy of communications with employees.

A proper definition of the scope of the audit in terms of a framework like COSO would clarify these types of questions.

Q. When would a negative assurance opinion be appropriate?

A. A negative assurance opinion is used when the auditor does not take responsibility for the sufficiency of the audit scope and procedures to find all concerns or issues. This is a lower level of assurance than a positive assurance opinion and should only be used when a lower level of assurance accomplishes the needs of the reader. Situations where a negative assurance opinion may be appropriate include:

— Work is being performed on a rotation basis across many audit units with the scope of the work performed based on work in multiple audit units. In this case, a negative assurance opinion may be appropriate on the individual units. However, the combination of the evidence from all the units may be sufficient to express a positive assurance opinion on the group of units.

— Resources devoted to the audit were limited such that the amount of audit evidence required to support a positive assurance opinion was not obtained. In this case, the negative assurance opinion should clearly state the extent of work performed.

Q. Don't "unsatisfactory" opinions require less audit evidence than "satisfactory" opinions?

A. It may be true that an internal auditor will be able to quickly, and with little effort, establish that internal controls do not meet a defined or expected level of effectiveness. In this case, expressing an "unsatisfactory" opinion may not require a large amount of audit evidence. However, in some cases, it may not be clear whether the internal controls meet or fall short of the threshold required for "satisfactory." The CAE must ensure that, with whatever opinion is expressed, sufficient audit evidence was collected to fully support that opinion.

Q. Do all opinions need to be written? What about oral opinions?

A. The substance of an opinion is the same whether it is written or oral. The concerns discussed above are as applicable to oral opinions as they are to written opinions. Internal auditors should be cautious when using only oral opinions. Oral opinions are more subject to misinterpretation, are less reliably communicated to other parties, and are subject to differences in recollection at a later time. If oral opinions are used, documentation of the opinion expressed would normally be desirable in the internal audit files.

Q. I perform audits of almost all of the transactional processes in an entity in my organization. Based on this work, can I express an opinion on the internal controls of the entity as a whole?

A. The audit work on the processes within the entity provides an excellent foundation for an overall audit opinion. However, this work alone may not be enough to provide the overall opinion. For most entities, aspects of internal controls like the control environment, risk assessment, information flows and monitoring are not performed solely within the transactional processes, but also operate separately at the entity level. An overall opinion of the entity would need to include audit work on these entity-level controls.

Q. Do internal controls need to meet some level defined by COSO to be adequate? Where does cost come into play when deciding whether internal controls are adequate?

A. In most cases, internal controls are not expected to eliminate all risk of error or problems. Internal controls are expected to reduce risk to a level justified when considering the cost of the control versus the benefit from the risk reduction. These concepts are all involved in the auditor's judgment as to whether or not internal controls are satisfactory. The CAE must clearly understand the risks of an organization in assessing the adequacy of internal controls. Because risks, and the cost of controls, differ by organization, no pre-defined level of controls can be applied across all organizations. COSO does not establish any defined level of control in an organization; it only provides the framework to make that evaluation.

Q. An external party wants an opinion from internal auditing on compliance with certain terms of the contract my organization has with that third party. Can I express an opinion in this situation?

A. It does not sound like this is an audit of internal controls, but an audit of compliance with a contract. Most internal auditors would have the competency to perform this

work. However, there are important concerns to keep in mind when deciding whether to express this opinion to an external party:

- Is the opinion clear as to the work performed, the scope of the opinion, and time period to which it applies?
- Is the wording of the opinion consistent with the level of assurance the audit evidence provides?
- Does performance of this type of work fall within the scope of the internal audit activity as described in the approved charter?
- Has legal counsel been appropriately engaged to ensure expression of this opinion does not subject the organization to improper legal exposure? Practice Advisory 2400-1 gives guidance in this respect.

Q. Will I be subject to criminal or civil liability if it turns out the opinion I expressed is wrong?

A. The *Standards* delineate basic principles that represent the practice of internal auditing, provide a framework for performing these activities, establish a basis for evaluating the performance of internal audit activities, and foster continuous improvement in internal audit activities. The *Standards* do not establish or define legal liability or the lack of such liability. This is determined by the laws and regulations in the country of the internal auditor.

Related Standards and Practice Advisories

2410.A1	Final communication of engagement results, where appropriate, contain the internal auditor's overall opinion and or conclusions.
2410.A3	When releasing engagement results to parties outside the organization, the communication should include limitations on distribution and use of results.

2120.A1 Based on the results of the risk assessment, the internal audit activity should evaluate the adequacy and effectiveness of controls encompassing the organization's governance, operations, and information systems. This should include:

- Reliability and integrity of financial and operational information.
- Effectiveness and efficiency of operations.
- Safeguarding of assets.
- Compliance with laws, regulations, and contracts.

2420 Communications should be accurate, objective, clear, concise, constructive, complete, and timely.

Practice Advisory 2060-2 Relationship with the Audit Committee, covers the internal auditor's interactions with the audit committee.

Practice Advisory 2120.A1-1 Assessing and Reporting on Control Processes, discusses the evidence needed to assess a system of internal controls and form an opinion.

Practice Advisory 2120.A1-3 The Internal Auditor's Role in Quarterly Financial Reporting, Disclosures, and Management Certifications, provides guidance on the requirements of Sarbanes-Oxley and related SEC rules.

Practice Advisory 2400-1 Legal Considerations in Communicating Results, gives cautions regarding the degree of assurance and the associated liabilities, focusing on U.S. law.

Practice Advisory 2410-1 Communication Criteria

Practice Advisory 2420-1 Quality of Communications.

Additional Resources:

1. Committee of Sponsoring Organizations of the Treadway Commission's (COSO) Internal Control - Integrated Framework (IC-IF).
2. Committee of Sponsoring Organizations of the Treadway Commission's (COSO) Enterprise Risk Management – Integrated Framework (ERM-IF).
3. A Framework for Internal Auditing's Entity-wide Opinion on Internal Control.
4. Internal Auditing's Role in Section 302 and 404 of the U.S. Sarbanes-Oxley Act of 2002.

IIA Guidance Web Page: http: //www.theiia.org/guidance