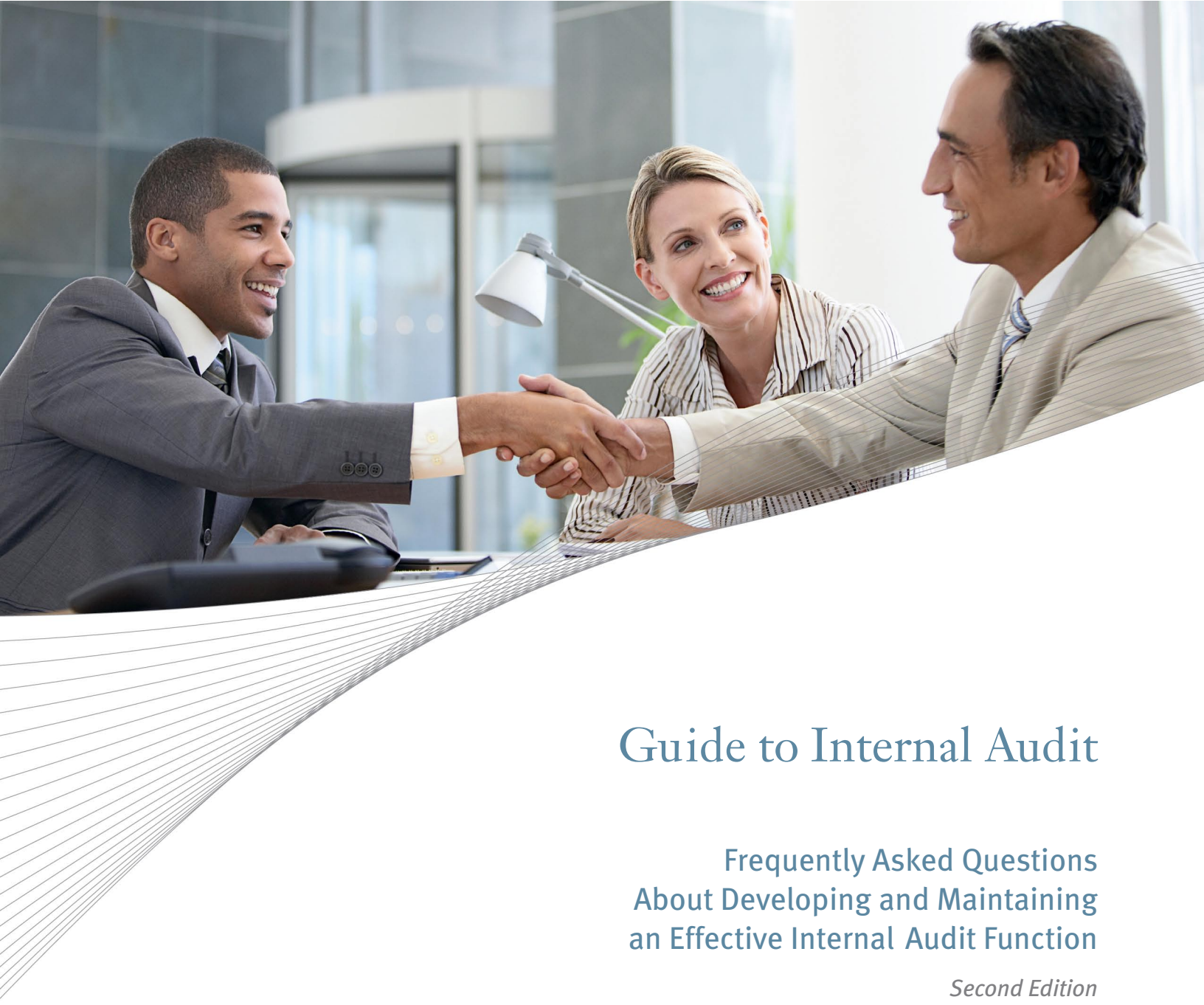


Guide to Internal Audit

Frequently Asked Questions About Developing and Maintaining an Effective Internal Audit Function

Second Edition

protiviti®
Risk & Business Consulting.
Internal Audit.

Powerful Insights. Proven Delivery.™

Table of Contents

* Indicates new or substantially revised material (in comparison to the first edition of this resource guide)

* Indicates new or substantially revised material (in comparison to the first edition of this resource guide)

* Indicates new or substantially revised material (in comparison to the first edition of this resource guide)

Introduction

"Management is doing things right; leadership is doing the right things."
–Peter Drucker

The internal audit (IA) profession has undergone remarkable growth since 2004, when we published the first edition of our *Guide to Internal Audit*. At that time, we determined guidance was needed to address a number of pivotal regulatory developments, most notably the revised listing requirements from the New York Stock Exchange (NYSE) that stated for the first time, "Every listed company must have an internal audit function."

Five years later, companies are far more likely to have in place highly developed IA functions that address not only the NYSE standards, but also the SEC's interpretive guidance on Section 404 of the Sarbanes-Oxley Act and PCAOB Auditing Standard No. 5 (AS5), *An Audit of Internal Control Over Financial Reporting That Is Integrated With an Audit of Financial Statements*, both of which were finalized in 2007. These regulatory developments have had a significant impact on internal audit functions. Given these and other changes, as well as the many lessons learned since the enactment of Sarbanes-Oxley in 2002, we decided our clients and the business community could benefit from a second edition of our resource guide of frequently asked questions about the practice of internal auditing.

Guide to Internal Audit is designed to be a helpful and easy-to-access resource that IA professionals can refer to regularly in their jobs. The publication offers detailed insights into everything from building an IA function to managing and improving the function as the organization evolves. To facilitate the location of topics of most interest to our readers, the questions are divided into eight sections. In the table of contents, new and significantly revised questions from the first edition are noted with an asterisk. Many of these new questions focus on Sarbanes-Oxley best practices and the ever-expanding role of IA functions.

As can be seen in our new questions and responses, the requirements – and some might say burden – of Sarbanes-Oxley compliance have eased over the past few years. Companies have developed best practices gained from hard-earned experience – and consequently, have greater confidence than before to adopt such practices. And as a result, costs for Sarbanes-Oxley compliance have begun to fall. According to a recent survey by the Financial Executives International (FEI), Section 404 auditing costs have dropped by 5.4 percent. This is in line with Protiviti's 2008 rebalancing survey findings,[1] which found that both the SEC's interpretive guidance on Section 404 and PCAOB AS5 are having their desired effects of making Sarbanes-Oxley compliance easier and more cost-effective for organizations – enabling them to devote more of their time to more traditional and broader internal auditing responsibilities.

The IA profession has undergone significant changes since the NYSE issued its new listing standard requiring an internal audit function, and it is likely the landscape will be different in another four years. At Protiviti, we look forward to assisting organizations and their internal audit functions in addressing the current landscape along with the many changes that undoubtedly lie ahead. We hope this resource guide proves beneficial as part of your efforts to enhance your internal audit processes for the betterment of your business.

Protiviti Inc.
January 2009

[1] *Moving Internal Audit Back into Balance*, available at **www.protiviti.com**

Acknowledgements

Protiviti wishes to thank The Institute of Internal Auditors both for providing material for this resource guide and for ably leading the IA profession through the evolving landscape.

The Internal Audit Profession

1. What is internal auditing?

The internal audit profession, through The Institute of Internal Auditors (IIA), has continued to redefine itself as business risk and organizational complexity have evolved. Prior to June 1999, The IIA defined internal auditing as follows:

> Internal auditing is an independent appraisal function established within an organization to examine and evaluate its activities as a service to the organization. The objective of internal auditing is to assist members of the organization in the effective discharge of their responsibilities. To this end, internal auditing furnishes them with analyses, appraisals, recommendations, counsel and information concerning the activities reviewed. The audit objective includes promoting effective control at reasonable cost.

Today, The IIA uses the following definition:

> 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 new definition is part of the *Professional Practices Framework* currently projected to be revised and reissued in 2009. Adherence to *The Professional Practice of Internal Auditing* (The IIA *Standards*) includes following this definition. Companies may choose to develop their own definition to best meet their needs. There is no regulatory requirement on how a company must define internal auditing. However, The IIA definition is generally accepted, and the U.S. Securities and Exchange Commission (SEC), New York Stock Exchange (NYSE) and other regulatory bodies may reasonably be expected to accept and adopt The IIA's definition of internal auditing.

Note: The IIA promulgates internal audit standards and practice advisories. Effective January 2004, The IIA's Internal Auditing Standards Board (IASB) is responsible for revising and updating The IIA *Standards*. The IIA *Standards* are updated to reflect current risk management and governance requirements. Ongoing updates incorporate numerous comments on issues received through a worldwide solicitation and public exposure process, upon which the IASB approves The IIA *Standards* for implementation.

2. How is the internal audit profession regulated?

The internal audit profession presently is not regulated by the SEC, Public Company Accounting Oversight Board (PCAOB) or any U.S. government agency. The IIA is the self-governing professional body that includes the IASB, which is charged with evaluating and developing practice standards that are issued in draft form and subject to a public comment period, much like other professional standards and accounting pronouncements.

The IIA *Standards* includes a code of ethics that members must follow or face disciplinary action, including expulsion. (See Question 5 and Appendix E.)

3. Is continuing professional education (CPE) required for internal auditors?

Yes, practicing internal auditors who hold the Certified Internal Auditor® (CIA®) designation must complete and report 80 CPE hours every two years. The CIA is issued by The IIA to individuals who pass a comprehensive examination and meet educational, experience and character requirements. In addition, many internal auditors are Certified Public Accountants (CPAs) or Chartered Accountants (CAs), designations that also require a minimum of 20 related CPE units per two-year period to maintain public accountancy certification (this may vary among boards of accountancy). Because internal auditors may hold multiple certifications, such as the Certified Information Systems Auditor (CISA), Certified Fraud Examiner (CFE) and other specialized certifications, it is not uncommon for CPE credits to count toward several closely related certification programs. (Individuals holding such certifications should consult the respective certification body for exact CPE requirements.)

CIAs are expected to maintain the high standards of the internal audit profession by selecting quality educational programs to fulfill the CPE requirements.

4. Are internal auditors required to be certified?

No. However, The IIA *Standards* require technical competence and training that can be demonstrated by various certifications, depending upon expertise and professional experience. The IIA also sponsors several additional certifications beyond the CIA, such as:

CFSA® – Certified Financial Services Auditor

CCSA® – Certification in Control Self-Assessment

CGAP®– Certified Government Auditing Professional

Additional internal audit-related certifications supported by other independent professional organizations include:

CISA – Certified Information Systems Auditor

CFE – Certified Fraud Examiner

In addition, the valuable CPA certification is recognized separately by each state. The CA designation, also valuable, is regulated by individual countries. For more information, see Question 3 and Appendix F.

Effective internal audit functions require most existing professionals and new hires to obtain and then maintain at least one certification, including but not limited to the CPA, CA, CIA, CISA and CFE. All certifications require annual CPE training. Skill sets, experience and industry familiarity are crucial in order to exhibit competence, identify and address risks appropriately, and perform in a manner that provides value to the organization.

Strong internal auditors bring together various skills, ranging from specialized industry and technical knowledge to seasoned business acumen that includes advanced degrees in business administration, finance and even law. It is not uncommon for internal auditors to possess professional designations from other disciplines beyond accounting. After all, internal audit functions examine all aspects of a business entity – a key challenge in today's complex business climate.

Therefore, while not required or mandated specifically, it is considered best practice for internal auditors to possess and maintain professional certifications applicable to their focus and responsibilities.

5. Are there professional standards that govern the practice of internal auditing?

Yes. The IIA promulgates the *Professional Practices Framework*, which consists of the following categories of guidance: the *Standards* and *Code of Ethics*, Practice Advisories, and Position Papers and Practice Guides. The first category (considered mandatory guidance) consists of core materials:

- *Definition of Internal Audit*
- *Code of Ethics*
- *International Standards for the Professional Practice of Internal Auditing*

Mandatory guidance is considered essential for the professional practice of internal auditing. Other elements of the framework are linked to these standards.

The *Standards* and *Code of Ethics* comprise attribute, performance and implementation standards. Attribute and performance standards apply to all internal audit services. Implementation standards apply to specific types of engagements, such as assurance and consulting activities. (See Appendix D for a summary of The IIA *Standards*.) Interpretations are included as part of many standards to provide clarification as to how they should be applied in practice.

While The IIA *Standards* do not have the rule of law, the practice of internal auditing, like other professions, is based upon elements of due professional care and a ruling body that develops standards of practice through a public exposure process. The IASB and adherence to The IIA *Code of Ethics* inculcate these standards into internal audit professional practices.

For more information, visit www.theiia.org.

6. Are internal audit functions required to follow The IIA *Standards*?

For CIAs, The IIA *Code of Ethics* requires adherence to The IIA *Standards.* Practice professionals usually look to the Practice Advisories for The IIA's recommendations on matters related to situations that are not covered directly. Concepts of due professional care permeate all practice activity, and apparent violations are investigated by The IIA.

7. What are The IIA Practice Advisories?

Practice Advisories (formerly referred to as Guidelines) provide additional guidance on certain topics and issues. These advisories are not mandatory. They may have a limited life or may be elevated to a *Standards* level based upon importance, usage and acceptance. In part, Practice Advisories help auditors interpret The IIA *Standards* and apply *Standards* to specific internal auditing situations.

Although some Practice Advisories may be applicable to all internal auditors, others may be developed to meet the needs of a specific industry, a specific audit specialty or a specific geographic area, including guidance on topics such as environmental issues, control self-assessment, information technology, government auditing, and guidance issued by other standard-setting bodies and adopted by appropriate committees of The IIA.

All Practice Advisories are subjected to a formal review process by The IIA's Professional Issues Committee or other group designated by the organization's Guidance Planning Committee.

(Source: The IIA website, www.theiia.org)

8. What jurisdiction do the SEC and the PCAOB have over internal auditors?

Neither of these regulatory bodies has direct jurisdiction over internal auditors at this time. The PCAOB can influence the nature and extent of internal audit work through the rules it issues about external auditors' reliance on the work of others. For example, on May 24, 2007, the PCAOB issued Auditing Standard No. 5, *An Audit of Internal Control Over Financial Reporting That Is Integrated With an Audit of Financial Statements* (AS5), which described a public accountant's reliance on the work of others, including internal auditors, during audits of internal control over financial reporting (ICFR).

Currently, these regulatory bodies set requirements and monitor compliance of publicly listed U.S. companies and the public accounting profession. The internal audit profession, like the legal profession, continues to be self-regulated by a required public comment process. The IASB promulgates updated professional standards (see Question 1).

9. Can existing employees become internal auditors?

Yes. There is no prohibition against employees of a company becoming internal auditors. A number of companies host a "guest auditor" program whereby employees are assigned to the company's internal audit function for a short duration of time or to assist on one or more specific internal audit-related matters. When transferring existing employees into the internal audit function, companies, management, internal audit function leadership and, when appropriate, audit committees should consider the following questions:

- Does the person have a positive employment record? Has the person performed at a high level in his or her current department or function? If not, why is this employee being considered for a transfer to internal audit?
- Does the employee possess:
  - Balanced assessment abilities, integrity and trustworthiness?
  - Relevant operating and functional experience to be effective?
  - Appropriate educational background to be successful?
  - Objective attitude and professional skepticism?
  - A commitment to competency, technical proficiency, continuing education and ethics as set forth in The IIA *Standards*?

All employees will not necessarily become, nor should they be expected to become, effective internal auditors.

10. What personal qualities, knowledge and skills should internal auditors possess?

Internal auditors should possess and demonstrate through their work, actions and communication a number of traits, including, but not limited to:

- A commitment to and demonstration of competence in the field of internal auditing
- Strong financial and operational background in accounting, IT, regulatory compliance or the industry in which a company operates
- Honesty and integrity
- Strong work ethic and attention to detail

In general, internal auditors should develop and maintain a healthy level of professional skepticism and objectivity to assist in evaluating information and making judgments. Additionally, internal audit professionals should possess exceptional verbal and written communication skills, and be proficient in negotiating and reasoning with a variety of departments and groups over which internal audit may have no formal authority. Finally, personal integrity, professional due diligence and curiosity are important traits for individuals tasked with conducting internal audit work.

Internal auditors also need to acquire and then master new areas of expertise and knowledge of emerging or re-emerging issues. This can be accomplished by attending internal and external training programs. Realizing the internal audit profession is continuously evolving, Protiviti has conducted a series of internal audit capabilities and needs surveys in recent years to provide benchmarks by which internal auditors can measure their knowledge and skills and identify gaps to be addressed. See Appendix J for a list of skills and knowledge used in this internal audit benchmarking study.

11. Do internal auditors have to comply with any professional ethics requirements?

Yes. Like most professions, members must adhere to a code of ethics as part of following The IIA *Standards*. In addition, other professional certifications that practitioners may hold typically require adherence to a standard of ethics. (See Question 5 and Appendix E.)

Along with the CIA designation, many internal auditors also hold CPAs, CISAs (IT auditors) or other certifications that require strict adherence to a formal code of ethics, with serious repercussions by an ethics board for violations.

In addition to professional ethics requirements, the organization in which internal auditors are employed may have its own specific code of conduct, rules of behavior and other ethical requirements that internal auditors need to be aware of, must comply with and may at times be responsible for validating compliance with.

12. How much should a company spend on internal audit?

The costs, focus and size of an internal audit function should be tailored to each company's individual needs. In addition, a company's written internal audit charter, approved by the audit committee, will impact the amount of annual internal audit investment. The amount invested should depend on the level and complexity of risks a company faces, its industry profile and the responsibilities given to the internal audit function.

This is supported by a 2007 study sponsored by Corporate Executive Board's Audit Director Roundtable®. Data from this study (shown below) indicates that internal audit budgets are correlated positively both to company size (as measured by revenue) and complexity. However, it is not a linear relationship.

Revenue Range	Budget as a Percentage of Company Revenue		
(Billions of USD)	First Quartile	Median	Third Quartile
‹$1B	.08%	.13%	.19%
$1B - $2B	.07%	.11%	.19%
$2B - $3B	.05%	.07%	.10%
$3B - $5B	.04%	.07%	.09%
$5B - $10B	.03%	.04%	.06%
$10B - $20B	.02%	.03%	.06%
›$20B	.02%	.03%	.05%

Corporate Executive Board goes on to state in this study that, "… even within similar revenue brands, there is significant variation [in internal audit budgets] across industries." Internal audit departments that operate in heavily regulated industries "must incorporate regulatory compliance into their processes, and at times, must audit at least two separate sets of books (statutory and accounting)."

The third edition of *Moving Internal Audit Back into Balance*,[2] which reviews the results of Protiviti's Internal Audit Rebalancing study, also supports the philosophy of matching these budgets to company risk profiles and internal audit responsibilities. In this study, more than half of the respondents said they expect no change in their internal audit budgets in the near future, as many of them are experiencing at least a moderate decrease in the amount of internal audit hours spent on Sarbanes-Oxley compliance. This is allowing internal audit to focus more of its time and budget on other areas of the COSO model rather than just Sarbanes-Oxley-related activities.

The IIA also has identified, through its annual Global Audit Information Network (GAIN) reports, a general range of internal audit expenditures from companies in many different industries and of varying sizes. These well-established practices and benchmarks tracked by The IIA provide average internal audit costs based upon revenue, although these often vary by industry. As mentioned above, these costs should be driven by the risk and complexity of the overall business environment, including potential exposures to business failure.

The GAIN estimations provide a general guideline for internal audit expenditures. Keep in mind that these estimates represent average internal audit costs of in-house resources. Depending on the strategy, risks and scope of the internal audit work, it is not uncommon for costs to fluctuate based upon significant events or changes that expose an organization to additional risks. For more information on the GAIN benchmarks as they relate to internal audit spend, please visit www.theiia.org/research/benchmarking/.

[2]For more information, see Protiviti's *Moving Internal Audit Back into Balance: A Post-Sarbanes-Oxley Survey*, available at **www.protiviti.com**.

13. Are there industry groups for internal auditors?

Yes, there are a number of internal audit groups that have been formed based upon industry affiliation. Their size and degree of formality vary widely. Industries that have formal internal audit organizations include, but are not limited to:

- Banking
- Media
- Gaming
- Pharmaceuticals
- Healthcare
- Colleges and universities
- High technology
- Consumer products
- Energy
- Utilities
- Governmental entities
- Insurance
- Construction
- Hospitality
- Hospitals
- Manufacturing
- Commercial airlines

We recommend that internal auditors seek out these organizations within their industries and become active participants in them. (See Appendix F for a list of other organizations.)

14. Isn't internal auditing a duplication of what external auditors do?

No, not at all. External auditors are hired by and report to a company's audit committee. Their historical objective has been to express an opinion on the fair presentation of the company's financial statements in conformity with generally accepted accounting principles (GAAP). Their audit is completed in accordance with generally accepted auditing standards (GAAS) that were originally established by The American Institute of Certified Public Accountants (AICPA) and are now the responsibility of, and are being updated by, the PCAOB. For public companies and certain other qualifying organizations, external auditors must provide an opinion on a company's ICFR, following AS5, which is now required by Section 404 of the Sarbanes-Oxley Act of 2002.

An easy-to-remember distinction might be that the external auditor is responsible for attesting to accounting reports issued to outside parties and investors, including reporting on ICFR, while an internal auditor is responsible for reviewing inside business practices and internal accounting and process controls.

As noted in Question 1, internal audit is defined by The IIA as an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. Internal auditors may be hired by and report to both management and the audit committee. Internal auditors assist management and the audit committee in identifying and evaluating key business risks, completing focused audits in high-risk areas, completing special investigations for the board and management and, at times, assisting external auditors with parts of their work on the company's financial statements. The scope of internal audit work is determined by the audit committee, management and the internal audit function itself. The standards internal auditors should follow in planning, executing and communicating the results of their work are The IIA *Standards*.

However, both internal and external auditors should collaborate to minimize duplication of effort. Internal and external auditors work in tandem to help management and the audit committee ensure that a company's financial reports and other information are accurate and that its system of internal control is effective (see Question 40).

External auditors may consider and use the work of internal auditors in connection with their integrated audit of the financial statements of a company. Currently, the authoritative literature on this relationship is the AICPA Statement of Auditing Standard 65 (SAS 65). In addition, the external auditor may also use the work of internal auditors in many circumstances in connection with an audit of ICFR, as noted by the PCAOB in Paragraphs 15–19 of AS5. (See Questions 47 and 53.)

15. How is "independence" defined differently for internal auditors and external auditors?

The term "independent" and the concept of independence are often referred to in connection with both internal and external auditors. However, there is a considerably different meaning, degree and context regarding independence for each.

For internal auditors, independence refers to an attitude that is free from bias or undue influence. It also embodies the reporting structure of an internal audit function, which includes reporting to the audit committee and the CEO, in order to allow for an appropriate level of organizational freedom and a lack of restriction in their work and access to records. There are no SEC regulations covering or requiring the independence of internal auditors. Additionally, internal auditors can be employees of the company they serve, whereas external auditors, of course, cannot be.

While The IIA *Standards* use the word "independence" to describe internal auditors in certain places, "objectivity" might be a better word to describe one of the primary characteristics that internal auditors need to exhibit. In fact, that is the word the PCAOB uses when describing the external auditor's evaluation of factors supporting the extent of reliance.

SAS 65 further supports this view and point of differentiation when it explains that, although internal auditors are not independent from the entity, The IIA *Standards* define internal audit as "an independent, objective and consultative activity designed to add value and improve an organization's operations." SAS 65 further states that this concept of "independence" is different from the independence the external auditor must maintain under the AICPA Code of Professional Conduct and SEC regulations. The standard describes how internal auditors maintain "objectivity" with respect to the activity being audited. To further underscore this distinction, the AICPA clarified in SAS 65 that the internal audit function is part of the entity's control environment. The PCAOB has reinforced this point of view.

For external auditors, however, independence is a much more structured and defined term, as well as a regulatory requirement for performance. External auditors are required to be independent under various SEC and AICPA professional standards. Requirements concerning external auditor independence include:

- Strict adherence to reporting directly and solely to the audit committee, including having the audit committee responsible for approving the external audit fees and, in some cases, pre-approving certain types of services to further ensure independence of the external auditor
- Prohibitions on the nature and extent of services that can be provided to an audit client, such as internal audit outsourcing, valuation services, bookkeeping, design of financial systems and other specifically listed services that the SEC has determined would undermine the independence of the external auditor
- Adhering to independence requirements in both appearance and fact
- Not being an advocate for an audit client or having a mutuality of or conflicting interest
- Scope and extent of audit work must be determined by the auditor alone
- Not taking on any responsibilities that could be construed to be those of a management function, and not being in a position of auditing the external auditor's own work
- No direct equity ownership in an audit client
- Required rotation of certain personnel on audit engagements
- Prohibitions on audit firm personnel at certain levels being hired by the companies they audit for a period of time after they cease to provide services to those companies

Also, under GAAS, external auditors are required to confirm their independence in writing to the audit committee of the companies they audit. Penalties can be levied against external auditors by the SEC and AICPA for violations of independence rules. The SEC also can require the financial statements to be re-audited for any period for which it determines that an audit firm was not independent while performing an audit of those statements.

16. What role and responsibility do internal auditors have for fraud?

The IIA Standard 1210.A2 regarding assurance engagements in internal auditor's work with respect to fraud states:

> Internal auditors must have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization, but are not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud.

The related Practice Advisory 1210.A2-1 goes on to state:

> Internal auditors are responsible for assisting companies [to] prevent fraud by examining and evaluating the adequacy and effectiveness of their internal controls' system, commensurate with the extent of a potential exposure within the organization. When meeting their responsibilities, internal auditors should consider the following elements:
>
> 1. **Control environment.** Assess aspects of the control environment, conduct proactive fraud audits and investigations, communicate results of fraud audits and provide support for remediation efforts. In some cases, internal auditors also may own the whistleblower hotline.
> 2. **Fraud risk assessment.** Evaluate management's fraud risk assessment, in particular, their processes for identifying, assessing, and testing potential fraud and misconduct schemes and scenarios, including those that could involve suppliers, contractors, and other parties.
> 3. **Control activities.** Assess the design and operating effectiveness of fraud-related controls; ensure that audit plans and programs address residual risk and incorporate fraud audits; evaluate the design of facilities from a fraud or theft perspective; and review proposed changes to laws, regulations, or systems, and their impacts on controls.
> 4. **Information and communication.** Assess the operating effectiveness of information and communication systems and practices, as well as provide support to fraud-related training initiatives.
> 5. **Monitoring.** Assess monitoring activities and related computer software; conduct investigations; support the audit committee's oversight related to control and fraud matters; support the development of fraud indicators; and hire and train employees so they can have the appropriate fraud audit or investigative experience.

It also seems clear from The IIA's definition of internal auditing (see Question 1) that internal audit should play a role in assisting management and the audit committee with fraud-related issues, including the prevention, detection and investigation of fraud as part of "bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes."

Statement on Auditing Standards No. 99, *Consideration of Fraud in a Financial Statement Audit* (SAS 99), updated by the AICPA in July 2007 and effective for audits of financial statements for periods beginning on or after December 15, 2002, is the current standard for external auditors concerning fraud. As part of this standard, "the auditor should evaluate whether entity programs and controls that address identified risks of material misstatement due to fraud have been suitably designed and placed in operation."

Though this standard provides guidance for external auditors in connection with their audits of company financial statements, it also suggests that a company and its management should be involved in or complete the following activities related to fraud:

- Determine key fraud risks at the company.
- Identify programs and controls to prevent and detect fraud, including an appropriate "tone at the top."
- Determine the effectiveness of such programs and controls to detect and prevent fraud.
- Investigate and resolve any reported instances of fraud.

Internal auditors, given their objectivity and role within the organization, can be of substantial assistance to management and the audit committee in meeting their responsibilities under SAS 99 and in matters related to fraud in general.

Additionally, Section 302 of Sarbanes-Oxley requires management to report to the external auditor and the audit committee, at least quarterly, "any fraud, whether material or not, that involves management or other employees who have a significant role in internal control." Again, internal audit logically can play a role in assisting management with investigating such reported instances, some of which may be detected and reported by internal audit. More importantly, internal audit can assist management and the audit committee in implementing processes and controls to prevent fraud in the form of education and orientation programs, enhanced internal controls and more robust fraud monitoring systems.

Companies and their internal auditors may want to access *Management Antifraud Programs and Controls*, a publication jointly developed and issued by The IIA, the Association of Certified Fraud Examiners, Financial Executives International, the AICPA and others.

AS5, in Paragraphs 11, 14 and 15, clearly identifies fraud considerations as an integral part of a company's ICFR. The PCAOB makes it clear that part of management's responsibility when designing a company's ICFR is to design and implement programs and controls to prevent, deter and detect fraud. In this regard, internal audit can be a qualified and logical source to assist management and the audit committee.

17. Are there university programs in internal auditing?

Yes. In fact, the number of formal collegiate internal audit programs is increasing. The IIA's Academic Relations Committee encourages and supports the implementation of internal audit curricula at the collegiate and graduate level worldwide. The IIA endorses programs that meet high-quality standards including faculty, student and program expectations.

A few of the pioneer and well-known programs include:

- Louisiana State University – www.bus.lsu.edu/centers/cia/
- Northern Illinois University – www.cob.niu.edu/
- University of Texas - Dallas – http://som.utdallas.edu/iaep/index.htm
- University of Texas - Austin – www.mccombs.utexas.edu/mpa/
- Universiteit van Amsterdam – www.abs.uva.nl/emia/home.cfm

More than 35 colleges and universities offer programs, concentrations and certificates as part of business degrees, including a doctorate dissertation scholarship program for internal audit studies. See Appendix G for a complete listing.

18. What is the Common Body of Knowledge?

The Common Body of Knowledge (CBOK) 2006 study is the largest project ever undertaken by The IIA Research Foundation. Chief audit executives (CAEs), internal audit practitioners of all levels of experience, and IIA Chapter and Institute leaders were surveyed for CBOK, which targeted the following topics:

- Compliance to and adequacy of The IIA *Standards*
- Current status of the internal audit activity within organizations
- Activities and types of audits being performed
- Tools and techniques used by internal auditors
- Skills and knowledge possessed by internal auditors

The IIA plans to repeat the CBOK study every three years, with the next study scheduled for 2009. The result will be a continuously expanding library of information about the internal audit profession worldwide. By examining how internal auditors are executing their work, CBOK will help The IIA to shape the future of the profession. For further information on CBOK, please visit www.theiia.org.

Starting an Internal Audit Function

19. How do we start an internal audit function?

A suggested set of guidelines for starting an internal audit function includes:

- Clarify expectations with senior management, the board and audit committee, including required listing standards for NYSE companies. Non-NYSE-listed organizations should consider voluntary compliance.
- Develop an audit charter, with audit committee input and approval.
- Consider the appropriate budget and staffing model (e.g., in-house, co-sourced or outsourced). As part of this process, research actions taken by similar companies in your industry.
- Formulate reporting responsibilities of the internal audit function.
- Identify the "universe" of auditable entities within the organization.
- Complete an initial risk assessment with company management and audit committee involvement. Consider using recognized approaches and frameworks for this effort, such as the COSO internal control and COSO enterprise risk management (ERM) frameworks. Other recognized and acceptable frameworks include the King Report on Corporate Governance for South Africa - 2002 (King II Report) and the Turnbull Report in the United Kingdom.
- Consider the results of the work required to comply with Sarbanes-Oxley when conducting the risk assessment.
- Develop an internal audit plan responsive to the risk assessment.
- Determine staffing requirements and whether the department will be staffed internally, co-sourced or outsourced.
- Plan and execute audit work called for in the audit plan, including a system to monitor and follow up on audit recommendations.
- Update the risk assessment for changing circumstances during the year.
- Continuously enhance and modify the internal audit function to meet changing needs of management and the audit committee.

See Appendix C for a listing of 16 steps developed by The IIA for creating an internal audit function.

20. How should an internal audit function be staffed?

Internal audit functions must be resourced adequately to ensure an effective evaluation and testing of internal controls, associated risks and execution of the internal audit plan and other activities as outlined in the company's written internal audit charter. The annual audit plan is based upon a risk assessment at both the entity and process levels, and should be approved by the audit committee and board.

Companies should look to their individual risk profiles to drive staffing decisions. A business facing a significant number of risks or particularly complex risks will require a broader range of specialists and expertise. Most internal audit departments are headed by a CAE and include layers of staff such as managers, senior auditors and auditors. Many companies also rely on other in-house professionals or tap into the specialized skill sets of outside providers.

Some of the more commonly accessed or desired specialized skills needed by today's internal audit function include:

- Relevant industry knowledge
- IT privacy and security
- Current, in-use enterprise resource planning (ERP) application expertise
- Business continuity management
- Specialized and complex industry or other related regulations
- Fraud prevention, detective and investigative capability
- United States GAAP and IFRS knowledge
- Specific business process knowledge in large, material and high-risk areas
- Resources needed in remote locations

21. To whom should the head of internal audit report?

The reporting line of internal audit is a dynamic issue today, especially considering recent corporate scandals and continued financial restatements, the emergence of regulations such as Sarbanes-Oxley and new listing standards of the stock exchanges. All these have substantially increased the responsibilities of the audit committee.

The IIA *Practice Advisory 1110-2*, *Chief Audit Executive (CAE) Reporting Lines*, states, "The chief audit executive should report to a level within the organization that allows the internal audit activity to accomplish its responsibilities." The Practice Advisory goes on to state: "The Institute (IIA) believes strongly that to achieve necessary independence, the CAE should report functionally to the audit committee or its equivalent. For administrative purposes, in most circumstances, the CAE should report directly to the chief executive (CEO) of the organization."

Unlike the company's external audit firm, which by regulation must be hired by, report to and be compensated by the audit committee, internal audit has a broader role to play through serving as a resource for both the audit committee and company management. Though this "dual reporting" is a somewhat sensitive arrangement and can be tricky in practice, it nevertheless provides important benefits to the company as a whole, including its overall corporate governance objectives as well as management's objectives for reliable financial reporting, compliance with applicable laws and regulations, and efficiency and effectiveness of operations (the COSO objectives of internal control).

Until regulations or standards change, internal audit is considered a part of the internal control system of a company, yet must also remain an independent, objective assurance and consulting activity that supports and reports to a company's CEO and audit committee.

22. Can employees in the company participate in internal audits?

Yes. Many companies choose to source management-training programs, employees with specific experience or guest internal auditor programs as part of resource planning. Some organizations have established two- to four-year rotation programs to help management understand the organization's internal control environment and other operational areas, and to provide individuals with management-training experience and career progression.

This type of flexibility and training often enhances organizational understanding of risk management and internal controls systems and motivates program candidates to strive for excellence. Conversely, internal audit management should be aware, in every instance, of the same conflicts of interest that arise naturally from such relationships in considering these candidates for potential positions in operations. For example, there may be a conflict of interest for individuals who join the internal audit department from an existing corporate function that would preclude them from auditing their former colleagues. Other situations include a natural tendency by a rotating internal auditor to hold a favorable bias in evaluating a business unit or function in which he or she may be seeking a full-time position.

23. What are the pros and cons of outsourcing/co-sourcing internal audit?

Up through the 1980s, most company internal audit functions were staffed primarily in-house with full-time, dedicated employees. This structure worked adequately and can still be effective today, but only if full-time internal auditors possess all of the skills needed to address key business risks faced by the organization. If this is not the case, then the internal audit function places its employer company at risk by not being able to address adequately the key risks that it has been asked to audit.

During the 1980s, as the concept of "core competency" gained more attention, companies evaluated many of their business functions and the potential for outsourcing them. Payroll, benefits, real estate, printing, information systems operation and maintenance, and even aspects of design or manufacturing, among other functions, were considered. Many companies found clear and tangible benefits, positive return on investment (ROI), and improved service levels as a result of outsourcing. In some cases, capital expenditures were reduced and the cost of these functions became more variable. Internal audit functions were a part of this analysis, and several new internal audit outsourcing and co-sourcing organizations, including the large accounting firms, created new structures to provide such services.

Today, all businesses, government and not-for-profit organizations face myriad risks due to the dynamic operating climates in which they operate. New and fast-changing regulations; significant technology-related risks such as security, business continuity, and application and data integrity; heightened instances of or opportunities for fraud and abuse; and other issues such as Sarbanes-Oxley require internal audit functions to have at their disposal a larger and deeper talent pool. These professionals must be able to address, react to and effectively audit and report on this more complex and faster-changing risk universe.

Given this dynamic risk environment, it is unlikely that a majority of internal audit functions have the continuous in-house capability to adequately address every risk they and their organizations must face. Thus, contracting, partnering or working with outside organizations that can provide specialized resources improves an internal audit function's ability to address risks and meet customer expectations. Additionally, these co-sourcing arrangements often assist in the knowledge transfer process to in-house resources, raising the level of competency of the function's full-time employees.

Likewise, many companies – especially public companies, large and diverse private companies, and even governmental entities and not-for-profit organizations – may find that full or partial outsourcing of their internal audit functions makes sense, is cost-effective and provides significant short- and long-term benefits.

Benefits of outsourcing include:

- Quick start-up of the function and execution of work, including already-developed methodologies and audit tools provided by the outsourcing organization
- A variable-cost arrangement rather than a fixed-cost function
- Access to a greater number and wider range of resources
- Potentially greater objectivity and independence

The NYSE's internal audit rule allows for the outsourcing of internal audit. In its commentary to the requirement, the NYSE stated, "A company may choose to outsource this function to a third-party service provider other than its independent auditor." Companies should also consider the potential negative impact of outsourcing or co-sourcing internal audit, which can include, but is not limited to, the potential loss of control since resources are not directly employed by the company.

From The IIA's perspective, internal auditing, regardless of who provides the service, should be performed in accordance with The IIA *Standards*. The IIA states in its position paper, *Resourcing Alternatives for the Internal Audit Function*, that a fully resourced and professionally competent staff is an integral part of the organization, whether insourced or outsourced. The IIA recognizes that many "partnering" arrangements with outside providers have been effective in helping organizations obtain internal auditing services to help achieve management's objectives.

While non-NYSE companies are not required to have an internal audit function, certain limitations apply to the nature and level of internal audit services that any public company's external auditor can provide per SEC rules and regulations.

Ultimately, deciding whether to outsource internal audit is not a matter of considering the general pros and cons. Instead, each company should ask:

- If we currently do not have an internal audit function, are we better off taking the time and effort to start our own in-house internal audit function? Or should we initially outsource it to gain quick start-up and access to a greater level of expertise and broader level of resources, and then monitor this decision and delivery model to ensure it is effective?
- If we already have an internal audit function, do we have the resources we need to effectively address all of the key risks we face and in which internal audit should be involved? Do we need to have all of these resources in-house all of the time? Might we be better off considering an arrangement to have one or more outside organizations assist us with addressing our risks?

There are many excellent internal audit functions consisting of primarily in-house, fully dedicated employee resources. What makes these functions most valuable, effective and appropriate, however, is a recognition of their own limitations. Many large internal audit functions (more than 25 full-time employees) recognize that in today's complex business environment, it would be cost-prohibitive to have all of the right resources at hand all of the time. They also understand that various forms of co-sourcing arrangements have benefited them greatly along with the companies, management and audit committees they serve.

Case Study: Co-sourcing

A large multinational corporation with a well-established and historically effective internal audit function realized that though it was well-staffed, new business risks and the need for new audit skills seemed to be surfacing all the time. Revised and complex treasury arrangements, a leading-edge information system, new joint ventures, as well as a just-acquired division in a new industry, were all stressing the department's capabilities. In addition, greater than average turnover of staff had occurred, leaving the department understaffed on a regular basis.

The internal audit director, a 20-year-plus veteran, sensed "there must be a better way." To her, co-sourcing with a firm that could meet specialized as well as just-in-time needs was the answer. Leveraging the co-sourcer's intellectual property and methods also seemed to be a valuable benefit.

After evaluation and selection of a co-sourcing partner, the audit director and her department significantly enhanced their overall capability and effectiveness in dealing with new and complex risk areas as well as auditee customer satisfaction.

Case Study: Complete Outsourcing

A consumer products manufacturing company with a strong forecast for growth and expansion was seeking to create an internal audit function as it reached a certain level of revenues and operational scope. Both management and the audit committee believed the company's situation warranted such a function to assist in the development of a risk assessment and risk management process and to complete focused internal audits as a result of the risk assessment. They also wanted the internal audit function to be able to address unexpected operating and internal control issues, and to assist with preparation for Section 404 of Sarbanes-Oxley.

After considering the options of creating and building a function in-house, hiring selected individuals and then co-sourcing or fully outsourcing the function, the company concluded that fully outsourcing the internal audit function initially made the most sense and provided the best benefits. Flexibility, quick start-up, access to varied skills and resources, as well as the resources, quality and reputation of the outsourcer, were among the reasons supporting this decision. This arrangement allowed the company to have an effective internal audit function almost immediately to help management and the audit committee meet their fiduciary and other responsibilities.

24. Where do I get more information on internal auditing?

The primary information resource on internal auditing is The IIA (see Appendix H). Other sources include consulting companies, various online information portals and universities with related programs.

KnowledgeLeader℠ (**www.knowledgeleader.com**), a subscription-based repository from Protiviti, provides best practice guidance, topical work programs and white papers on internal audit, business risk and technology risk. Thirty-day free trials are available.

See Appendices F, G and H for more information on resources.

The Process of Internal Auditing

25. How is internal audit work actually performed?

Once a company forms an internal audit function, completes the risk assessment process and develops an internal audit plan that is responsive to the risk assessment, it can initiate individual internal audit assignments.

A framework for initiating and executing internal audit projects should include the following actions:

- **Confirm the audit assignment** (e.g., timing, purpose, scope) with the area or process to be audited (in some cases, it may be appropriate to not announce the audit, but to perform the work on a surprise or unannounced basis).
- **Complete appropriate planning** for the audit assignment. This can include the following:
  - Assess the risks of the specific area to be reviewed.
  - Develop a written work program.
  - Agree on scope, locations, sample sizes and period under review.
  - Develop a report format that will be effective.
  - Request and receive certain advance information from the area to be reviewed.
  - Access operating information, performance measures, etc., on the area to be reviewed.
  - Review any prior audits of this area by internal audit or other parties, such as regulators, external auditors and consultants.
  - Hold joint planning discussions with management and process owners of the area to be reviewed to learn their areas of interest and concern.
  - Consider whether self-assessment activities would be helpful.
  - Gather outside information on best practices.
  - Identify the internal audit resources to be assigned to the audit and ensure they have an appropriate level of experience and competency.
  - Determine if outside resources or guest auditors should be utilized, including information technology resources.
  - Consider formal entrance and closing conferences.
- **Execute actual internal audit work,** including evaluation of process and control design, as well as testing methods to determine control operating effectiveness such as inquiry, observation, examination and reperformance. Discuss and clear items noted and potential findings with management and process owners. For consulting engagements, perform agreed-upon work steps to meet the objectives of the assignment.

- **Develop a report** or other appropriate communication method responsive to the work completed and findings made. Areas that might be considered include:

  – Executive summary of major issues and findings

  – Background, objectives and scope

  – Audit findings, including management's action plan for addressing these findings

  – Other analysis and information, including appendices

  The format of internal audit reports varies by company. What is most important is to create an approach that is effective at communicating key issues and achieving positive change and resolution to the issues reported. For example, some companies may find that single-page reports are effective. Others may find that management should respond separately and apart from the audit report itself.

  In addition, the circulation of a draft report for discussion is often an appropriate and effective way to refine wording and ensure the accuracy of all information in the report.

- **Develop an effective method for tracking and following up** on audit findings and agreed-upon actions by management. This may include recording all findings in a database, scheduling follow-up audits or conference calls, or requesting status from the auditee. It may even include having management of the audited area report to senior management and the audit committee. Internal audit should also determine the extent to which resolution of auditing findings should be validated independently.

There is no one-size-fits-all approach to the execution and completion of internal audit work. Internal audit leadership, management and the audit committee should work together to create an approach that is most effective for their respective organizations. The IIA *Standards* and Practice Advisories can also provide guidance and a framework to follow.

26. Should an internal audit function consider information technology risks?

Absolutely. IT general controls and application controls are key and pervasive to the management of risk. The importance of considering information technology risk is supported by The IIA's *General Audit Guide No. 4 - Management of IT Auditing* (GTAG 4), which states:

> **Evaluate IT-related Risk** – It is clear that the evolution of IT introduces new risks into an organization. This guide will help the CAE understand how to best identify and quantify these IT-related risks. Doing so will help ensure that IT audit procedures and resources are focused on the areas that represent the most risk to the organization.

GTAG 4 also states:

> **Emerging Issues** – IT evolves rapidly. This evolution can introduce significant new risks into an organization. The world class CAE focuses IT audit attention on not just the basic building blocks of IT, but also new and emerging technologies. A section on emerging issues will provide specific information on a number of emerging technologies, evaluate the risks that these technologies pose to an organization, and provide recommendations for how the CAE should respond to these risks.

Failing to consider the impact of IT will result in an incomplete and ineffective internal audit function. An internal audit function should be driven by risk, and in today's business, technology has a direct relationship to risk. Technology both enables key controls in the business process or function and brings certain inherent risks. It is critical to understand how technology risks impact the overall risks to the organization. For instance, if a company considers technology a strategic business differentiator for certain business processes, the risk around the applications, technology and components related to those processes becomes more critical to the success of the business.

Technology enables controls such as segregation of duties and limiting the execution of transactions to only those intended by management (through application security and its appropriate administration). In addition, technology provides critical controls through the programmed logic in the applications, which validates transactions, performs appropriate calculations accurately and completely, and handles error and reasonableness checks.

The inherent risks around technology include the security of the company's network and data, computer networks and related data, which are subject to internal and external risks from hackers, disgruntled employees, corporate espionage and individuals who may want to disrupt the business or learn its secrets.

As highlighted in GTAG 4, technology risks evolve on an ongoing basis. New control challenges such as Wi-Fi, remote access and global networks present an ever-changing and dynamic risk profile. Therefore, IT is an integral part of any internal audit function's focus and capability. Generally speaking, all internal audit functions should have a measurable part of their activities concentrated on IT-related risks and issues. These activities should include stand-alone initiatives and initiatives that integrate technology risks and controls into the business process audit work. In certain instances, the entire business process may be automated and the business process audit is therefore related entirely to the technology involved. Coordinating these efforts with a company's CIO organization is critical.

Effective compliance with Section 404 also requires various documentation and evaluation efforts at both the general and application control levels, further underscoring the need for an appropriate IT capability within internal audit functions.

Given the breadth and rapid change of technology and its related risks, internal audit functions should consider what outside resources, if any, are needed to supplement their own skill bases in this area. In some cases, it may be prudent to avoid increasing full-time staff levels for certain forms of IT risks and issues, and instead rely on outside resources for recurring assistance.

27. What types of IT audit skills should be included in an internal audit department?

While specific skills required for IT audit may differ by industry and an entity's applications, there are a number of technology skills customarily needed for an IT audit department. As technology continues to evolve and become more interwoven with business processes, the skills of the auditor must evolve and change as well. We have defined a number of specific skills that may be required to complete an IT audit plan. These include:

- **IT risk assessment and planning** – At most organizations, performing an IT risk assessment requires a distinct set of skills. Risk assessment is an art, not a science, and the better one's understanding of how technology and business risks interrelate, the more on-target the risk assessment and audit plan will be. Effective IT audit planning requires knowledge of both internal auditing and technology risks.
- **IT governance and management** – Organizations are struggling to understand all that IT governance entails, and skills in this area are evolving quickly; they include IT portfolio management, return on investment considerations, issues around IT alignment and service to the organization.
- **Security and privacy skills** – The knowledge needed to audit and understand the security and privacy areas is complex and changing rapidly. A number of regulations impact security and privacy, including the Gramm-Leach-Bliley Act, HIPAA and Sarbanes-Oxley. One of the most important areas to many companies is around Payment Card Industry (PCI) credit card security standards and how personal information and data are handled and used.
- **Enterprise application controls – security and configuration skills** – Knowledge of how IT applications function is critical. Critical programmed controls include data validation and error-checking routines, reasonableness checks around certain key processing points, logical segregation of duties, and limitations on who can initiate and view transactions. In today's large ERP applications, these controls are a critical part of the configuration of the application. Skills are needed around how these programmed controls and configurations interact with the manual procedures. Industry-specific application skills also are needed.
- **Technology infrastructure components and configurations** – This area includes knowledge of critical technology infrastructure, such as networks, databases and platforms. A number of these skills relate to complex security and configuration requirements. In addition, there are needs around specific operational aspects for the technologies, such as backup, recovery and performance issues.
- **IT process skills** – A number of process skills are needed to audit IT processes. These include security administration in the application and technical component areas, business continuity and disaster-recovery planning, data center operations, application change management, infrastructure change management, and asset and service management.

- **Information strategy, data and records management** – Data is becoming more and more independent of applications. Data shared between applications must be owned and managed. Data management issues surround e-discovery and records retention requirements, as well as other key legal issues. A growing number of skills are needed to adequately address these areas at most organizations.

All internal auditors should have a base-level capability related to IT risks and controls. In many cases, deeper specialties are needed in specific applications, ERP systems and other areas discussed above. In a number of cases, organizations choose to develop an IT specialty practice within their internal audit department, given the magnitude and recurring nature of certain IT-related issues and risks.

Internal audit functions should evaluate the depth, breadth and frequency of their IT audit resource needs, and consider when and how external resources and organizations can be of assistance to achieve the best balance of people and skills.

28. What should we look for in an internal audit report?

A well-written internal audit report is a highly effective tool for management, the audit committee and the process owners affected by the report to bring about positive change and to improve controls, accuracy of information and the underlying process reviewed.

The audit report should consider the following questions:

Objective and background – Why was the area selected for audit? Was it due to inherent or perceived high risk, known problems, history of past issues, a management change, materiality of the area or other factors? What are the key aspects, risks and objectives of the area reviewed? Was it part of the original plan arising from the risk-assessment process?

Scope – What was the scope of the work and when was it performed? What time period and business units did it cover, and which facets of operations were included? What key risks did the work try to address?

Findings – What were the overall findings? How severe were they? Are there only minor issues to be addressed, or are there significant deficiencies in internal controls or the process being reviewed?

Recommendations – What actions must management take to adequately address the audit findings?

Management action plans – Is there a clear plan to correct the deficiencies noted? Who will take responsibility for the corrective action? When will the issues be corrected?

Follow-up and tracking – How is internal audit monitoring management's progress in addressing noted deficiencies? Quarterly and annual internal audit reporting to the audit committee should include tracking and confirmed resolution of management action plans resulting from audit findings. One measure of an internal audit function's effectiveness is the ability to foster positive and agreed-upon changes in the organization that produce an improvement and enhanced awareness of the management internal control structure.

See Question 25 for additional information on internal audit reports.

29. What is control self-assessment (CSA)?

CSA is a process through which internal control effectiveness is examined and assessed. The objective is to provide reasonable assurance by those doing the work that all business objectives will be met.

The responsibility for the process is shared among all employees in an organization. CSA is conducted within a structured environment in which the process is thoroughly documented and, as an incentive for continuous improvement, is repeatable. The CSA process allows management and work teams directly responsible for a business function to:

- Participate in the assessment of internal control.
- Evaluate risk.
- Develop action plans to address identified weaknesses.
- Assess the likelihood of achieving business objectives.

The IIA believes CSA generates information on internal control that is useful to management and internal auditors in judging the quality of control. It can also positively influence the control environment. As operating staff buy into the process, control consciousness increases.

30. Is there a standard definition for internal controls?

Yes. The following definition is provided by the COSO Internal Control – Integrated Framework. The SEC and PCAOB have acknowledged that the COSO framework is a suitable framework for purposes of evaluating internal control. Outside the United States there are other recognized and acceptable internal control frameworks that also include definitions for internal control and other suggested objectives.

Internal control is a process effected by an entity's board of directors, management and other personnel. It should provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

Key Concepts

- Internal control is a *process*. It is a means to an end, not an end in itself.
- Internal control is effected by *people*. It is not merely policy manuals and forms, but people at every level of an organization.
- Internal control can be expected to provide only *reasonable assurance*, not absolute assurance, to an entity's management and board.

Internal control is geared to the achievement of objectives in one or more separate but overlapping categories. Internal control consists of five interrelated components. These are derived from the way management runs a business and are integrated with the management process. Although the components apply to all entities, small and midsize companies may implement them differently than large ones (smaller companies' controls may be less formal and structured). The components are:

- **Control Environment** – Sets the tone of an organization, influencing the control consciousness of its people. This is the foundation for all other components of internal control, providing discipline and structure.
- **Risk Assessment** – This component is the entity's identification and analysis of relevant risks to the achievement of its objectives, forming a basis for determining how the risks should be managed.
- **Control Activities** – Includes the policies and procedures that help ensure management directives are carried out.
- **Information and Communication** – This component consists of processes and systems that support the identification, capture and exchange of information in a form and time frame that enable people to carry out their responsibilities.
- **Monitoring** – Consists of the processes that assess the quality of internal control performance over time.

31. How does the COSO internal control framework relate to internal auditing?

The COSO Internal Control – Integrated Framework impacts internal auditing in two important ways. First, it provides a context for the internal auditing activity by including it as part of the "Monitoring" component of the framework. COSO states that internal auditing is a periodic monitoring technique. Second, the framework provides a foundation on which to plan, execute and report on the results of the internal audit plan. The framework:

- Provides authoritative criteria for documenting, evaluating, testing and improving internal control.
- Supports training of internal auditors, management and process owners as to the components and attributes of internal control.

- Facilitates the articulation of the scope of the internal audit plan.
- Provides a common language for use during presentations at all levels of the organization.
- Provides a stepping-stone for implementing the COSO ERM framework released in September 2004.

Now that COSO is recognized as the framework of choice for purposes of management complying with Section 404 of Sarbanes-Oxley, most internal auditors are likely to adopt it for their use. Many internal audit departments already have adopted COSO and have found it to be an effective internal control model.

32. Are internal auditors required to follow COSO?

No. However, because the SEC and PCAOB recognize the COSO framework as suitable and available for management's assessment of ICFR, as required by Section 404, the PCAOB based its performance and reporting directives in its internal control auditing standard on the framework. Further, the COSO framework has clearly emerged as the framework of choice in the United States.

Though not required to be followed by internal auditors for their internal audit work, COSO's widespread recognition as the preferred Section 404 framework suggests that adopting COSO as the standard for internal audit work related to internal control is appropriate. As one of the founding COSO members, The IIA strongly supports COSO as a preferred internal control framework.

Outside of the United States, other similar control models have been developed and adopted. These include:

- CoCo (Canada) – The Criteria of Control Board of the Canadian Institute of Chartered Accountants (CICA) issued Guidance on Control in 1995, a framework for making judgments about control. There are large areas of overlap and consistency between COSO and CoCo, although they differ in some respects.
- The Turnbull/Cadbury Report (England) – Also called the *Combined Code of Corporate Governance*. Calls for companies to embed risk management and risk controls within the organization.
- KonTraG (Germany) – Act on Control and Transparency in the Corporate Sector provided corporate governance reform.
- King Report on Corporate Governance for South Africa – 2002 (King II Report – South Africa) – The Institute of Directors and the King Committee on Corporate Governance issued this report to promote high corporate governance standards in South Africa.

33. What is the COSO ERM framework and what is its relevance to internal auditing?

Following the development of the COSO Internal Control – Integrated Framework, COSO released the enterprise risk management framework in September 2004. The ERM project was initiated to develop a conceptually sound framework providing integrated principles, common terminology and practical implementation guidance supporting a company's programs to develop or benchmark its enterprise risk management processes.

As set forth in the executive summary of the COSO ERM framework, every entity, whether for-profit, not-for-profit or a governmental body, exists to provide value for its stakeholders. All entities face uncertainty; the challenge for management is to determine how much uncertainty the entity is prepared to accept as it strives to grow stakeholder value. ERM provides a framework for management to effectively deal with uncertainty and associated risk and opportunity, and thereby enhance its capacity to build value.

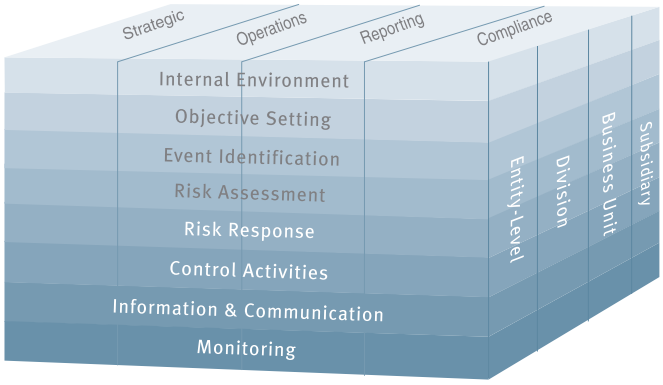
The COSO ERM framework bolsters, supports and extends aspects of the original COSO internal control framework. The framework is based on eight key components:

- Internal environment
- Objective setting
- Event identification
- Risk assessment

- Risk response
- Control activities
- Information and communication
- Monitoring

Also included in the conceptual approach is a mandate for coordination of all of these components in order to achieve the maximum effectiveness of a company's risk assessment process.

Similar to the COSO Internal Control – Integrated Framework, the COSO ERM framework is depicted in a cube-like fashion.



Thus, in terms of relevance, since COSO is the current definitive standard for internal control, the COSO ERM framework is seen as a definitive standard as it relates to risk assessment. As internal audit functions complete their risk assessment processes, they should look to the COSO ERM framework as a possible approach to complete this activity.

The IIA, a member of COSO and a participant in the development of the COSO ERM framework, supports its use by internal auditors. This framework provides a benchmark with detailed guidance for internal auditors to use in the evaluation of their organization's risk management efforts. It also suggests guidance on various risk management processes and tools to consider when implementing or strengthening an organization's ERM process.

COSO comprises the following organizations:

- American Institute of Certified Public Accountants (AICPA)
- American Accounting Association (AAA)
- Financial Executives International (FEI)
- The Institute of Internal Auditors (The IIA)
- Institute of Management Accountants (IMA)

The framework can be found at www.erm.coso.org.

34. Are there specific performance measures for internal auditing?

Like any function or process within an organization, appropriately developed performance measures help to drive results, performance, quality and continuous improvement. Internal audit should also have its own set of performance measures or key performance indicators.

Example performance measures for internal audit could include:

Quality

- Customer/process-owner satisfaction scores from auditees
- Audit committee and management evaluation scores
- External audit evaluation score from company's external auditor
- Upward feedback scores on CAE and internal audit managers from internal audit staff
- Percentage of internal audit staff with CIA or other relevant certifications
- Performance evaluation scores on internal audit staff
- Control breakdowns/deficiencies in areas recently reviewed by internal audit
- Internal control scorecard results by major area within the company
- Results of internal and independent quality assessment reviews

Cost

- Percentage of fully loaded internal audit cost as a percentage of company revenues and assets
- Actual cost per internal audit report and average
- Average cost per internal auditor
- Cost per audit hour in total
- Cost per audit hour based upon actual audit work only, excluding administration
- Travel costs of the internal audit function and average cost per trip
- Training cost and training cost per auditor
- Technology licensing costs and other outside costs
- Costs related to use of outside resources

Timeliness

- Report cycle time from completion of fieldwork to issuance and finalization of report
- Budgeted hours versus actual hours by individual audit
- Percentage of audits called for in the audit plan that are not yet complete
- Unresolved/incomplete recommendations from prior audit reports
- Average length of audit assignment in person hours or weeks
- Major risk areas not audited in the last year
- Aging/status of open, unresolved audit findings (especially those beyond their due date)

Other

- Degree of reliance on internal audit work by external auditor
- Turnover rates
- Percentage change rate in the annual audit plan
- Percentage of assets, revenues, locations, business units, etc., covered by the internal audit plan
- Linkage of key risks to specific skills of the internal audit team
- Degree of IT-related audit work relative to total audit effort

A selected number (approximately six to 12) of key performance measures should be agreed upon between internal audit, the audit committee and management. Having too many measures is not productive in the long run, nor is utilizing too few. Also, a balanced scorecard of measurements focusing on cost, quality and timeliness will help to drive the most effective result for a company. Of course, companies should develop their own specific measures that best meet their needs.

Reporting of these measurements at least annually is appropriate in some cases. However, certain measurements might be reported at each audit committee meeting or more frequently than once a year.

35. Should internal audit departments consider using an automated work paper software package?

Yes. Automated work paper software packages are becoming best practice. They provide an organized, efficient approach to completing and documenting internal audits. The software often allows team members to share and review work papers at any time or at any stage of the audit process. The automated tool can also be used to boost efficiency and serve as a capacity multiplier for understaffed departments. Other benefits of using work paper software packages include:

- Creates a central and secured repository for all audit documentation.
- Enables multiple users to access documentation at the same time.
- Enables access to audit information and documentation regardless of location, time zone or stage of audit process.
- Improves ability to control and validate final version of reports and information.
- Provides a highly structured format to support the audit process, reporting, follow-up and document management.
- Potentially reduces document storage costs.

For many organizations, identifying the need for an automated work paper tool is an emerging process. Different factors drive the need for this type of software package. For example, an organization may be starting a new department or facing specific events, issues or key risks; a merger may bring together two sets of auditors; departments without audit technology may realize they have become inefficient; or firms with technology already in place may find that it is no longer effective and may need to update their current software package to properly assess governance, risk and compliance all at once.

Because of these evolving needs, it makes sense for internal audit organizations to assess the need for a tool during the annual planning process. When considering this need, internal audit departments should ask the following questions. If you answer "yes" to any of these questions, your department might be in need of an automated work paper tool:

- Is your internal audit department tasked with managing Sarbanes-Oxley compliance in addition to traditional internal audit responsibilities?
- Are you seeking a flexible, configurable application that will allow you to automate your audit process from risk assessment through reporting?
- Do you wish to achieve any of the following?
  - Improve audit efficiency, accuracy and quality
  - Automate issue tracking
  - Access prior or current work papers from remote locations
  - Perform the same audit multiple times in one fiscal year and compare results
- Are your current tools being used ineffectively?

- Have any of the following events recently occurred?
  - Change of leadership
  - Significant staff turnover
  - Significant technology event such as a changeover in company platforms

36. What factors should internal audit consider when issuing an opinion on internal control?

Senior management and the board often expect the CAE to communicate an overall judgment about the organization's risk management process and system of internal control. This opinion can be one of positive or negative assurance.

The IIA recommends in its paper *Practical Considerations Regarding Internal Auditing Expressing an Opinion on Internal Control* that when the CAE is issuing an opinion on internal control, he or she needs to consider the scope of the audit work and the nature and extent of audit work performed, and evaluate what the evidence from the audit says about 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 is responsible for establishing and maintaining internal control
- The specific type of opinion being expressed by the auditor

The IIA also recommends that CAEs consider a few other items in this process:

1. Be careful that the opinion expressed is consistent with the internal audit activity's charter as approved by the board and supported by a sufficient amount of audit evidence.
2. Resist expressing an opinion related to a subject that is inconsistent with the charter.
3. Do not express an opinion that is not supported by sufficient audit evidence.
4. Understand fully the reason and proposed use of any opinion he or she is requested to use.
5. Ensure that any opinion is appropriate for its intended use and audience.

With regard to Sarbanes-Oxley Section 404, a number of CAEs have been asked to sign an attestation stating that internal auditing has evaluated ICFR and found either that the controls were effective or that they have material weaknesses or deficiencies. These attestations are often 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.

The IIA recommends that CAEs carefully consider the wording of such an attestation before signing it. Signing an attestation is similar in effect to expressing an opinion and is subject to the concerns discussed above. The IIA further recommends that CAEs consider:

- Whether a positive or negative assurance opinion is appropriate for the situation
- Limiting the opinion to the areas that have been audited according to the audit plan
- Not implying that the CAE has any management responsibility for internal control as part of his/her opinions expressed in support of Section 404
- Whether there has been any impairment of internal audit's independence and objectivity

37. What is an integrated audit?

A good way to think about an integrated audit is that it encourages a holistic approach to the internal audit process. To fully incorporate integrated auditing into an internal audit approach, auditors must be able to understand and assess the risks the organization faces at the strategic, operational and tactical levels. They also need to know about corporate governance, risk management and control models. Internal audit functions should consider moving toward using this audit approach if they are not already doing so.

In the past, the term "integrated audit" was used to describe performing a single audit to address both automated and manual controls and related risks at the same time. These days, the term refers to audits of internal control that are integrated not just across the process and IT areas, but also across all three spheres of the COSO model: financial reporting, regulatory compliance and operational effectiveness and efficiency. This brings to the forefront the importance of assembling and orchestrating teams with the right skills for these audits who will work in tandem.

Following the COSO frameworks can help a company perform an integrated audit. It is important to note that COSO does not demand the use of an integrated audit approach. However, if a company follows the COSO model in the audit planning and execution stages, it will likely conduct an integrated audit.

AS5 also encourages using an integrated audit approach when external auditors are performing the audit of ICFR and the audit of the financial statements to accomplish the objectives of both audits simultaneously. In addition, AS5 supports this approach through encouraging external auditors to rely on the work of others, where appropriate, when issuing an opinion on ICFR. The PCAOB believes this will help make the Sarbanes-Oxley compliance process more efficient and effective.

38. What is continuous monitoring and how does it strengthen the internal audit process?

In the *Global Technology Audit Guide 3: Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment* (GTAG 3), The IIA defines continuous monitoring as "the process that management puts in place to ensure that policies, procedures and business processes are operating effectively. It typically addresses management's responsibility to assess the adequacy and effectiveness of controls."

This GTAG goes on to report that the key to continuous monitoring is for management to own and perform the process as part of its responsibility to implement and maintain an effective control environment. Since management is responsible for internal controls, it should have a means to determine, on an ongoing basis, whether the controls are operating as designed. By being able to identify and correct control problems on a timely basis, the organization's overall control environment can improve. A typical additional benefit to the organization is that instances of error and fraud are significantly reduced, operational efficiency is enhanced, and bottom-line results are improved through a combination of cost savings and a reduction in overpayments and revenue leakage.

Continuous monitoring can be achieved through automated technology or through manual processes and procedures. But before deciding on which approach to take, the key is for management to determine what works best for the organization to achieve the ultimate goal: strengthening the control environment. This goal is in line with the definition of internal auditing, which says the function should help "an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes."

When an organization effectively implements continuous monitoring processes, the amount of detailed testing required by internal auditors decreases. This further allows the internal audit function to employ a risk-based audit approach and focus on areas of the organization with the greatest need.

39. How can internal audit assist in developing and maintaining an effective corporate governance environment?

Internal auditors are part of the foundation on which effective corporate governance is built. By being involved in this arena, internal auditors can better fulfill the complete definition of internal auditing.

However, it is important to be clear that it is the responsibility of the board of directors to develop and maintain an effective corporate governance environment. The IIA states in the position paper *Recommendation for Improving Corporate Governance* that internal audit's role is to be "a critical, independent observer of that process." The IIA *Standards*, which follow the COSO model, acknowledge that evaluating the corporate governance environment is part of internal audit's role in the organization. This evaluation process in turn assists management (and thus the board) in developing and maintaining an effective corporate governance environment.

Standard 2100 – Nature of Work states that "The internal audit activity must evaluate and contribute to the improvement of governance, risk management, and control processes using a systematic and disciplined approach."

2110 Governance – The internal audit activity must assess and make appropriate recommendations for improving the governance process in its accomplishment of the following objectives:

- Promoting appropriate ethics and values within the organization
- Ensuring effective organizational performance management and accountability
- Communicating risk and control information to appropriate areas of the organization
- Coordinating the activities of and communicating information among the board, external and internal auditors, and management

The role internal audit plays in governance is highly influenced by the maturity level of the organization's governance processes and structure, as well as the roles and qualifications of internal auditors. Typically, internal auditors operate in two capacities regarding corporate governance. First, auditors provide independent, objective assessments on the appropriateness of the company's governance structure and the operating effectiveness of specific governance activities. Second, they act as catalysts for change, advising or advocating improvements to enhance the organization's governance structure and practices.

Internal audit should have a clear set of published audit objectives to ensure that corporate governance mechanisms such as the internal control systems, risk management processes and financial reporting systems are monitored at all times. By providing assurance on the risk management, control and governance processes within an organization, internal auditing can fulfill its role as one of the cornerstones of effective organizational governance.

40. To what degree should the internal audit function coordinate its activities with its external audit firm?

While internal and external auditors differ with regard to their relationships to the organization, the scope of their work, their audit objectives and their mutual interest in the organization's internal control structure should drive the board of directors to require coordinated audit efforts. Doing so will increase the economy, efficiency and effectiveness of the overall audit process and help the board fulfill its audit process oversight responsibilities.

The IIA recommends that internal and external auditors meet periodically to discuss common interests; benefit from their complementary skill, areas of expertise and perspectives; gain an understanding of each other's scope of work and methods; discuss audit coverage and scheduling to minimize redundancies; provide access to reports, programs and working papers; and jointly assess areas of risk.

Practice Advisory 2120-A1-4, *Auditing the Financial Reporting Process*, also outlines a number of roles the CAE may consider to better coordinate internal and external audit activities and ensure the reliability and integrity of financial reports. These additional efforts facilitate internal audit's role in supporting the organization's governance process and the governing board and audit committee's oversight responsibilities.

AS5 also emphasizes the importance of this coordinated effort through its "relying on the work of others" language and the importance of reviewing internal audit reports related to ICFR.

41. What should the role of internal audit be in connection with a company's compliance efforts?

Internal audit should most definitely be involved with a company's compliance efforts since "compliance with applicable laws and regulations" is an integral part of COSO's definition of internal control. However, it is important to remember that compliance efforts are management's responsibility. The role of internal audit is to verify that management meets that responsibility through the risk assessment and audit process. Ultimately, management must own the responsibility around compliance in the applicable locations and areas.

The IIA *Standards*, which follow the COSO model, acknowledge that regulatory compliance risk is part of internal audit's role. Compliance with applicable laws and regulations is an integral part of the definition of internal control. Internal audit's involvement in a company's compliance efforts is directly supported by *Standard 2100 – Nature of Work*, which says the internal audit activity must evaluate and contribute to the improvement of governance, risk management and control processes.

Standard 2120.A1 further notes that internal audit must evaluate risk exposures relating to the organization's governance, operations and information systems regarding the reliability and integrity of financial and operational information; effectiveness and efficiency of operations; safeguarding of assets; and compliance with laws, regulations and contracts.

42. Should an internal audit function coordinate its efforts with the company's chief risk officer?

A successful risk management process is truly an integrated effort and should involve a number of key players throughout the organization. Because of this, it is critical for the internal audit function to coordinate its risk management role with the company's chief risk officer (CRO).

The role of the CRO, like that of the CAE, has evolved in recent years from being a compliance officer to serving as a high-profile, board-level advisor. CROs now play a pivotal role in determining an organization's risk strategy and ensuring the completeness and consistency of the organization's risk management processes across different business areas. The risk management function's value increases when risk professionals partner with the business lines (including internal audit), and vice versa, to achieve better understanding of the business operations and associated risks.

The IIA *Standards* support internal audit's role in identifying and evaluating significant risk exposures to the company. This effort should be a normal and ongoing part of internal audit's duties and provides invaluable insight to the risk management process. Practice Advisory 2100-3 recommends that internal audit's role in risk management efforts "be codified in the charters of the internal audit activity and the audit committee."

This Practice Advisory further states that risk management "responsibilities and activities should be coordinated among all groups and individuals with a role in the organization's risk management process. These responsibilities and activities should be appropriately documented in the organization's strategic plans, board policies, management directives, operating procedures and other governance type instruments."

Such a coordinated effort is a win-win situation for the company. First and foremost, establishing a risk strategy enables an organization to determine the priorities of the internal audit plan. Creating a risk strategy also allows an organization to establish a framework for assessing risk. This framework can in turn act as the cornerstone of a company's ongoing risk management foundation.

43. What should the role of internal audit be in evaluating a company's use of outsourced services?

Outsourcing services traditionally executed internally by the organization is not a new phenomenon. For decades, this trend has been sparked by an increase in productivity through technological innovations or a change in geopolitical institutions to foster a supportive environment for business. This strategy brings with it significant risks that must be recognized and managed. If not properly managed, companies may negatively affect their operations – and their customers. The execution of a service can be outsourced, but the ownership of the service cannot. The risk for delivering the service stays with the company. Because of the significant operational and financial risks associated with outsourcing processes to third parties, the internal audit function should be continually involved in assessing the risks and internal controls related to the processes performed by the service provider.

Practice Advisory 2100-13, *Effect of Third Parties on an Organization's IT Controls*, outlines procedures to be performed by internal auditors in reviewing the risks and internal controls related to outsourced services. These include:

- Obtain and document an understanding of the relationship between the services provided by the third party and the organization's control environment.
- If third-party services are significant to the organization, assess these controls to determine whether they function as described, operate effectively and assist the organization in achieving its control objectives.
- Assess the likelihood (or control risk) that the IT environment has weaknesses in control existence, design or operation. The auditor should identify where the control weakness exists, assess whether the control risk is significant and determine what effect it has on the control environment.
- Review the contract (possibly with the assistance of the organization's legal counsel) to determine the third-party's role and responsibility for assisting the organization in achieving its control objectives.
- Identify and review the components of the third-party service provider's corporate governance process.
- Consider the contractual relationship between the organization and the third-party provider and the third-party provider's evaluation and reporting on their controls.
- Review reports from independent sources on the third-party provider's controls.
- Consider whether the third party has an internal audit department. The presence of internal auditors can enhance the strength of the control environment.
- If the auditor decides to directly review and test controls at the third-party provider, the auditor should:
  - Work with management and, as applicable, internal audit of the third-party provider to plan the engagement, set its objectives and scope of review, and determine timing, staffing needs and other issues.
  - Address issues such as access to third-party systems and assets, as well as confidentiality.
  - Develop an audit program, budget and engagement plan.
  - Validate control objectives.
- Determine whether the third party uses subcontractors to provide systems and services, as well as the effect the subcontractors may have on the third-party's controls.

Outsourcing is a critical component of many companies' processing capabilities, and all indicators point to outsourcing's continued growth. Organizations must establish ways to effectively manage and control their outsourced processes in order to meet the growing scrutiny of regulators, management and key stakeholders.

Performing a Quality Assessment Review

44. Should internal audit conduct a quality assessment review (QAR) periodically?

The IIA *Standards* require a QAR once every five years. The relevant standard states that "External assessments must be conducted at least once every five years by a qualified, independent reviewer or review team from outside the organization."

Many internal audit departments already comply with this standard and also perform their own internal assessments on a more frequent basis. In addition, many internal audit functions seek to go beyond mere compliance with The IIA *Standards* and include as part of the scope of their QARs a "best practices" component to foster continuous improvement within the function.

Other internal audit functions realize that for whatever reason (new company business models, risks, regulations, new products and services issues, for example), the function needs to change substantially from its current structure. In these cases, internal audit functions and their audit committees take a "transformation" approach and typically work with outside advisors to redirect and reorganize the function to meet current reality.

Also, the audit committee should seek the viewpoint of the company's external auditor on the performance, competency and objectivity of its internal audit function, including the degree of coordination with the external audit firm and the degree of reliance the firm places on internal audit's work. The relevant standard also indicates:

> A qualified reviewer or review team consists of individuals who are competent in the professional practice of internal auditing and the external assessment process. The evaluation of the competency of the reviewer and review team is a judgment that considers the professional internal audit experience and professional credentials of the individuals selected to perform the review. The evaluation of qualifications also considers the size and complexity of the organizations that the reviewers have been associated with in relation to the organization for which the internal audit activity is being assessed, as well as the need for particular sector, industry, or technical knowledge.
>
> An independent reviewer or review team means not having either a real or an apparent conflict of interest and not being a part of, or under the control of, the organization to which the internal audit activity belongs.

Whatever exact form the review takes, the audit committee should be apprised of the process and the results of the review, as well as the agreed-upon actions resulting from this effort.

45. How does completing a quality assessment review strengthen the value internal audit brings to the organization?

The quality assessment review process should assess the internal audit function's current state of performance, evaluate the desired state and future needs, identify gaps, provide recommendations to narrow those gaps, and establish a basis to measure future improvement. Completing a quality assessment review provides internal audit with a direct measurement of the effectiveness of its efforts, as well as assurance that internal audit is in conformance with The IIA *Standards* and *Code of Ethics*. This process represents an opportunity for internal audit departments to learn whether they are going beyond the basics to become valued advisors within their companies.

In addition, the scope of many external quality assessments provides the opportunity to compare the reviewed function to current leading practices and identify gaps in performance with these leading practices.

46. What types of assessments are available to comply with quality assessment review requirements?

When satisfying the quality assessment requirement laid out in The IIA *Standards*, CAEs have two options: an *external quality assessment* or a *self-assessment with external validation*. Both options are acceptable according to The IIA *Standards*. The difference between these two alternatives lies primarily in *who* does the work. Both types of assessments review the internal audit function for efficiency and effectiveness, conformity with the *Standards* and stakeholder expectations.

In an *external quality assessment*, the work is performed by an independent reviewer or review team from outside the company. According to The IIA, an external quality assessment should review the following elements of the internal audit activity:

- Compliance with The IIA *Standards*, The IIA's *Code of Ethics* and the internal audit activity's charter, plans, policies, procedures, practices, and applicable legislative and regulatory requirements
- Expectations of the internal audit activity expressed by the board, executive management and operational managers
- Integration of the internal audit activity into the organization's governance process, including the attendant relationships between and among the key groups involved in that process
- Tools and techniques employed by the internal audit activity
- Mix of knowledge, experience and disciplines within the staff, including staff focus on process improvement
- Determination as to whether or not the activity adds value and improves the organization's operations

In the *self-assessment with external validation* option, the basic review work is done by the internal audit function and then an independent team, external to the organization, validates the work performed by internal audit. When considering this option, the internal department should weigh the benefits and savings of this internal approach against the opportunity cost. Would the department need to alter the audit plan schedule to accommodate the self-assessment?

For internal audit functions with limited resources, the self-assessment with external validation option can help them comply by limiting the scope of the review. According to The IIA, this option should include the following features:

- A comprehensive and fully documented self-assessment process, which should emulate the external assessment process, at least with respect to evaluation of compliance with The IIA *Standards*.
- An independent on-site validation by a qualified reviewer.
- Economical time and resource requirements with the primary focus on compliance with The IIA *Standards*. Attention to other areas such as benchmarking, review and consultation as to employment of best practices, and interviews with senior and operating management may be reduced or omitted.
- Otherwise, the same requirements and criteria as set forth in Practice Advisory 1312-1 for external quality assessments would apply for:
  - General considerations
  - Qualifications of the independent validator (external reviewer)
  - Independence, integrity and objectivity, competence, approval by management and the board, and scope (except for areas such as employment of tools, techniques, other best practices, career development and value-adding activities)
  - Communication of results (including remedial actions and their accomplishment)

Variation to the actual scope of each option can be considered depending on the full objective of the review. For example, under the self-assessment with external validation option, the internal audit function may drive the independent reviewer to increase its scope to include more management and audit committee interviews, review additional audits completed and evaluate the internal audit activity against leading practices.

Internal Audit's Role in Sarbanes-Oxley Compliance

47. Does the Sarbanes-Oxley Act of 2002 require companies to have an internal audit function?

No, Sarbanes-Oxley does not specifically require the existence of an internal audit function.

However, the Public Company Accounting Oversight Board (PCAOB) makes note of internal audit functions in AS5, specifically in Paragraphs 16-19 of the section "Using the Work of Others." This guideline presumes that some percentage of public companies, especially large and more complex ones, already have an internal audit function in place, and that external auditors may rely to an extent on the work of internal audit.

It is important to note that the PCAOB significantly reduced the number of references to internal audit in AS5 versus AS2, specifically as it relates to indicators of a significant deficiency. This does not imply that the PCAOB no longer views having an internal audit function as important; instead, it encourages external auditors to support a principles-based approach to the assessment of ICFR, rather than a prescriptive approach as defined by AS2.

48. Should internal auditors play a role in our Sarbanes-Oxley activities?

Internal auditors possess many skills and experiences that can add value to a company's Sarbanes-Oxley compliance efforts. A risk-and-controls orientation, knowledge of processes and operations, clear understanding of the need for complete and accurate documentation, and experience in compliance with regulations, among other attributes, make an internal audit function, or selected internal audit resources, a logical choice for participating in Sarbanes-Oxley compliance projects, especially those related to Sections 301, 302 and 404.

The actual role that internal audit should play in Sarbanes-Oxley activities will vary by company. Factors to consider include the size and resources of the current internal audit function, other resources available in the company, the level of outside advisors being utilized, and the timing and scope of Sarbanes-Oxley efforts. In addition, the company's external auditors should be consulted on their views related to the role internal audit may play and the extent to which they would rely on the work of internal audit in carrying out that role.

Internal audit's charter may serve as a guide to determining and concluding on the function's role. The PCAOB's AS5, on ICFR audits, provides guidance about the role internal audit should play, especially the extent to which the external auditor may use the work of internal auditors in connection with the audit.

Care should be taken, however, to ensure that internal audit does not "own" a company's Sarbanes-Oxley projects. Compliance with Sarbanes-Oxley is the responsibility of company management, the certifying officers and, in some cases, such as Section 301, the audit committee. A key success factor for Section 404 projects is the assumption of responsibility of effective ICFR by accountable process owners. It is important that internal audit's role be compatible with the overall mission and charter of the internal audit function. Its role should also not impair internal audit's objectivity, nor its ability to cover the major risk areas of the organization. Sarbanes-Oxley compliance is one of the risks to be included in the annual risk assessment process, and it should not be the function's *only* focus.

The IIA recommends, in its paper *Internal Auditing's Role in Section 302 and 404 of the U.S. Sarbanes-Oxley Act of 2002*, that internal audit's role in Sarbanes-Oxley projects "should ideally be one of support through consulting and assurance." Activities recommended for internal auditors when supporting Section 302 and 404 requirements include:

- Project oversight
- Consulting and project support
- Ongoing monitoring and testing
- Project audit

Questions to consider when defining internal audit's role related to Sarbanes-Oxley compliance include:

- Does internal audit have the right skill sets to be effective in the company's Sarbanes-Oxley compliance efforts?
- Does internal audit have the "bandwidth" to take on this work while continuing to perform its duties to fulfill the current year's internal audit plan and address risks identified as part of the risk-assessment process?
- Will there be any independence or objectivity issues if internal audit is too involved in the design and documentation of processes and controls, and is then asked to test such controls as part of the Section 404 work to determine the operating effectiveness of internal controls? Will these issues arise if internal audit performs tests of areas and controls as part of the current year's audit plan?
- Could too much involvement by internal audit hinder an "ownership attitude" among management and process owners toward process and internal control documentation and the evaluation of such documentation?

The ongoing role of internal audit in Sarbanes-Oxley efforts should be discussed with and agreed upon by the audit committee and management. Companies also should consider consulting with their external auditors.

49. How has the role of internal audit in Sarbanes-Oxley compliance changed since the inception of the legislation in 2002?

The internal audit function continues to contribute to the many activities that support Sarbanes-Oxley compliance. Trends noted in the three editions of Protiviti's Internal Audit Rebalancing study are consistent with the call for internal audit to return to traditional and broader duties – executing the best risk assessment possible, using a top-down approach and addressing the issues of most concern to the company.

When Sarbanes-Oxley was enacted in 2002, internal audit was often management's first-choice resource for internal control expertise. Internal auditors responded promptly to educate management and audit committees on the new internal control reporting requirements and to help scope these projects and provide guidance. In many cases, internal auditors went beyond what some might consider the "normal role" of an internal audit function.

Internal audit's roles during the first three years of Sarbanes-Oxley compliance typically included:

Planning	Control design evaluation
Operational effectiveness testing	Year-end update testing
Documentation	Aggregation/Reporting of deficiencies
Monitoring	Remediation

Protiviti's most recent Internal Audit Rebalancing survey, detailed in its report titled *Moving Internal Audit Back into Balance, Third Edition*,[3] notes the following trends in the changes to internal audit's primary roles during the first three years of Sarbanes-Oxley compliance:

- Control design evaluation and testing of operational effectiveness are the most frequently cited internal audit roles in Sarbanes-Oxley compliance efforts, especially in Year One.
- Internal audit staffing hours dramatically decrease in Years Two and Three of compliance when compared to Year One.
- Internal audit's roles for assisting organizational efforts in Sarbanes-Oxley compliance decrease markedly in Years Two and Three, most noticeably in the area of documentation.
- The role of developer of documentation drops sharply after Year One.
- Consistently important roles across all three years include:
  - Control design evaluation and testing of operational effectiveness
  - Lead responsibility
  - Membership in the compliance team/steering committee
- Planning assistance and control design evaluation are the most common assisting roles in Year One; in Years Two and Three, operational effectiveness testing is the most important assisting role.

Also of note, both the SEC's interpretive guidance to management on implementing Section 404 of Sarbanes-Oxley and the PCAOB's Auditing Standard No. 5 (both of which were finalized in 2007) are having a significant positive impact on internal audit rebalancing initiatives. Specifically, the SEC's and PCAOB's guidance is helping to spur rebalancing activities, establish a finite number of key controls to document and test, and reduce the time devoted to Sarbanes-Oxley compliance.

These notable trends and others are evidence that internal audit leaders are reining in their internal audit resources from a complete focus on Sarbanes-Oxley, and evaluating where their role adds the most value to this compliance effort, so that the internal audit function can appropriately address risks impacting the entire organization.

50. Is an ineffective internal audit function a significant deficiency under Section 404 of Sarbanes-Oxley?

It depends on the facts and circumstances of the organization. While the superseded Auditing Standard No. 2 (AS2) listed an ineffective internal audit function as one strong indicator of a significant deficiency, the guidance in AS5 does not list any strong indicators. That language was eliminated from the new standard by the PCAOB to encourage auditor judgment and to support a principles-based approach to the assessment of ICFR, rather than the more prescriptive approach defined by AS2. However, because of the important role internal audit plays in creating and maintaining an effective internal control structure, there is the potential for an ineffective internal audit function to be a significant deficiency if it is deemed to have an adverse impact on the organization's monitoring process. That impact merits attention from those responsible for oversight of the registrant's financial reporting.

Therefore, though the NYSE may not have delineated specific guidance on internal audit functions (see Questions 70 - 90), companies – especially large, complex entities – should be reviewing the nature, size, scope and overall effectiveness of their existing internal audit functions in connection with their Sarbanes-Oxley Section 404 compliance efforts.

Possible indicators of a substandard internal audit function include:

- An inadequately funded function, especially when compared to the results of the company's risk assessment, similar organizations in the same industry, previous years' funding, etc.
- Extremely narrow scope of the function, again as compared to the results of the company's risk assessment
- A significant lack of focus or attention on IT-related risks and issues

[3]For more information, see Protiviti's *Moving Internal Audit Back into Balance: A Post-Sarbanes-Oxley Survey*, available at **www.protiviti.com**.

- Clearly unqualified personnel, given the required focus of the function from the company's risk assessment process
- Poor results from a quality assessment review
- A weak or ineffective CAE, or the lack of a CAE for an extended period of time
- A history of inaccurate or low-quality work that cannot be relied on by the external auditor
- Assignment of otherwise competent auditors to perform work in areas in which they were recently assigned responsibilities

Note that in determining a significant deficiency in any area of a company's operations or processes, considerable judgment is required, as each situation is unique.

51. Are there alternative structures to consider outside of internal audit when planning ongoing compliance with Sarbanes-Oxley?

Yes. For example, a risk control group separate from internal audit may help process owners to document controls, evaluate change, assess controls design, test controls operation and remediate controls. These specialists can be invaluable to process owners who may not have the capacity for, and often need assistance with, documenting, evaluating, testing and improving controls. Risk control specialists:

- Assist and coach process owners during times of change
- Ensure consistency of the assessment approach across processes
- Provide increased assurance to certifying officers
- Provide assistance to process owners as self-assessments identify gaps requiring formulation and execution of remediation plans

The skill sets of risk control specialists include understanding the business and how it operates, knowledge of risk, being able to analyze and map processes, understanding control practices and controls assessment, knowing how to integrate IT risks and controls, understanding the various requirements and rules, being able to translate the rules into terms others will understand, and working well with people. Risk control specialists do not execute processes and controls. They only assist process owners with their responsibilities to establish and maintain them. The number of risk control specialists depends on the complexity and number of processes. They may report to a C-level executive (such as the CFO, the CRO or CCO) or may be embedded within operations.

52. Is it important for an internal audit function to adhere to The IIA *Standards* as it relates to Sarbanes-Oxley?

While there is no general rule of law or specific provision in Sarbanes-Oxley to follow The IIA *Standards*, it certainly is prudent to do so on several grounds. First, The IIA *Standards* are those promulgated by the principal professional organization of internal auditors and to which all Certified Internal Auditors (CIAs) and members of The IIA are bound to follow logically and professionally. Second, The IIA *Standards* are well thought-out and reasonable, and provide an excellent, well-organized set of principles and processes. Finally, if an internal audit function desires to complete a quality assessment review, it needs to follow and be able to demonstrate that it adheres to The IIA *Standards* through actual application.

It remains to be seen whether the external auditor will have to determine on his or her own if The IIA *Standards* are being followed by an internal audit function. A quality assessment review by a third party may provide the objective and sufficient evidence required by the external auditor to make this determination. On the other hand, the external auditor may conclude that he or she must perform his or her own evaluation of the audit client's internal audit function to determine the exact degree, amount and nature of internal audit work to review, test and ultimately rely upon in connection with their work.

It should be noted, however, that merely following The IIA *Standards* is not enough to allow the external auditor to place maximum reliance on internal audit work. Additional qualities for the external auditor to consider include the competence and objectivity of the internal audit function and its reporting lines, and the accuracy and completeness of work completed – values that are embedded throughout the *Standards*.

53. Can external auditors rely on the work of internal auditors relating to Section 404 compliance?

Yes. Tests of the effectiveness of ICFR performed by management, internal auditors or others are critical to the continued effective functioning of ICFR. This work can have a significant effect on the nature, timing and extent of the work the independent auditor will need to perform. Generally, the more testing management and others (including internal audit) perform, and the more reliable that work, the less work the external auditor will need to perform.

When internal auditors perform ICFR work under the direction of management

In AS5, the PCAOB adopted a principles-based approach providing the auditor considerable flexibility by allowing the exercise of professional judgment about the use of the work of others, including internal auditors. The Board concluded that the provisions of SAS 65 are sound and appropriate. However, these provisions – which are described in detail in AU section 322, *The Auditor's Consideration of the Internal Audit Function in an Audit of Financial Statements* (AU 322) – were altered slightly in AS5 for application to internal control assessments.

The PCAOB encourages greater use of the work of others in AS5 by requiring auditors to (1) understand the relevant activities of others and determine how the results of that work may affect his or her audit and (2) evaluate whether and how to use their work to reduce audit testing. There is no reason why the external auditor should not do this, particularly if an effectively functioning internal audit function is in place. AS5 emphasizes the importance of assessing the competency and objectivity "of the persons who the (external) auditor plans to use to determine the extent to which the (external) auditor may use their work. The higher degree of competence and objectivity, the greater use the (external) auditor may make of the work."

The guidance included in AS5 applies the principles in AU 322 to focus the auditor's use of the work of others more specifically on altering the nature, timing and extent of the external auditor's work than otherwise would have been performed to test controls as part of an integrated audit of the financial statements and ICFR. The basic premise of AS5 is that the external auditor may use work performed by, or receive assistance from, internal auditors, other company personnel (in addition to internal auditors) and third parties working under the direction of management or the audit committee that provides evidence about ICFR effectiveness.

AU 322 emphasizes the following principles when making this assessment:

(1) The nature of the controls being tested

The external auditor should consider several factors when evaluating the nature of the controls subjected to the work of others. These factors include:

- The materiality of the financial reporting elements the control addresses
- The degree of judgment required to evaluate operating effectiveness
- The pervasiveness of the control
- The level of judgment or estimation required in the account or disclosure affected by the control
- The potential for management override of the control

As these factors increase in significance, the need for the external auditor to perform his or her own work increases. As these factors decrease in significance, the external auditor may rely more on the work of others. AS5 further states, "The extent to which the auditor may use the work of others in an audit of internal control also depends on the risk associated with the control being tested. As the risk associated with a control increases, the need for the auditor to perform his or her own work on the control increases."

(2) The competency and objectivity of the individuals performing the work

The Board provided criteria for the separate evaluation of competence and objectivity. The external auditor must make this evaluation by obtaining or updating information from prior years. This evaluation could result in testing factors relating to *competence* (e.g., education, certifications, performance evaluation) and *objectivity* (e.g., organizational status, reporting lines, policies with respect to assigning individuals to test areas to which they were recently assigned). The context of the auditor's assessment of competence in conjunction with an audit of ICFR is whether the persons performing the work have the qualifications and ability to perform the work the auditor plans to use. The context of the auditor's assessment of objectivity in conjunction with an audit of ICFR is whether factors are present that either inhibit or promote a person's ability to perform, with the necessary degree of impartiality and freedom of bias, the work the auditor plans to use.

The standard notes that internal auditors "are expected to have greater competence and objectivity in performing the type of work that will be useful to the (external) auditor." This point of view suggests that the auditor will be able to rely to a greater extent on the work of a "highly competent and objective internal audit or equivalent testing or compliance function" than on work performed by others within the company. That said, the external auditor will also be able to rely on the work of company personnel other than internal auditors, as well as third parties functioning under the direction of management if they meet the competency and objectivity criteria.

(3) Testing the work of others

The Board stated that testing the work of others is an important part of an ongoing assessment of their competence and objectivity. The external auditor must consider factors such as:

- Scope of work is appropriate to meet the objectives of the work.
- Work programs are adequate.
- Work performed is adequately documented, including evidence of supervision and review.
- Conclusions are appropriate in the circumstances.
- Results are consistent with the results of the work performed.

Section 404 compliance teams will want to make sure they are managing their work appropriately, consistent with the above criteria. With respect to reperformance of the work of others (often referred to as "over-testing"), the PCAOB did not set any specific requirements as to the extent of the reperformance.

In applying the above criteria, AS5 eliminated the restriction in AS2 that prevented the auditor from using the work of others to reduce the work he or she performs with respect to the control environment, as defined by the COSO framework. The external auditor can use the work of others in conjunction with the performance of walkthroughs, but only on the basis of direct assistance, as described in Paragraph 27 of AU 322.

In summary, the PCAOB's approach under AS5 clearly allows the external auditor to appropriately use the work of others, and not just internal auditors, as a basis for altering the scope of an audit of ICFR. The PCAOB standard makes clear that the external auditor is responsible for compiling evidence from all sources to support its opinion on the effectiveness of ICFR. Relying on the work of others is only one of the sources of evidence available to external auditors in this assessment.

AS5 describes the different sources of evidence external auditors should rely upon. The PCAOB's intent is to provide flexibility in using the work of others while also preventing over-reliance on the work of others. For example, federal bank regulators commented to the PCAOB that, in their experience with FDICIA, external auditors have a tendency to rely too heavily on the work of management and others.

When internal auditors perform separate evaluations of ICFR, independent of the work performed by the Section 404 compliance team

The external auditor considers all relevant and available information about internal control when evaluating internal control effectiveness. The PCAOB standard encourages the external auditor to consider the results of tests by internal audit when designing the audit approach and ultimately in forming an opinion on the effectiveness of ICFR by

requiring an understanding of the relevant activities of others, a determination as to how the results of that work may affect the audit, and evaluating whether and how to use the work to reduce audit testing. To this end, the standard requires the auditor to review all reports issued during the year by internal audit (or similar functions, such as the loan review function in a financial institution) that address ICFR, and to evaluate any internal control deficiencies identified in those reports. This review would include reports issued by internal audit as a result of operational audits, or specific reviews of key processes if those reports address controls related to ICFR. Again, the competence and objectivity of the persons performing the work will be vital to the external auditor.

54. What does it mean to "rebalance" the internal audit function?

Protiviti defines "rebalancing" as:

> The process of moving internal audit activities away from Sarbanes-Oxley to a broader coverage of the COSO framework.

Prior to Sarbanes-Oxley, internal auditors generally completed a risk assessment, working closely with company management and the audit committee, to determine "what could go wrong" in a number of areas, including operations, finance, and compliance with laws and regulations. When Sarbanes-Oxley was enacted in July 2002, companies and their internal audit departments became highly focused on helping their organizations establish, design and test internal control over financial reporting as required by Sarbanes-Oxley.

But in the process, internal audit may have gone too far. The intense focus on Sarbanes-Oxley compliance prevented internal audit activities from addressing other important business risks. Attention and resources were redirected from other essential or historical roles in the risk management areas within the organization. In many companies, the processes and controls associated with these other business risks have not been audited in several years, since the inception of Sarbanes-Oxley. At times, auditors may have crossed the line of being fully objective or independent as required by the *Standards* promulgated by The IIA.

The truth, of course, is that internal audit professionals have a much broader mandate than simply ensuring the reliability of controls over financial reporting. Thus, the concept of rebalancing the internal audit function was born.

As part of the effort to rebalance, internal audit should work with management to establish ongoing, sustainable Sarbanes-Oxley compliance processes that will be less time-intensive over the long term. When doing so, internal audit should also take the opportunity to address risks recently overshadowed by Sarbanes-Oxley activities and reconsider risk management effectiveness across the complete COSO framework. Companies should also return to the full suite of business objectives as articulated by the COSO internal control framework. This would include covering the effectiveness and efficiency of operations, compliance with applicable laws and regulations, and the safeguarding of assets, in addition to the reliability of financial reporting.

55. Why should companies evaluate the need to rebalance their internal audit functions?

Now that the initial burden of Sarbanes-Oxley compliance is lightening for many companies, CAEs are feeling pressure from all sides to rebalance their internal audit activity. Management continues to push for reduced time and money dedicated to Sarbanes-Oxley compliance. Audit committees are demanding that auditors be attentive to other areas of the business, not just financial reporting risks.

The reality is this: Internal audit functions cannot be effective over time if they solely focus on internal control over financial reporting. To reach an appropriate level of effectiveness, companies must re-evaluate and rebalance internal audit activities with a focus on stakeholder expectations and risk-based auditing.

Effective internal audit functions are those that focus on the full suite of control objectives as articulated by the COSO internal control framework. These functions also help organizations accomplish their business objectives by bringing a systematic, disciplined approach to evaluating and improving the effectiveness of governance, risk management and control processes. Being an effective internal audit function is an ongoing and evolving process in today's dynamic business environment.

56. How should organizations align their Sarbanes-Oxley and internal audit resources to achieve effective rebalancing?

A key part of achieving rebalancing is to effectively align Sarbanes-Oxley and internal audit resources so that the internal audit function can appropriately address enterprisewide risk, significant areas of controls and activity, and other organizational needs, including Sarbanes-Oxley compliance. By taking a realistic but balanced approach to what truly needs to be accomplished, organizations can avoid major impediments toward rebalancing progress.

Rebalancing the internal audit activity is not as simple as going back to what had been done before Sarbanes-Oxley. Internal auditors have played a key role in Sarbanes-Oxley efforts as management and others looked to them for advice and resources. As a result, the intensity of Sarbanes-Oxley challenged the internal auditing function's ability to complete its original plans. Like it or not, Sarbanes-Oxley will continue to be a large part of many internal audit functions' focus in the foreseeable future.

To achieve rebalancing, it is important to first identify all activities critical to internal audit and Sarbanes-Oxley efforts. This can be accomplished by completing a risk assessment and identifying which activities related to these efforts the organization should continue to resource. Next, identify who in the organization is responsible for these critical areas. Then, perform a resource budget-to-actual comparison through the following steps:

1. Develop a budget for Sarbanes-Oxley testing or other Sarbanes-Oxley areas for which internal audit will be responsible.
2. Develop a budget based on the risks related to all other audit areas – operational and compliance.
3. Consider what overlaps or synergies exist, or could exist, between the planned work activities in steps one and two to arrive at a consolidated budget.

While developing a resource budget, companies can work toward aligning their Sarbanes-Oxley and internal audit resources through one – or many – of the following tactics:

Reallocate existing resources	Add additional resources
Rescope workload (Sarbanes-Oxley and internal audit)	Conduct an enterprisewide risk assessment
Utilize more self-assessment and self-audits by process owners and executives	Use third parties to complete certain work to assist in rebalancing
Create a separate risk and controls function to focus primarily on Section 404	Increase ownership by process owners

Source: *Moving Internal Audit Back into Balance: A Post-Sarbanes-Oxley Survey*, available at **www.protiviti.com**

Effectively realigning resources will allow organizations to experience one or many of the following rebalancing benefits:

More appropriate coverage of risk	Increased effectiveness and efficiency of operations
Internal audit able to perform more traditional audits	Increased objectivity
Reduced Section 404 and 302 compliance costs	Increased reliance by external auditors on work of internal audit

Source: *Moving Internal Audit Back into Balance: A Post-Sarbanes-Oxley Survey*, available at **www.protiviti.com**

Management and Audit Committee Considerations

57. How can management utilize internal audit most effectively?

Internal audit represents a valuable resource to management as it seeks to meet business objectives, especially as it relates to the objectives of internal control: efficiency and effectiveness of operations, reliability of financial reporting, compliance with applicable laws and regulations, and the safeguarding of assets.

Each company's internal audit function possesses unique individuals, skills and competencies, which management needs to understand and use effectively in helping meet its objectives. Internal audit should not be a function for the exclusive use of the audit committee. As the SEC and related literature suggest, an internal audit function, by its very nature, is a part of management's systems of internal control and thus should be an asset and tool for management.

While the charter of, need for and capability of each company's internal audit function vary, management may find the following suggestions helpful in determining how to best leverage internal audit resources to achieve strong, well-designed and effective risk management, internal control and corporate governance processes:

- Utilize internal audit resources as part of the company's enterprisewide risk assessment/management process to identify, source, measure, prioritize and develop a plan to address and manage the most significant business risks it faces in achieving its business objectives.
- Provide key input to the internal audit function in the development of the annual internal audit plan and changes to the plan during the year to focus limited resources on risks and areas of the greatest importance.
- Discuss and develop plans for internal audit to assist in efforts related to compliance with Sarbanes-Oxley, specifically Sections 301, 302 and 404.
- Consider how the internal audit function might be used as a rotational management-training program for company employees. Also, consider how guest auditor and short-term temporary assignments of employees can provide needed specialized skills to the function. Evaluate and discuss with internal audit the need to supplement its resource base and skill sets with outside resources.
- Support the function in connection with its key findings and its plan for process owners to make changes and improvements to internal controls and process issues and deficiencies.
- Visibly support and encourage the mission and efforts of the internal audit function with an appropriate "tone at the top."
- Work closely with the audit committee to help ensure the internal audit function remains objective and adds value to the organization.

58. What should the audit committee's relationship be with an organization's board of directors, compensation committee, disclosure committee, and nominating and governance committee?

The audit committee is a separately chartered committee of the board of directors. The audit committee has a direct relationship with the board of directors as it reports to the board on a quarterly or more frequent basis on such things as audit plans, audit findings and other items deemed to be significant. Generally, the audit committee's purpose is to assist the board in overseeing the:

- Reliability of the entity's financial statements and disclosures
- Effectiveness of the entity's internal control and risk management systems
- Compliance with the entity's code of business conduct and legal and regulatory requirements
- Independence, qualifications and performance of the external auditors
- Performance of the internal audit activity

The role of the audit committee has significantly expanded in recent years. Realizing this, the board of directors has begun to shift some of the audit committee's responsibilities to separately chartered committees to create a balance of duties and ensure they are effectively executed. These additional committees have often included a compensation committee, disclosure committee, and nominating and governance committee.

The audit committee, compensation committee, disclosure committee, and nominating and governance committees have interlocking goals. These goals, along with defined roles and responsibilities, should be documented within individual committee charters. Strong working relationships with these committees enable the audit committee to help each one fulfill its responsibilities to senior management, the greater board of directors, shareholders and other stakeholders. A direct channel of communication between committees is essential to this process.

59. What is the audit committee's role with respect to establishing and monitoring corporate governance practices?

The audit committee plays a critical role in establishing and monitoring corporate governance practices. The board of directors has overall responsibility and accountability for risk management, internal control and corporate governance within the organization. The audit committee's role, as a separately chartered committee of the board of directors, includes focusing on the qualitative aspects of financial reporting to shareholders, on the company's processes to manage business and financial risk, and on compliance with significant applicable legal, ethical and regulatory requirements.

As part of the audit committee's oversight of the internal audit process, the internal audit function is responsible for auditing the organization's corporate governance process and communicating these results to the audit committee. In turn, the audit committee is responsible for monitoring the process put in place to implement needed improvements in corporate governance processes and controls. The execution of this system is carried out by management and the internal audit activity.

It is important to note that corporate governance and the role of the audit committee, like any other organizational structure, are significantly affected by the legal, institutional, financial, cultural and political circumstances in each country.

60. What is an audit committee's role with respect to an internal audit function?

Although the exact nature, charter, scope and reporting lines of internal audit may vary between companies, the audit committee plays a key role in supporting and overseeing aspects of an internal audit function's activities. While needing to ensure it does not assume day-to-day oversight activities on behalf of management or the internal audit function, the audit committee generally should be involved in the following matters:

- Provide input and approve the written charter for the internal audit function, including periodic review and updating.
- Understand, discuss and approve the company's risk assessment and resulting internal audit plan. As appropriate, review, discuss and approve changes to the audit plan during the year.
- At least annually, evaluate the internal audit function in relation to meeting the needs of the company and the audit committee, including compliance with its written charter.
- Hold executive sessions with the company's CAE.
- Provide input and direction as to the appropriate escalation protocols for significant findings and issues.
- Review, discuss and approve the compensation of the CAE, any changes therein and the hiring or termination of the CAE.
- Understand, discuss and approve the funding level for the internal audit function, and discuss its appropriateness and adequacy with management and the CAE.
- Review ongoing activities of the internal audit function, including its reports, and inquire as to any other matters that should be brought to the committee's attention.
- Direct the internal audit function, as necessary, to perform special reviews on behalf of management or the audit committee, including investigations of fraud or suspected fraud.
- Participate with internal audit to design and provide control, governance and ethics training to employees.

While the above listing is not intended to be all-inclusive, it provides reasonable overall guidance. Each audit committee should discuss, along with input from management, the role it should play in connection with the company's internal audit function. Of course, the requirements of all related regulations and stock exchange listing standards related to audit committees should be followed.

61. Should executive sessions (without management present) be held with the internal auditors as part of an audit committee meeting?

Yes. Executive sessions are beneficial to the audit committee and the company as a whole in furthering effective corporate governance. Our experience is that most high-performing audit committees already allow for such executive sessions (one each for the external and internal auditors) and that it is a best practice.

Further, we believe that executive sessions should be a standing part of the audit committee's regular agenda, whether or not there are specific matters or concerns that the internal audit function would like to communicate. This approach eliminates the discomfort that can occur when, during an audit committee meeting, the CAE calls for an executive session with the committee.

62. What should internal audit report to the audit committee?

Appropriate reporting by internal audit varies considerably from company to company based on a number of factors, including the charter and scope of the function, frequency and length of audit committee meetings, amount of material provided, and communications between meetings, as well as issues arising at the company.

However, as a guide, it might be reasonable to expect the following information to be reported to the audit committee by internal audit (assuming that meetings are conducted quarterly):

- Activities and audits completed during the last quarter
- Presentation and discussion of key findings from audits recently completed

- Status of past audit recommendations requiring resolution
- Planned activities for next quarter
- Any reported instances of fraud and internal audit's role in investigating such fraud
- In highly regulated environments, the results of recently completed audits by outside regulatory agencies
- Depending on the role and scope of internal audit, a status report on calls received from the company's hotline developed in connection with Section 301 of Sarbanes-Oxley
- As appropriate, reports related to assistance provided by internal audit in connection with other areas of Sarbanes-Oxley, such as Section 302 and 404 compliance efforts
- An update on any new risks or other issues facing the company that internal audit thinks should be addressed, and a determination whether the current internal audit plan should be modified to take these matters into consideration
- Other matters specifically requested of management or the audit committee

Every audit committee meeting presents an opportunity for internal audit to assist in educating the committee on timely issues and current matters. As an example, it might be appropriate for internal audit's presentation to include educational materials, articles and white papers for later reading by both management and the audit committee.

Internal audit adds considerable value in reporting its findings, observations and viewpoints to management as well as to the audit committee. Though management is often present at audit committee meetings, there should be more frequent, in-depth and informal communication between internal audit and company management. Internal audit should not be viewed solely as an instrument for the audit committee. In management's ongoing efforts to meet objectives related to risk management, controls and corporate governance, it should be working closely with internal audit.

63. What is the audit committee's role in evaluating the chief audit executive (CAE)?

The audit committee has a responsibility to evaluate the role of the CAE in conjunction with the executive to whom the CAE administratively reports. The IIA recommends that the audit committee endorse decisions regarding the hiring or termination of the CAE. The chairman of the audit committee should also be appropriately involved in performance evaluation and compensation decisions related to the CAE.

An evaluation of the CAE might include items such as:

- Results of a recent external quality assessment review
- Establishment of a process to monitor and follow up on management's actions related to audit findings
- Execution of audit plan (completed vs. planned audits)
- Operating a successful quality assessment and improvement program
- Quantitative and qualitative metrics established to measure internal audit performance
- Contributions to the improvement of risk management, control and governance process
- Stakeholder satisfaction
- Consistent processes for gathering, summarizing and analyzing measurement of data and providing timely feedback
- Training and retention of internal audit staff

In addition, the audit committee's written charter may specifically address the evaluation of the CAE, including the required frequency criteria to be used and reporting requirements.

64. How should the audit committee evaluate the effectiveness of internal audit?

Every audit committee should assess the effectiveness of the organization's internal audit function at least annually, if not throughout the year. The critical role that internal audit plays requires the audit committee to ensure the organization receives substantial benefit from the investment made in the internal audit function. Though the charter, scope, funding and activities of internal audit vary from company to company, audit committees should at least consider the following questions when evaluating their company's internal audit function:

- Has the function met the terms of its written charter?
- Is the function assisting the company in identifying and addressing the most significant risks?
- Is the function sufficiently objective in its mindset and approach? Is the audit committee assisting in creating and maintaining this objective viewpoint?
- Are members of the internal audit function technically competent and proficient? Does the function have the necessary resources to address key risks and issues adequately and appropriately?
- Is the function being led by a competent CAE who has the respect of company management, the audit committee and the internal audit staff?
- Is the function efficient in its efforts, methods and approach?
- Is the function delivering on the definition of internal auditing? That is, is it adding value, helping to improve operations, and bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes?

Evaluations of internal audit functions range from informal processes to formal, documented appraisals, including the use of outside advisors and the completion of a quality assessment review every five years, in accordance with The IIA *Standards*. Audit committees need to determine the appropriate scope and formality of this evaluation.

The audit committee should also receive an annual self-assessment on the internal audit function from the head of internal audit. This could be supplemented by discussions with management, external auditors and other stakeholders as relevant. It is essential that the evaluation process is understood and agreed upon by the board, audit committee and appropriate stakeholders.

65. What is the role of the audit committee in evaluating the role of the external auditor?

The audit committee serves as the liaison among the board of directors, external auditors, internal auditors and financial management. It owns the responsibility for recommending the appointment, reappointment and removal of external auditors. It is best practice to make this assessment an annual practice as this allows sufficient time to identify concerns associated with external auditor activity and correlates to the timing and release of the annual audit of the financial statements produced by the external auditor.

According to the United Kingdom's Financial Reporting Council's *Audit Committees – Combined Code Guidance (The Smith Report)*, criteria for evaluating the role of the external auditor may include:

- The relevance and appropriateness of the auditor's procedures
- The quality of the audit partner and audit staff from a technical accounting and auditing perspective, including their industry knowledge and their specialist technical expertise
- The qualifications of key members of the audit team
- Whether the auditors appeared to be unduly influenced by management during the audit
- Whether the work of internal audit was used appropriately
- Whether formal audit documents such as the audit plan and management letters were of sufficient quality

Other publications on the role of the audit committee, many of them produced by large public accounting firms, address such topics as how the audit committee should evaluate its external auditor.

External Auditor Considerations

66. Can we use our external auditors to perform internal audit work?

The NYSE rule is reasonably clear: The answer is "no." The rule states, "A company may choose to outsource this function to a third party other than its independent auditor."

Non-NYSE companies attempting to answer this question should consult with their legal counsel. However, both the SEC and Sarbanes-Oxley provide guidance on this topic. Section 201(a) of Sarbanes-Oxley adds a new section 10A(g) to the Securities Exchange Act of 1934. This section states that it shall be unlawful for a registered public accounting firm that performs an audit of an issuer's financial statements to provide that issuer, contemporaneously with the audit, any non-audit service, including nine services set forth in Sarbanes-Oxley. One of the nine listed and prohibited services is "internal audit outsourcing."

Interpretation of the new law is complex, and legal counsel should be consulted on this topic. However, the SEC perhaps summed it up most clearly when it stated, "Since the external auditor typically will rely, at least to some extent, on the existence of an internal audit function and consider its impact on the internal control system when conducting the audit of the financial statements, the accountant may be placed in the position of auditing his or her firm as part of the internal control system. In other words, if the internal audit function is outsourced to an accountant, the accountant assumes a management responsibility and becomes part of the company's control system."

Now that the same external auditor is also responsible for expressing an opinion on the company's ICFR under Section 404, the argument against such arrangements is even stronger.

67. Can external auditors rely on the work of internal auditors in connection with their financial statement audit?

Yes, but they are not required to do so. SAS 65 has long provided guidance on this issue. As noted in Question 53, the PCAOB slightly altered in AS5 the provisions of SAS 65 for application to internal control assessments, referring to AU 322.The guidance contained in the PCAOB's AS5 is similar in concept to that of SAS 65.

Section AU 322 (SAS 65) was issued more than 15 years ago by the Auditing Standards Board to address how an auditor considers the work and direct assistance of an internal audit function when performing an audit of financial statements in accordance with generally accepted auditing standards (GAAS). AU 322 requires that the external auditor inquire about internal audit's (1) organizational status within the company, (2) application of professional standards, (3) audit plan and (4) access to records. In addition, the external auditor is to inquire about any scope limitations in the internal auditor's work. AU 322 also provides guidance on how the external auditor assesses the competence and objectivity of internal auditors.

In AS5, the PCAOB refers to AU 322 (SAS 65) to encourage using an integrated audit concept when completing the financial statement audit and audit of ICFR. The PCAOB believes "that a single framework for the auditor's use of the work of others is preferable to separate frameworks for the audit of internal control and the audit of financial statements. The factors used to determine whether and to what extent it is appropriate to use the work of others should be the same for both audits."

Under AS5, the auditor may evaluate the use of the work of others based on two fundamental principles relating to (1) the risk associated with the control being tested and (2) the competency and objectivity of the individuals performing the work the auditor plans to use. With respect to the first principle, the PCAOB states the following: "As the risk associated with a control increases, the need for the auditor to perform his or her own work on the control increases." This principle replaces the "principal evidence" ceiling and explicit restrictions (such as testing the control environment) on using the work of others previously included in the now superseded AS2.

SAS 65 (AU 322) indicates that the external auditor considers many factors in determining the nature, timing and extent of auditing procedures to be performed in an audit of an entity's financial statements. One of those factors is the existence of an internal audit function.

Procedures required under SAS 65 (AU 322) in order for the external auditor to ultimately rely on the work of internal auditors include:

- Obtaining an understanding of the entity's internal audit function, including:
  - Organizational status within the entity
  - Application of professional standards
  - Audit plan, including the nature, timing and extent of internal audit work
  - Access to records and whether there are limitations on the scope of the internal auditing activity
- Assessing the competence and objectivity of the internal auditors

Areas related to competence:

- Educational level and professional experience of internal auditors
- Professional certification and continuing education
- Audit policies, programs and procedures
- Practices regarding assignment of internal auditors
- Supervision and review of internal auditors' activities
- Quality of working-paper documentation, reports and recommendations
- Evaluation of internal auditors' performance

Areas related to objectivity:

- The organizational status of the internal auditor responsible for the internal audit function, including:
  - Whether the internal auditor reports to an officer of sufficient status to ensure broad audit coverage and adequate consideration of, and action on, the findings and recommendations of the internal auditors
  - Whether the internal auditor has direct access and reports regularly to the board of directors, the audit committee or the owner-manager
  - Whether the board of directors, the audit committee or the owner-manager oversees employment decisions related to the internal auditor

– Policies to maintain internal auditors' objectivity about the areas audited, including:

- Policies prohibiting internal auditors from auditing areas where relatives are employed in important or audit-sensitive positions
- Policies prohibiting internal auditors from auditing areas where they were recently assigned or are scheduled to be assigned on completion of responsibilities in the internal audit function

Given today's heightened sensitivity to internal control, financial reporting and governance issues, it is even more critical for the coordination and potential reliance on internal audit procedures by the external auditor to be properly understood, evaluated, considered and communicated among the audit committee, management and internal audit leadership.

We strongly encourage audit committees, management and internal audit leadership to work closely with their external auditors to develop an appropriate and effective plan regarding the work of and degree of reliance on internal audit in connection with their financial statement audit, as well as in connection with their audit of ICFR. Complying with professional standards in this area as they exist today, or as they are changed by the PCAOB, is a primary consideration.

68. Do all internal audit reports need to be reviewed by the external auditor?

In the past, the answer was no, as there are no formal requirements to do so. However, since internal and external audit should be collaborating and coordinating efforts, it has been accepted and, in fact, customary to share internal audit reports with the external auditor.

Today, this practice varies by company and by audit firm. External auditors certainly should be able to see any and all internal audit reports they choose. What they should review (or should request) are those reports that have a bearing on their work.

The PCAOB's AS5 requires the external auditor to review all internal audit reports of a certain kind. As noted on Page A1-29, Paragraph 71 of AS5, "… the (external) auditor should review reports issued during the year by internal audit (or similar functions) that address controls related to ICFR and evaluate control deficiencies identified in those reports."

69. Can a company's external auditors perform an external quality assessment review of the company's internal audit function?

Yes. Practice Advisory 1312–1, *External Assessments* names external auditors as a possible qualified party for conducting an external quality assessment review of internal audit. However, when considering the organization's external auditors as candidates for this review, the CAE – in consultation with the audit committee and board of directors – should consider any real or apparent conflicts of interest that might impact this assessment.

The NYSE Internal Audit Requirement

70. What companies are impacted by the SEC's approval of the NYSE rules?

Only NYSE-listed firms are affected. While the SEC also approved new listing standards for the NASDAQ, these did not include an internal audit requirement. However, many companies with diverse and complex operations, both private and listed on other exchanges, may find that developing an effective internal audit function will assist them in maintaining, validating and improving internal controls; identifying opportunities to reduce costs and improve processes; and enhancing their corporate governance.

Additionally, with these standards now in place for NYSE companies, other regulatory bodies, governments and stock exchanges outside of the United States may choose to follow the lead of the NYSE.

71. What do the NYSE rules require?

Regarding internal audit, the NYSE regulations require that listed companies have an internal audit function. In added commentary on the rule, the NYSE states:

> Listed companies must maintain an internal audit function to provide management and the audit committee with ongoing assessments of the company's risk management processes and system of internal controls. A company may choose to outsource this function to a third-party service provider other than its independent auditor.

However, the guidance does not stipulate the minimum requirements of an internal audit function, nor does it establish any specific parameters for maintaining an internal audit function or department on an ongoing basis. The size, budget and structure of internal audit functions depend on many factors (see Questions 12 and 19–24). Most effective internal audit functions provide a risk-based assessment that incorporates appropriate personnel resources and skills to evaluate an entity's risk management processes and internal control systems. We believe the NYSE requirement begins by stating the end goal because organizations vary widely and effective risk management, internal controls and governance can be accomplished in different ways.

72. Does the NYSE provide listed companies with any instructions or guidance beyond the rule requiring an internal audit function?

The NYSE issued its own Frequently Asked Questions document, dated February 13, 2004, covering Section 303A, which includes the internal audit rule. Section 303A also contains a number of new listing rules related primarily to the board of directors and related board committee issues.

The Section 303A FAQs can be found on the NYSE website at www.nyse.com. (Please note that the internal audit rule is not addressed in detail.) This document may be amended from time to time. NYSE-listed companies should check the exchange's website periodically for updates.

73. When are the rules effective?

The NYSE internal audit rule is effective immediately for all companies on the day they list on the NYSE through an IPO or when transferring from another stock exchange.

However, there are some exceptions: Listed companies that are foreign private issuers (as such term is defined in Rule 3b-4 under the Exchange Act) are permitted to follow home-country practice in lieu of the provisions of Section 303A (except 303A.06, .11 and .12(b), which are not related to the internal audit function requirement). The NYSE-provided commentary discusses this interaction as an audit committee oversight component.

74. When and how does this rule regarding internal audit apply to companies transferring from another stock exchange?

According to the NYSE, when the exchange or market the company is transferring from does not have a similar internal audit requirement, then the company will need to be in compliance with the internal audit provision of Section 303A within one year of transferring to the NYSE.

75. Must foreign private issuers comply with this rule?

The NYSE Frequently Asked Questions document dated February 13, 2004, addresses this question in a general way as follows:

Foreign private issuers are required to comply with only the following parts of Section 303A:

- 303A.06 – Audit committee requirements
- 303A.11 – Requirements to disclose significant differences between their corporate governance practices and NYSE requirements for domestic listed companies
- 303A.12(b) – Foreign private issuer provides the NYSE with prompt notice if it fails to comply with the two sections noted above

We believe that foreign private issuers without an internal audit function must determine if these differences are significant. If so, then as required by Section 303A.11, the differences must be disclosed by the company, along with any other significant differences, either in the annual report required by the NYSE to be distributed to shareholders, or on the company's website.

As to the timing of this disclosure, the NYSE has stated:

> As of the company's Section 303A compliance date, if the company chooses to include the required disclosure on its website, it must do so promptly after it makes that determination.

76. Does the rule apply to companies with public debt?

No. The internal audit rule does not generally apply to companies listing only preferred or debt securities on the NYSE. According to the exchange, to the extent required by Rule 10A-3 under the Exchange Act, all companies listing only preferred or debt securities on the NYSE are required to comply with the requirements of Sections 303A.06 and .12(b).

77. Does the rule affect other stock exchanges and private companies?

No. The rule applies only to NYSE-listed companies. The NASDAQ and AMEX do not have internal audit requirements at the present time. Private companies are not affected by this rule. However, these organizations, their boards, audit committees and management may want to consider whether creating an internal audit function would provide tangible benefits and serve to demonstrate a higher level of corporate governance.

Many non-NYSE listed companies, large non-U.S. companies and large private companies have recognized the benefits an effective internal audit function can bring to their operations and compliance efforts, and have created such functions with positive and measurable results.

78. Are there similar proposals in process requiring an internal audit function for companies listed on other exchanges in the United States?

Not at the present time. However, the SEC, per its ruling commentary on the NYSE's revised listing requirements, is interested in "achieving symmetry between exchanges where possible." We understand many companies are choosing to move forward with internal audit functions for "best practices" benefits and institutional investor grading purposes.

In addition, board and audit committee members of NYSE companies who also serve on boards of companies on other stock exchanges may want to consider the inconsistency with their own form of corporate governance and oversight of not having an internal audit function at the non-NYSE companies at which they serve as directors.

In January 2003, The Conference Board Blue Ribbon Commission on Public Trust and Private Enterprise issued its findings and recommendations with respect to auditing and accounting. Under Principle III: Improving Internal Controls and Internal Auditing, one of the "Suggested Best Practices" states:

> All companies should have an internal audit function, regardless of whether it is an "in-house" function or one performed by an outside accounting firm that is not the firm that acts as the company's regular outside auditors.

We believe all firms should evaluate the need for an internal audit function if they do not have one. Additionally, after meeting with a member of the Blue Ribbon Commission, we have confirmed that the term "accounting firm" was not intended to preclude outsourcing to a qualified internal audit services provider.

79. When and how does this rule regarding internal audit apply to initial public offerings (IPOs) listing on the NYSE?

For companies going public after October 31, 2004, compliance with the internal audit rule must be by their listing date on the NYSE.

80. Does this rule require a company to hire new employees?

No. To the extent that the company already employs qualified professionals who can serve effectively in the professional and objective capacity of internal auditors, those individuals may be transferred to the new internal audit function (which would also have a written and approved charter in place). Existing functions should be examined for risk-based audit planning, technical competency and independence in areas such as reporting lines and scope of coverage.

The commentary attached to the rule specifically states, "A company may choose to outsource this function to a third-party service provider other than its independent auditor." Outsourcing could be an attractive option for many NYSE-listed companies that find themselves needing to quickly establish an internal audit function to achieve compliance. Companies that find they do not have the appropriate level of resources and talent internally, and that also do not want to spend time on a lengthy search process, may find outsourcing allows for accelerated start-up, potentially greater independence and objectivity, access to substantially greater skills, and more flexibility to increase or decrease internal audit activities to meet changing risks and conditions.

Additionally, outsourcing allows a company to curtail or halt internal audit work at certain times of the year when there may be conflicting priorities such as plant closings, mandatory vacations, year-end reporting, annual planning and budgeting.

Many companies find that some form of rotation in and out of an internal audit function can be beneficial to both the employee and the organization. Under this approach, a company utilizes full-time professionals with important knowledge and understanding of the company's business and operations. These individuals gain valuable experience in seeing, understanding, evaluating and helping to improve many areas within the organization. Also, once their rotation is completed, these employees are better prepared to identify, understand and deal with internal control and risk management-related issues. This type of program in a sense "fertilizes" the organization with professionals who gain practical knowledge and background regarding internal controls and business risks.

81. What is required if a company already has an internal audit function?

Nothing new is specifically required except possibly determining the adequacy of the existing internal audit function. By having an existing internal audit function, NYSE-listed companies comply with the new rule. That said, we recommend that companies with existing internal audit functions review their appropriateness and adequacy by asking themselves the following questions:

- Do we have an adequately resourced internal audit function?
- How does our function compare to that of other companies in our industry?
- Does our internal audit function meet The IIA *Standards*?
- Has our internal audit function undergone a quality assessment or peer review recently? (See Questions 44-46 for a description of QARs of internal audit functions, which are required by The IIA *Standards*.)
- Do the board, management, audit committee and key process owners believe internal audit is a value-added activity? If not, how should the function be changed to be more effective?

82. Can part-time internal auditors meet the NYSE rule?

According to our discussions with the NYSE, part-time internal auditors may meet the requirement. At smaller organizations, the extent of key business risks – and therefore the amount of appropriate time and effort required to address such risks – may not justify full-time resources. Independence and objectivity of resources should be strongly considered.

However, care should be taken to ensure that part-time internal auditors do not audit areas that they themselves supervise, or in which they initiate, complete, approve, record or reconcile transactions. Also, if part-time internal audit employees with other organizational duties are required to audit areas for which their own supervisors have responsibility, it could impair their objectivity either in fact or appearance, bringing into question the value or veracity of their audit findings.

Given the size, breadth and scope of most NYSE companies, we believe that, in most cases, part-time resources would not fulfill the spirit of the internal audit requirement and would not be in the best interests of management, the audit committee or shareholders.

83. How will NYSE-listed companies be expected to demonstrate compliance with the internal audit rule?

Every NYSE company must confirm annually, in writing, its compliance with all NYSE listing standards, one of which is the internal audit requirement. Our discussions with officials at the NYSE indicated that this written confirmation will be the primary form of compliance communication with the new rule. Under the Listing Rules of the NYSE, companies determined to have affirmed, but not actually complied with any of the listing standards, are subject to disciplinary action, including delisting from the exchange.

84. Does the rule require a written internal audit charter?

The NYSE rule makes no mention of requiring a written internal audit charter. However, Section 1000 of The IIA *Standards* makes it clear that a charter should exist for an internal audit function:

> The purpose, authority, and responsibility of the internal audit activity must be formally defined in an internal audit charter, consistent with the Definition of Internal Auditing, the Code of Ethics, and the Standards. The chief audit executive must periodically review the internal audit charter and present it to senior management and the board for approval.

We believe that under the NYSE internal audit rule, it would be inconsistent to communicate that an internal audit function exists when its scope of authority, independence and reporting responsibilities are not defined in a written internal audit charter, approved by the audit committee. (See Appendices A and B.)

85. Does the NYSE rule require that The IIA *Standards* be followed?

The NYSE rule does not require companies to follow – nor does it mention – The IIA *Standards*. However, given The IIA's standing as the leading global professional organization for internal audit, The IIA *Standards* themselves would seem to be guidelines that most, if not all, internal audit functions would follow, particularly those functions led or staffed by CIAs.

Therefore, while there is no specific requirement within the NYSE rule, we believe there is a general expectation in the industry that a company's internal audit function would adhere to The IIA *Standards* as an accepted best practice. Additionally, in most circumstances, this would allow maximum reliance by the external auditor on the results of internal audit procedures.

86. Have internal audit functions been required previously?

No. However, certain industries have built-in requirements for internal audit and compliance functions, such as financial services (Federal Deposit Insurance Corporation Improvement Act), healthcare, government and energy, to name a few. The NYSE rule is the first broad internal audit requirement for a market.

87. Is there any minimum amount of expenditure or effort required under the NYSE rule?

No, there is no minimum specified. Our discussions with the NYSE indicated that no amount of minimum expenditure is mandated.

We believe, however, that it would be wise and prudent for boards, management and their audit committees to consider the following factors when allocating resources for an internal audit department.

A. *Results of the entity-level risk assessment*

- What key risks have been identified and how should internal audit be involved in those areas?
- What level of effort does the risk assessment seem to indicate?

B. *Internal audit investment made by comparable companies*

- What is the level of expenditure and effort of similarly sized companies in your industry?
- Are there some obvious differences that would support spending less or more? (For example, obvious or significant differences in business model, organization, degree of centralization or decentralization, regulation and scope of services.)

C. *Preferences of the board and management*

- What role and scope has management and the audit committee established for its internal audit function?

D. *Past, present and future*

- Have there been, are there or will there be events, issues, risks or major changes that would warrant more or less investment in internal audit?

E. *Complementary functions*

- Are there other functions within the company that serve to evaluate key areas and risks objectively, such as:
  - Quality control and loss prevention?
  - Regulatory and legal compliance?
  - Risk management and insurance?
  - Operational and financial control units?

- If so, are these risk mitigation and control efforts already performed to a degree that a professional internal audit function might otherwise perform? Is there inherent conflict of interest in performance feedback for existing functions?
- Have independence and objectivity been considered? (See Questions 1 and 15.)

See Question 12 for additional guidance on what companies should spend on internal audit.

88. What must a company have in place by the effective date of the NYSE rule?

While no specific actions are mandated in the rule itself, we believe that a reasonable approach to compliance by the effective date would include the following steps:

1. Create a written internal audit charter and have it approved, preferably by both the audit committee and the board of directors.
2. Hire a CAE or sign an outsourcing arrangement with an outside organization other than the company's external auditor.
3. Complete an initial risk assessment.

Additionally, we believe it would be desirable to have in place by the effective date or shortly thereafter:

- A formal internal audit plan, responsive to the risk assessment completed and approved by company management and the audit committee.
- As needed, an appropriate level of internal audit staff if the company intends to utilize employee resources, in addition to or in lieu of any outsourced arrangements.

89. Is a formal risk assessment required? Is there a preferred framework to be utilized by the internal audit function, such as the COSO internal control framework and COSO ERM framework?

Again, officials at the NYSE state that the exchange has allowed for listed companies to be able to develop, craft and modify their internal audit functions to meet their specific needs. However, COSO is the current definitive standard for public companies to follow in connection with Section 404. (See Question 30.)

The NYSE believes each listed company should determine the most effective and practical way to accomplish internal audit activities, including the risk-assessment process. The COSO ERM framework (see Question 33) is one framework available to companies, but there are other acceptable and appropriate frameworks and approaches to risk assessment that can be equally or even more effective in certain circumstances, based upon the size, industry and nature of an organization.

90. What other authoritative views strongly recommend the establishment of an independent internal audit function?

Perhaps the most relevant and timely organization strongly advocating internal audit functions is the PCAOB. In AS5, the PCAOB notes numerous times the existence of and potential reliance on the work of internal auditors.

In addition, in a speech on February 11, 2004, at the 22nd Annual Institute of Federal Securities, PCAOB board member Daniel L. Goelzer stated, referring to the proposing release (exposure draft): "The [standard] permits the auditor in some circumstances to rely on central testing performed by company personnel, particularly internal auditors who are adequately funded and independent of management … The proposal tries to strike a balance in a way that will encourage strong and independent internal audit functions."

A number of well-recognized organizations have issued comments about the desirability of forming and maintaining an effective internal audit function:

- The COSO internal controls framework describes the internal audit function as a critical component of monitoring and evaluating the management control structure.
- According to the National Commission on Fraudulent Financial Reporting (Treadway Commission), "All public companies must have an effective and objective internal audit function."
- The Conference Board's "Commission on Public Trust and Private Enterprise" recommends, through release of an analysis designed to address recent corporate scandals and decline of confidence in United States capital markets, that:

  All companies should have an internal audit function, regardless of whether it is an in-house function or one performed by an outside accounting firm (or other outside provider) that is not the firm that acts as the company's regular outside auditor.

  – The internal auditors should prepare for review and approval by the audit committee a multi-year audit plan of not less than three years centered on the corporation's risks and vulnerabilities.

  – The audit committee and any other committee on the board dealing with risk management should review and update this risk-based plan on an annual basis.

  – The Conference Board, January 2003

- The IIA has previously stated:

  All publicly held companies should establish and maintain an independent, adequately resourced, and competently staffed internal audit function to provide management and the audit committee with ongoing assessments of the organization's risk management processes and the accompanying system of internal control.

Appendix A

The IIA Practice Advisory 1000-1: Internal Audit Charter

Interpretation of Standard 1000 from the International Standards for the Professional Practice of Internal Auditing:

Related Standard

1000 Purpose, Authority, and Responsibility

The purpose, authority, and responsibility of the internal audit activity should be formally defined in a charter, consistent with the *Standards*, and approved by the board.

Nature of this Practice Advisory: Internal auditors should consider the following suggestions when adopting an internal audit charter. This guidance is not intended to represent all the considerations that may be necessary when adopting a charter, but simply a recommended set of items that should be addressed.

1. The purpose, authority, and responsibility of the internal audit activity should be defined in a charter. The chief audit executive (CAE) should seek approval of the charter by senior management as well as acceptance by the board. The approval of the charter should be documented in the governing body minutes. The charter should (a) establish the internal audit activity's position within the organization; (b) authorize access to records, personnel, and physical properties relevant to the performance of engagements; and (c) define the scope of internal audit activities.
2. The internal audit activity's charter should be in writing. A written statement provides formal communication for review and approval by management and for acceptance by the board. It also facilitates a periodic assessment of the adequacy of the internal audit activity's purpose, authority, and responsibility. Providing a formal, written document containing the charter of the internal audit activity is critical in managing the auditing function within the organization. The purpose, authority, and responsibility should be defined and communicated to establish the role of the internal audit activity and to provide a basis for management and the board to use in evaluating the operations of the function. If a question should arise, the charter also provides a formal, written agreement with management and the board about the role and responsibilities of the internal audit activity within the organization.
3. The CAE should periodically assess whether the purpose, authority, and responsibility, as defined in the charter, continue to be adequate to enable the internal audit activity to accomplish its objectives. The result of this periodic assessment should be communicated to senior management and the board.

Appendix B

Internal Audit Charter – Sample

Source: The Institute of Internal Auditors (www.theiia.org)

Mission and Scope of Work

The mission of the internal auditing department is to provide independent, objective assurance and consulting services designed to add value and improve the organization's operations. It helps the organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

The scope of work of the internal auditing department is to determine whether the organization's network of risk management, control, and governance processes, as designed and represented by management, is adequate and functioning in a manner to ensure:

- Risks are appropriately identified and managed.
- Interaction with the various governance groups occurs as needed.
- Significant financial, managerial, and operating information is accurate, reliable, and timely.
- Employee's actions are in compliance with policies, standards, procedures, and applicable laws and regulations.
- Resources are acquired economically, used efficiently, and adequately protected.
- Programs, plans, and objectives are achieved.
- Quality and continuous improvement are fostered in the organization's control process.
- Significant legislative or regulatory issues impacting the organization are recognized and addressed properly.

Opportunities for improving management control, profitability, and the organization's image may be identified during audits. They will be communicated to the appropriate level of management.

Accountability

The chief audit executive (CAE), in the discharge of his/her duties, shall be accountable to management and the audit committee to:

- Provide annually an assessment on the adequacy and effectiveness of the organization's processes for controlling its activities and managing its risks in the areas set forth under the mission and scope of work.
- Report significant issues related to the processes for controlling the activities of the organization and its affiliates, including potential improvements to those processes, and provide information concerning such issues through resolution.
- Provide information periodically on the status and results of the annual audit plan and the sufficiency of department resources.
- Coordinate with and provide oversight of other control and monitoring functions (risk management, compliance, security, legal, ethics, environmental, external audit).

Independence

To provide for the independence of the internal auditing department, its personnel report to the CAE, who reports administratively to the chief executive officer and functionally to the board and audit committee in a manner outlined in the above section on Accountability. It will include as part of its reports to the audit committee a regular report on internal audit personnel.

Responsibility

The CAE and staff of the internal auditing department have responsibility to:

- Develop a flexible annual audit plan using appropriate risk-based methodology, including any risks or control concerns identified by management, and submit that plan to the audit committee for review and approval.
- Implement the annual audit plan, as approved, including, and as appropriate, any special tasks or projects requested by management and the audit committee.
- Maintain a professional audit staff with sufficient knowledge, skills, experience, and professional certifications to meet the requirements of this Charter.

- Establish a quality assessment program by which the CAE assures the operation of internal auditing activities.
- Perform consulting services, beyond internal auditing's assurance services, to assist management in meeting its objectives. Examples may include facilitation, process design, training, and advisory services.
- Evaluate and assess significant merging/consolidating functions and new or changing services, processes, operations, and control processes coincident with their development, implementation, and/or expansion.
- Issue periodic reports to the audit committee and management summarizing results of audit activities.
- Keep the audit committee informed of emerging trends and successful practices in internal auditing.
- Provide a list of significant measurement goals and results to the audit committee.
- Assist in the investigation of significant suspected fraudulent activities within the organization and notify management and the audit committee of the results.
- Consider the scope of work of the external auditors and regulators, as appropriate, for the purpose of providing optimal audit coverage to the organization at a reasonable overall cost.

Authority

The CAE and staff of the internal auditing department are authorized to:

- Have unrestricted access to all functions, records, property, and personnel.
- Have full and free access to the audit committee.
- Allocate resources, set frequencies, select subjects, determine scopes of work, and apply the techniques required to accomplish audit objectives.
- Obtain the necessary assistance of personnel in units of the organization where they perform audits, as well as other specialized services from within or outside the organization.

The CAE and staff of the internal auditing department are not authorized to:

- Perform any operational duties for the organization or its affiliates.
- Initiate or approve accounting transactions external to the internal auditing department.
- Direct the activities of any organization employee not employed by the internal auditing department, except to the extent such employees have been appropriately assigned to auditing teams or to otherwise assist the internal auditors.

Standards of Audit Practice

The internal auditing department will meet or exceed the *International Standards for the Professional Practice of Internal Auditing* of The Institute of Internal Auditors.

_____

Chief Audit Executive

_____

Chief Executive Officer

_____

Audit Committee Chair

_____

Dated

Appendix C
Establishing an Internal Audit Shop

Source: http://www.theiia.org/guidance/additional-resources/corporate-governance/?search=establishing%20an%20audit%20shop&C=859&I=2477

Have you ever been asked to set up a new internal audit department? The following suggestions and resources can help you get started.

Step 1:

Establish the authority of the internal audit activity and review the new definition of internal auditing and the *International Standards for the Professional Practice of Internal Auditing (Standards)* to become familiar with what is required.

Step 2:

Interview senior management and board of directors/audit committee [chairpersons] to build rapport, to ensure those at the top have a clear picture of the internal audit function, and to clarify expectations of all. Use this opportunity to quickly learn and address what management and the board view as the greatest risks to the organization, while keeping in mind issues, problems, and opportunities that have already been identified. Develop a system for cataloging such information, including date and name of person interviewed for quick reference in the future. There are many considerations that should be evaluated in determining the optimal structure and source for internal auditing resources. Those responsible for making such determinations should evaluate the additional guidance and considerations outlined in The IIA position paper "Resourcing Alternatives in the Internal Audit Function."

Step 3:

Obtain and review the audit committee charter. Of course, no sample charter encompasses all activities that might be appropriate to a particular audit committee, nor will all activities identified in a sample charter be relevant to every committee. Accordingly, this charter must be tailored to each committee's needs and governing rules.

Step 4:

Understand "benchmarking" needs, i.e., industry, specialty groups, organizations with same staff size, etc. Ask senior management who they consider to be leaders and laggards in your organization's market niche. Check out IIA's GAIN services. Review past GAIN surveys.

Step 5:

Obtain and review your organization's written policies and procedures, especially the policy pertaining to management's responsibility to control the organization.

Step 6:

Discuss with external auditors open and closed internal control issues, which they may have identified during their reviews.

Step 7:

Start to develop the "audit universe," or the list of all auditable entities.

Step 8:

Map the major processes/operations within the organization. Meet with operations managers, including those in information technology, in order to understand their risks and concerns.

Step 9:

Develop a risk assessment for your organization. This should be a macro-level assessment, which includes both external and internal risk factors.

Step 10:

Develop a charter for Internal Audit. Ensure that both senior management and the audit committee review and approve the charter. Information on audit charters can be found within the *Professional Practices Framework* or Establishing an Internal Audit Activity Manual. Additional samples are provided below.

Step 11:

Build the budget, including personnel and travel.

Step 12:

Based on your risk assessment, develop an audit plan. The amount of the plan that can be accomplished in the allotted time period (usually a year) will depend on the risks identified and the internal audit resources and staff. You should always leave time in your audit plan for management requests (usually 10 percent).

Step 13:

Hire your staff and develop a plan for staff training. Ensure your staff covers the range of expertise needed based on your risk assessment. You may also consider outsourcing portions of your audit plan to outside service providers or using professionals internal to the organization. Additional information is available within The IIA's Resourcing Alternatives for the Internal Audit Function.

Step 14:

Ensure that senior management notifies other departments of your existence and calls for complete cooperation. (The IIA has complimentary brochures, such as "All in a Day's Work," "Adding Value Across the Board", and "Guidance for the Profession.") Become familiar with The IIA's Web site and use the search feature on its home page to help you identify valuable resources.

Step 15:

Work with management to establish best-practice reporting relationships, to ensure internal audit is promoted throughout the organization, and to develop a methodology for following up on audit recommendations and measuring performance.

Step 16:

Establish a quality assurance program.

Appendix D

Summary Outline of The IIA *Standards*

The IIA *Standards* consist of Attribute Standards, Performance Standards and Implementation Standards. Attribute Standards address the attributes of organizations and individuals performing internal audit services. The Performance Standards describe the nature of internal audit services and provide quality criteria against which the performance of these services can be measured. The Attribute and Performance Standards apply to all internal audit services. The Implementation Standards expand upon the Attribute and Performance Standards, providing the requirements applicable to assurance (A) or consulting (C) activities.

Attribute Standards

1000 – Purpose, Authority, and Responsibility

The purpose, authority, and responsibility of the internal audit activity must be formally defined in an internal audit charter, consistent with the Definition of Internal Auditing, the Code of Ethics, and the *Standards*. The chief audit executive must periodically review the internal audit charter and present it to senior management and the board for approval.

1200 – Proficiency and Due Professional Care

Engagements must be performed with proficiency and due professional care.

1300 – Quality Assurance and Improvement Program

The chief audit executive must develop and maintain a quality assurance and improvement program that covers all aspects of the internal audit activity.

Interpretation:

A quality assurance and improvement program is designed to enable an evaluation of the internal audit activity's conformance with the Definition of Internal Auditing and the Standards and an evaluation of whether internal auditors apply the Code of Ethics. The program also assesses the efficiency and effectiveness of the internal audit activity and identifies opportunities for improvement.

Performance Standards

2000 – Managing the Internal Audit Activity

The chief audit executive must effectively manage the internal audit activity to ensure it adds value to the organization.

Interpretation:

The internal audit activity is effectively managed when:

- *The results of the internal audit activity's work achieve the purpose and responsibility included in the internal audit charter;*
- *The internal audit activity conforms with the Definition of Internal Auditing and the Standards; and*
- *The individuals who are part of the internal audit activity demonstrate conformance with the Code of Ethics and the Standards.*

2100 – Nature of Work

The internal audit activity must evaluate and contribute to the improvement of governance, risk management, and control processes using a systematic and disciplined approach.

2200 – Engagement Planning

Internal auditors must develop and document a plan for each engagement, including the engagement's objectives, scope, timing, and resource allocations.

2300 – Performing the Engagement

Internal auditors must identify, analyze, evaluate, and document sufficient information to achieve the engagement's objectives.

2400 – Communicating Results

Internal auditors must communicate the engagement results.

2500 – Monitoring Progress

The chief audit executive must establish and maintain a system to monitor the disposition of results communicated to management.

2600 – Resolution of Management's Acceptance of Risks

When the chief audit executive believes that senior management has accepted a level of residual risk that may be unacceptable to the organization, the chief audit executive must discuss the matter with senior management. If the decision regarding residual risk is not resolved, the chief audit executive must report the matter to the board for resolution.

GLOSSARY

Charter – The internal audit charter is a formal document that defines the internal audit activity's purpose, authority, and responsibility. The internal audit charter establishes the internal audit activity's position within the organization; authorizes access to records, personnel, and physical properties relevant to the performance of engagements; and defines the scope of internal audit activities.

Code of Ethics – The Code of Ethics of The Institute of Internal Auditors (IIA) are Principles relevant to the profession and practice of internal auditing, and Rules of Conduct that describe behavior expected of internal auditors. The Code of Ethics applies to both parties and entities that provide internal audit services. The purpose of the Code of Ethics is to promote an ethical culture in the global profession of internal auditing.

Consulting Services – Advisory and related client service activities, the nature and scope of which are agreed with the client, are intended to add value and improve an organization's governance, risk management, and control processes without the internal auditor assuming management responsibility. Examples include counsel, advice, facilitation, and training.

Governance – The combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives.

Residual Risk – The risk remaining after management takes action to reduce the impact and likelihood of an adverse event, including control activities in responding to a risk.

Appendix E
The IIA Code of Ethics

Introduction

The purpose of The Institute's Code of Ethics is to promote an ethical culture in the profession of internal auditing.

> 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.

A code of ethics is necessary and appropriate for the profession of internal auditing, founded as it is on the trust placed in its objective assurance about risk management, control, and governance. The Institute's Code of Ethics extends beyond the definition of internal auditing to include two essential components:

1. Principles that are relevant to the profession and practice of internal auditing;
2. Rules of Conduct that describe behavior norms expected of internal auditors. These rules are an aid to interpreting the Principles into practical applications and are intended to guide the ethical conduct of internal auditors.

The Code of Ethics together with The Institute's Professional Practices Framework and other relevant Institute pronouncements provide guidance to internal auditors serving others. "Internal auditors" refers to Institute members, recipients of or candidates for IIA professional certifications, and those who provide internal auditing services within the definition of internal auditing.

Applicability and Enforcement

This Code of Ethics applies to both individuals and entities that provide internal auditing services.

For Institute members and recipients of or candidates for IIA professional certifications, breaches of the Code of Ethics will be evaluated and administered according to The Institute's Bylaws and Administrative Guidelines. The fact that a particular conduct is not mentioned in the Rules of Conduct does not prevent it from being unacceptable or discreditable, and therefore, the member, certification holder, or candidate can be liable for disciplinary action.

Principles

Internal auditors are expected to apply and uphold the following principles:

Integrity

The integrity of internal auditors establishes trust and thus provides the basis for reliance on their judgment.

Objectivity

Internal auditors exhibit the highest level of professional objectivity in gathering, evaluating, and communicating information about the activity or process being examined. Internal auditors make a balanced assessment of all the relevant circumstances and are not unduly influenced by their own interests or by others in forming judgments.

Confidentiality

Internal auditors respect the value and ownership of information they receive and do not disclose information without appropriate authority unless there is a legal or professional obligation to do so.

Competency

Internal auditors apply the knowledge, skills, and experience needed in the performance of internal auditing services.

Rules of Conduct

1. Integrity

Internal auditors:

1.1. Shall perform their work with honesty, diligence, and responsibility.

1.2. Shall observe the law and make disclosures expected by the law and the profession.

1.3. Shall not knowingly be a party to any illegal activity, or engage in acts that are discreditable to the profession of internal auditing or to the organization.

1.4. Shall respect and contribute to the legitimate and ethical objectives of the organization.

2. Objectivity

Internal auditors:

2.1. Shall not participate in any activity or relationship that may impair or be presumed to impair their unbiased assessment. This participation includes those activities or relationships that may be in conflict with the interests of the organization.

2.2. Shall not accept anything that may impair or be presumed to impair their professional judgment.

2.3. Shall disclose all material facts known to them that, if not disclosed, may distort the reporting of activities under review.

3. Confidentiality

Internal auditors:

3.1. Shall be prudent in the use and protection of information acquired in the course of their duties.

3.2. Shall not use information for any personal gain or in any manner that would be contrary to the law or detrimental to the legitimate and ethical objectives of the organization.

4. Competency

Internal auditors:

4.1. Shall engage only in those services for which they have the necessary knowledge, skills, and experience.

4.2. Shall perform internal auditing services in accordance with the *International Standards for the Professional Practice of Internal Auditing*.

4.3. Shall continually improve their proficiency and the effectiveness and quality of their services.

Appendix F
Internal Audit–Related Organizations and Links

The Institute of Internal Auditors	www.theiia.org
The Institute of Internal Auditors IT Audit	www.itaudit.org
American Institute of CPAs	www.aicpa.org
Financial Accounting Standards Board	www.fasb.org
American Accounting Association	www.aaa-edu.org
Chief Financial Officers Council	www.cfoc.gov
Association of Inspectors General	www.inspectorsgeneral.org
Government Accountability Office	www.gao.gov
Information Systems Audit and Control Association	www.isaca.org
Institute of Management Accountants	www.imanet.org
Institute of Management and Administration	www.ioma.com
International Federation of Accountants	www.ifac.org
Canadian Institute of Chartered Accountants	www.cica.ca
Association of Certified Fraud Examiners	www.cfenet.com
Association of Healthcare Internal Auditors	www.ahia.org
Association of Public Pension Fund Auditors	www.appfa.org
Association of College and University Auditors	www.acua.org
Corporate Executive Board	www.executiveboard.com
MIS Training Institute	www.misti.com
Financial Executives International	www.financialexecutives.org
The ISO 27000 Directory	www.27000.org
U.S. Securities and Exchange Commission	www.sec.gov
Public Company Accounting Oversight Board	www.pcaobus.org
Committee of Sponsoring Organizations of the Treadway Commission (COSO)	www.coso.org

Other Online Resources

www.knowledgeleader.com – 30-day free trials are available to this unique online service providing information, tools, templates and other resources to those involved with internal audit, security and other business and technology risk issues.

www.auditnet.org – Auditnet is an electronic resource for the worldwide audit community. Its purpose is to provide auditors with access to their peers around the world as well as provide access to relevant information vital to the auditing industry.

www.accounting.rutgers.edu – Audit-related mailing lists and links to audit resources.

Appendix G

The IIA's Internal Auditing Education Partnership (IAEP)

The IIA sponsors The Internal Auditing Education Partnership (IAEP) to respond to the growing interest in internal audit education at institutions of higher learning. The IAEP is designed to support universities and colleges at three levels of participation: Center for Internal Auditing Excellence, Partner, and Basic. At each level, the school receives a distinct amount of support and resources, and in return must meet specific requirements. There are IAEP schools throughout the United States and in China, France, Lebanon, Malaysia, the Netherlands, South Africa, Thailand, and the United Kingdom.

A list of IAEP schools, including contact information and website links, follows:

(Source: www.theiia.org/guidance/academic-relations/iaaaf/iaep-schools/)

Centers for Internal Auditing Excellence

A Center for Internal Audit Excellence is committed to sustaining a comprehensive internal audit program. All educators must be Certified Internal Auditors (CIA). All students in the program will be required to sit for the CIA exam and are encouraged to participate in an internship as part of their course of study.

Erasmus Universiteit Rotterdam
The Netherlands
Ron de Korte, RA, RE, RO, CIA
E-mail: r.de.korte@acs.nl
Website: www.esaa.nl/opl/postinit/ioa/index.htm

Louisiana State University
United States
Glenn E. Sumners, DBA, CIA
E-mail: gsumners@hotmail.com
Website: www.bus.lsu.edu/centers/cia/

University of Pretoria
South Africa
Philna Coetzee
E-mail: philna.coetzee@up.ac.za
Website: http://web.up.ac.za/default.asp?ipkCategoryID=484

University of Texas – Dallas
United States
Mark Salamasick, CIA, CISA, CSP
E-mail: Mark.Salamasick@utdallas.edu
Website: http://som.utdallas.edu/iaep/index.htm

Universiteit van Amsterdam
The Netherlands
A.J.G. Driessen, RO, CIA
E-mail: a.j.g.driessen@uva.nl
Website: www.abs.uva.nl/emia/home.cfm

Partner

Schools at the Partner Level offer an internal audit curriculum to students in various educational disciplines.

Bentley College
United States
Priscilla A. Burnaby, Ph.D.
E-mail: pburnaby@bentley.edu
Website: www.bentley.edu/accountancy/programs.cfm

Birmingham City University
United Kingdom
Robin Pritchard
E-mail: robin.pritchard@bcu.ac.uk
Website: www.business.uce.ac.uk/

Bradley University
United States
Simon Petravick
E-mail: simonp@bradley.edu
Website: www.bradley.edu/fcba/undergraduate/accounting/index.shtml

Chulalongkorn University
Thailand
Dr. Pornanong Budsaratragoon
E-mail: pornanong@acc.chula.ac.th
Website: www.chula.ac.th/cuweb_en/

Eastern Michigan University
United States
Robert Okopny, Ph.D., CIA
E-mail: robert.okopny@emich.edu
Website: www.accfin.emich.edu/degree.html

Nanjing Audit University
China
Dr. Shi Xian
E-mail: Xianshixian001@yahoo.com.cn
Website: http://english.nau.edu.cn/index.jsp

Northern Illinois University
United States
David Sinason, Ph.D.
E-mail: dsinason@niu.edu
Website: www.cob.niu.edu/

Old Dominion University
United States
Douglas E. Ziegenfuss, Ph.D., CIA
E-mail: dziegenf@odu.edu
Website: http://bpa.odu.edu

Pittsburg State University
United States
Rebekah Heath, Ph.D., CIA, CPA
E-mail: rheath@pittstate.edu
Website: www.pittstate.edu/acctg/programs.html

University at Buffalo
United States
Alex Ampadu
E-mail: ampadu@buffalo.edu
Website: http://academicprograms.buffalo.edu/mgtbp.php

Université Aix-Marseille
France
Jacques Vera, Ph.D.
E-mail: jacques.vera@iae-aix.com
Website: www.iae-aix.com/

University of Alabama at Birmingham
United States
Deborah W. Tanju, Ph.D., CIA
E-mail: dtanju@uab.edu
Website: www.business.uab.edu//

University of New Orleans
United States
Joyce C. Lambert, Ph.D.
E-mail: jlambert@uno.edu
Website: http://business.uno.edu/acct/

University of North Texas
United States
Raymond Clay, DBA, CPA
E-mail: clay@unt.edu
Website: www.unt.edu/pais/insert/ubusiness.htm

University of Pisa
Italy
Giuseppe D'Onza
E-mail: gdonza@ec.unipi.it
Website: www.masteraudit.it/

University of South Africa
South Africa
Prof. J.J. (Kobus) Wentzel
E-mail: WENTZJJ@unisa.ac.za
Website: www.unisa.ac.za/Default.asp?Cmd=ViewContent&ContentID=189

University of Tennessee
United States
Jack E. Kiger, Ph.D.
E-mail: jkiger@utk.edu
Website: http://bus.utk.edu/undergrad

University of Texas – Austin
United States
Urton L. Anderson, Ph.D., CIA
E-mail: urton@mail.utexas.edu
Website: www.mccombs.utexas.edu/dept/accounting

Basic

Schools at the Basic Level include internal audit components in their programs.

Baruch College
United States
Jan Sweeney
E-mail: Jan_Sweeney@baruch.cuny.edu
Website: www.baruch.cuny.edu/ugradprograms/acc.htm

Boise State University
United States
Thomas English
E-mail: tenglish@boisestate.edu
Website: http://ac.boisestate.edu/

California State University – San Bernardino
United States
Linvol G. Henry, M.S., CPA
E-mail: lhenry@csusb.edu
Website: www.cbpa.csusb.edu/

Cleveland State University
United States
Heidi Hylton Meier, DBA
E-mail: h.meier@csuohio.edu
Website: www.csuohio.edu/academic/majors/accounting.html

Florida Atlantic University
United States
Alan Friedberg, Ph.D.
E-mail: friedber@fau.edu
Website: www.business.fau.edu

Grand Valley State University
United States
David Cannon
E-mail: cannond@gvsu.edu
Website: www.gvsu.edu/business/index.cfm?id=000E578C-F8CB-1EDD-993580E715660000

Indiana University – Purdue University Indianapolis
United States
Eric Johnson
E-mail: erijohns@iu.edu
Website: http://kelly.iupui.edu/home.cfm

Kennesaw State University
United States
Richard Clune
E-mail: rclune@kennesaw.edu
Website: http://coles.kennesaw.edu/KSUColes

Missouri State University
United States
M. Virginia Cerullo, Ph.D.
E-mail: MVCerullo@MissouriState.edu
Website: www.missouristate.edu/registrar/dept_ac.html

San Francisco State University
United States
John J. O'Shaughnessy, Ph.D., CIA
E-mail: joshaun@sfsu.edu
Website: http://cob.sfsu.edu/cob/index.cfm

Southern Illinois University – Carbondale
United States
Marcus Odom
E-mail: modom@cba.siu.edu
Website: www.siu.edu/pres/int_audit.html/

Texas A&M University
United States
L. Murphy Smith, DBA, CPA
E-mail: Lmsmith@tamu.edu
Website: http://acct.tamu.edu/smith/eiap.htm

Tshwane University of Technology
South Africa
Houdini Fourie
E-mail: fourieh@tut.ac.za
Website: www.tut.ac.za/Students/facultiesdepartments/EconomicsFinance/departments/Documents/auditing.pdf

University of Malaya
Malaysia
Nurmazilah Mahzan
E-mail: nurmazilah@um.edu.my
Website: www.um.edu.my/

University of Texas at Arlington
United States
Martin Taylor, Ph.D.
E-mail: mtaylor@uta.edu
Website: www.uta.edu/business/

Valdosta State University
United States
Leisa Marshall
E-mail: lmarshal@valdosta.edu
Website: www.valdosta.edu/lcoba/acctfin/current.shtml

Widener University
United States
Lori Fuller, Ph.D.
E-mail: lrfuller@mail.widener.edu
Website: www.widener.edu/sba

Appendix H
About The Institute of Internal Auditors

Established in 1941, The IIA serves approximately 150,000 members in internal auditing, governance and internal control, IT audit, education, and security worldwide. The world's leader in certification, education, research, and technological guidance for the profession, The Institute serves as the profession's watchdog and resource on significant auditing issues around the globe.

Presenting important conferences and seminars for professional development, producing leading-edge educational products, certifying qualified auditing professionals, providing quality assurance reviews and benchmarking, and conducting valuable research projects through The IIA Research Foundation are just a few of The Institute's many activities.

The IIA also provides internal audit practitioners, executive management, boards of directors and audit committees with standards, guidance, and information on best practices in internal auditing.

The Institute is a dynamic international organization that meets the needs of a worldwide body of internal auditors. The history of internal auditing has been synonymous with that of The IIA and its motto, "Progress Through Sharing."

For more information, please contact:
The Institute of Internal Auditors
247 Maitland Ave.
Altamonte Springs
Florida 32701-4201, United States
Phone: +1.407.937.1100
Fax: +1.407.937.1101
www.theiia.org
E-mail: iia@theiia.org

Appendix I
Sample Job Description

Title:
Vice President, Internal Audit

Duties:
The Vice President, Internal Audit reports functionally to both the CEO and the Audit Committee of the Board of Directors. This individual will be responsible for the design and implementation of the Company's worldwide internal audit program. Working with the senior management team, he/she will have primary leadership responsibility to develop and maintain a world-class internal control environment.

This individual must have a proven track record of managing an audit function in a large, complex organization. This individual must have credibility and be viewed as an authoritative source by the senior management team and all of the business operating units.

This individual must be capable of building and leveraging internal and external alliances while driving for results.

Specific responsibilities include:

- Develops and executes a comprehensive audit program that is responsive to the operational, financial and control risks within the Company.
- Presents to the Audit Committee the annual audit plan, including periodic updates of status and changes required in the plan.
- Organizes, directs and controls the Internal Audit department and the work of all internal audit staff.
- Communicates information to and from the Audit Committee and others as appropriate on the executive management team regarding the audit function.
- Works in partnership with Company executives to design and implement cost-effective procedures to ensure that internal controls are effective and to eliminate redundant or inefficient procedures where necessary.
- Determines that the Company's operating units are in compliance with corporate standard operating procedures and other operating policies.
- Disseminates and shares knowledge on best practices to both senior management and the Board's Audit Committee.
- Coordinates scope and coverage with the Company's independent external auditors.
- Recruits, trains and mentors a high-performing organization that will be seen as a superb training group for future Company financial leadership.
- Ensures the Audit function is viewed as a "value add" in helping the organization achieve its operational and financial goals.
- Works with the Vice President and Corporate Controller to satisfy the requirements of Sarbanes-Oxley.
- Reviews existing as well as new products, services and procedures to ensure compliance with appropriate regulatory authorities. Suggests policy and procedure changes or reviews as appropriate.
- Reviews and records actions and plan taken by management to correct conditions reported by audit findings.
- Maintains audit files by documenting the audit procedures used and each of the audit reports completed.
- Investigates potential fraud situations within the organization.

Education:
Undergraduate degree in accounting, finance or other business-related field. A CIA or CPA is required; an advanced degree is highly desirable.

Experience:
The ideal candidate will be a seasoned financial executive with at least ___ years of total business experience, including a proven track record of managing a "Best in Class" audit function, preferably with initial training at a "Big Four" accounting firm. He/she must be technically strong especially in operating finance and processes to enable him/her to conduct operational and financial audits effectively.

Experience working with government contracts or in a regulated environment is preferred. This individual must possess strong communication skills and executive presence as demonstrated through crisp writing, speaking and thinking. He/she must be comfortable and credible presenting to senior management and the Board of Directors. The successful candidate must be a high potential executive with the ability to build, develop and motivate a first-rate audit capability.

Key Assessment Criteria:

- Outstanding financial acumen blended with business partnership and leadership
- Ability to provide sound business judgment, strategic thinking, and broad financial and business perspective across the organization
- Highly refined analytical skills to quickly review and analyze business processes to identify control deficiencies as well as business operating problems and opportunities
- Strong and engaging presence, inspiring a spirit of cooperation among the management team and all outside constituencies
- Demonstrated track record of attention to detail, time management and prioritization skills
- Ability to challenge norms and processes and relentlessly look for ways to add value and position the organization for success
- Thorough understanding of U.S. GAAP, PCAOB and IIA *Standards for the Professional Practice of Internal Auditing*
- Excellent written and verbal communication and presentation skills and the ability to frame and interpret issues for internal clients
- High level of energy and commitment
- Proven track record of process improvement and experience with financial systems and process change initiatives
- Strong organizational and leadership skills with the ability to attract, retain and develop exceptional global talent
- Strong interpersonal skills and teamwork; ability to cope with complexity and change
- Passionate, visionary leader, capable of driving speed and discipline throughout the organization
- High personal standards and professional ethics with a commitment to excellence

Appendix J

Protiviti's Internal Audit Capabilities and Needs Survey

Protiviti conducted its Internal Audit Capabilities and Needs Survey in 2006 and 2007 to determine where internal audit professionals currently see a need for improvement, and how they prioritize those needs. Respondents answered questions in three subject areas: General Technical Knowledge, Audit Process Knowledge, and Personal Skills and Capabilities. Following are the knowledge/skills in each of these areas respondents were asked to assess.

General Technical Knowledge – Issues/Areas of General Knowledge

Standards for the Professional Practice of Internal Auditing (IIA *Standards*)	ISO 9000 (quality management and quality assurance)
COSO internal control framework	Gramm-Leach-Bliley Act (GLBA)*
COSO enterprise risk management framework	Basel II
Fraud Risk Management	Six Sigma
Enterprise Risk Management	Corporate Governance Standards*
PCAOB Auditing Standard No. 5 (An Audit of ICFR That Is Integrated With an Audit of Financial Statements)*	ISO 14000 (environmental management)
Sarbanes-Oxley Section 301 (Complaints regarding accounting, internal controls or auditing matters)*	FDICIA*
Sarbanes-Oxley Section 302 (Disclosure controls and procedures)*	COBIT
Sarbanes-Oxley Section 404 (ICFR)*	ISO 27000 (information security)
SEC Interpretive Guidance for management regarding its evaluation and assessment of ICFR	AU Section 322 – The Auditor's Consideration of the Internal Audit Function in an Audit of Financial Statements
U.S. GAAP	FIN 48 (Tax Uncertainties)
Tax Laws (in your applicable region/country)	Fair Value Accounting (FAS 159, Fair Value *Option for Financial Assets and Liabilities)*
International Financial Accounting Standards (IFRS)	

**or country equivalent*

Audit Process Knowledge – Issues/Areas of General Knowledge

Assessing risk • Entity level • Process, location, transaction level	Use of self-assessment techniques
Audit planning • Entity level • Process, location, transaction level	Conducting opening/closing meetings
Assessing controls design (entity level) • Company-level controls • Monitoring controls • Tone/Soft controls	Developing recommendations
Assessing controls operating effectiveness (entity level) • Company-level controls • Monitoring controls • Tone/Soft controls	Internal quality assessment (ongoing assessment)
Assessing controls design (process level) • Compliance controls • Financial controls • Operational controls	Internal quality assessment (periodic review)
Assessing controls operating effectiveness (process level) • Compliance controls • Financial controls • Operational controls	External quality assessment (IIA Standard 1312)
Auditing IT • Security • Change control • Computer operation • Program development • Continuity	Interviewing
Top-down, risk-based approach to assessing ICFR	Marketing internal audit internally
Operational auditing • Risk-based approach • Effectiveness, efficiency and economy of operations approach • Value cost improvement and fair characteristics of effective processes	Planning audit strategy
Fraud • Fraud risk management/prevention • Fraud detection/investigation • Monitoring • Auditing	Presenting to senior management
Continuous auditing	Presenting to the audit committee
Data analysis tools • Statistical analysis • Data manipulation • Sampling	Report writing
Computer-Assisted Audit Tools (CAATs)	Resource management (hiring, training, managing)

Personal Skills/Capabilities – Issues/Areas of General Knowledge

Change management	Leveraging others' expertise
Coaching/Mentoring	Negotiation
Creating a learning internal audit function	Personnel performance evaluation
Developing audit committee relationships	Presenting (public speaking)
Developing other board committee relationships	Presenting (small groups)
Developing rapport with senior executives	Persuasion
Developing outside contacts/networking	Strategic thinking
Leadership (within your organization)	Time management
Leadership (within the internal audit profession)	Written communication

Appendix K
NYSE Internal Audit Rule

From Section 303A, which revised the NYSE listing standards to incorporate new corporate governance rules (approved by the SEC on November 4, 2003):

> Every listed company must have an internal audit function.
>
> Commentary: Listed companies must maintain an internal audit function to provide management and the audit committee with ongoing assessments of the company's risk management processes and system of internal control. A company may choose to outsource this function to a third-party service provider other than its independent auditor.

Glossary of Commonly Used Acronyms and Terms

AICPA – The American Institute of Certified Public Accountants.

AMEX – The American Stock Exchange.

Auditing Standard No. 2 (AS2) – Issued by the PCAOB on March 9, 2004, *An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements.* Superseded by Auditing Standard No. 5 (see below).

Auditing Standard No. 5 (AS5) – Issued by the PCAOB on May 24, 2007, *An Audit of ICFR That Is Integrated With an Audit of Financial Statements.*

CAE – Chief audit executive.

CBOK – Common Body of Knowledge. A survey conducted by The IIA Research Foundation focused on the internal audit profession and how the profession is being practiced worldwide.

CIA – Certified Internal Auditor.

CISA – Certified Information Systems Auditor.

CoCo – The Criteria of Control Board of the Canadian Institute of Chartered Accountants (CICA).

COSO – The Committee of Sponsoring Organizations of the Treadway Commission.

COSO ERM framework – The enterprise risk management framework, developed by COSO, bolsters support and extends aspects of the original COSO internal control framework.

COSO Internal Control – Integrated Framework – Developed by COSO, the definitive standard for public companies to follow in connection with Section 404 of the Sarbanes-Oxley Act.

CPE – Continuing professional education.

CSA – Control self-assessment.

ERP – Enterprise resource planning.

FDICIA – Federal Deposit Insurance Corporation Improvement Act.

GAAP – Generally accepted accounting principles.

GAAS – Generally accepted auditing standards.

GAIN – The IIA's Global Auditing Information Network.

GRC – Governance, risk and compliance.

IASB – The IIA's Internal Auditing Standards Board.

ICFR – Internal control over financial reporting. Generally refers to the company's internal control structure and procedures over financial reporting.

The IIA – The Institute of Internal Auditors.

The IIA *Code of Ethics* – The Institute of Internal Auditors' Principles relevant to the profession and practice of internal auditing, and Rules of Conduct that describe the behavior expected of internal auditors.

The IIA *Standards* – The Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*.

IT – Information technology.

NASDAQ – The computerized stock exchange established by the National Association of Securities Dealers.

NYSE – The New York Stock Exchange.

PCAOB – The Public Company Accounting Oversight Board. Established by the Sarbanes-Oxley Act, the PCAOB oversees the audits of the financial statements of public companies through rigorous registration, standard-setting, inspection and disciplinary programs.

Professional Practices Framework – Professional standards promulgated by The IIA consisting of three categories of guidance: *Standards and Code of Ethics*, *Practice Advisories*, and *Development and Practice Aids*.

QAR – Quality assessment review.

Sarbanes-Oxley – The Sarbanes-Oxley Act of 2002 – corporate governance and oversight legislation signed into law on July 30, 2002.

SAS 65 – The AICPA's Statement on Auditing Standards No. 65, *The Auditor's Consideration of the Internal Audit Function in an Audit of Financial Statements*.

SAS 99 – The AICPA's Statement on Auditing Standards No. 99, *Consideration of Fraud in a Financial Statement Audit*.

SEC – The U.S. Securities and Exchange Commission.

SEC interpretive guidance – Provides guidance for management regarding its evaluation and assessment of internal control over financial reporting. The guidance sets forth an approach by which management can conduct a top-down, risk-based evaluation of internal control over financial reporting.

Section 301 – Refers to Section 301 of the Sarbanes-Oxley Act, which addresses public company audit committees.

Section 302 – Refers to Section 302 of the Sarbanes-Oxley Act, which addresses certifications by the principal executive officer (the CEO) and principal financial officer (usually the CFO).

Section 303A – Refers to Section 303A of the New York Stock Exchange Internal Audit Requirement. Section 303A also contains a number of new listing rules related primarily to the board of directors and related board committee issues. See Question 72 for more information.

Section 404 – Refers to Section 404 of the Sarbanes-Oxley Act, which addresses ICFR.

About Protiviti Inc.

Protiviti (**www.protiviti.com**) is a global business consulting and internal audit firm composed of experts specializing in risk, advisory and transaction services. We help solve problems in finance and transactions, operations, technology, litigation, governance, risk, and compliance. Our highly trained, results-oriented professionals provide a unique perspective on a wide range of critical business issues for clients in the Americas, Asia-Pacific, Europe and the Middle East.

Protiviti is proud to be a Principal Partner of The IIA. More than 1,000 Protiviti professionals are active members of The IIA, and these members are involved with local, national and international leadership to provide thought leadership, speakers, best practices, training and other resources that develop and promote the internal audit profession.

Protiviti has more than 60 locations worldwide and is a wholly owned subsidiary of Robert Half International (NYSE symbol: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

Internal Audit Solutions

Protiviti works with companies of virtually any size, public or private, to assist them with their internal audit activities. This can include starting and running the activity for them on a fully outsourced basis or working with an existing internal audit function to supplement their team when they lack adequate staff or skills. Protiviti's services also include providing clients with highly specialized resources such as IT Security, Business Continuity and Fraud Detection, among many others, and assisting with internal audits in multiple countries.

One of Protiviti's key features is that we are not an audit/accounting firm; thus, there is never an independence issue in the work we do for our clients. Protiviti is able to use all of our consultants to work on internal audit projects – this allows us at any time to bring in our best experts in various functional and process areas.

In addition, Protiviti can conduct an independent review of a company's internal audit function – such a review is called for every five years under standards from The Institute of Internal Auditors.

Among the services Protiviti's internal audit practice provides are:

- Audit committee advisory
- Co-sourcing and specialized resource enhancement
- Full outsourcing
- Internal audit technology and tool implementation
- Internal audit quality assessments and readiness reviews
- Internal audit transformation
- Information technology audit services
- Start-up and development advice

For more information about Protiviti's internal audit solutions, please contact:
Robert B. Hirth Jr.
Executive Vice President,
Global Internal Audit
Protiviti Inc.
+1.415.402.3621 (direct)
robert.hirth@protiviti.com

KnowledgeLeader℠ provided by protiviti®

KnowledgeLeader℠ is a subscription-based website that provides information, tools, templates and resources to help internal auditors, risk managers and compliance professionals save time, stay up-to-date and manage business risk more effectively. The content is focused on business risk, technology risk and internal audit, and is updated weekly.

The tools and resources available on KnowledgeLeader include:

- **Audit Programs** – A wide variety of sample internal audit and IT function audit work programs are available on KnowledgeLeader. These work programs, along with the other tools listed below, are all provided in downloadable versions so they can be repurposed for use in your organization.
- **Checklists, Guides and Other Tools** – More than 600 checklists, guides and other tools are available on KnowledgeLeader. They include questionnaires, best practices, templates, charters and more for managing risk, conducting internal audits and leading an internal audit department.
- **Policies and Procedures** – KnowledgeLeader provides more than 200 sample policies to help in reviewing, updating or creating company policies and procedures.
- **Articles and Other Publications** – Informative articles, survey reports, newsletters and booklets produced by Protiviti and other parties (including *Compliance Week* and Auerbach) about business and technology risks, internal audit and finance.
- **Performer Profiles** – Interviews with internal audit executives who share their tips, techniques and best practices for managing risk and running the internal audit function.

Key topics covered by KnowledgeLeader:

- Business Continuity Management
- Control Self-Assessment
- Corporate Governance
- COSO
- Credit and Operational Risk
- Enterprise Risk Management
- Fraud and Ethics
- Internal Audit
- Sarbanes-Oxley Act
- Security Risk
- Technology Risk

KnowledgeLeader has an expanding library of methodologies and models – including the robust Protiviti Risk Model[SM], a process-oriented version of the Capability Maturity Model, the Six Elements of Infrastructure Model, and the Sarbanes-Oxley 404 Service Delivery Model.

With a KnowledgeLeader membership, subscribers have access to AuditNet Premium (Paid) Content; discounted certification exam preparation material from ExamMatrix; discounted MicroMash CPE Courses to maintain your professional certification requirements; audit, accounting and technology standards and organizations; certification and training organizations and information; brief review of applicable laws and regulations; and best business links.

To learn more about KnowledgeLeader, sign up for a complimentary 30-day trial by visiting our website at **www.knowledgeleader.com**. Protiviti clients and alumni, and members of The IIA, ISACA and AHIA, are eligible for a subscription discount. Additional discounts are provided to groups of five or more.

KnowledgeLeader members have the option of upgrading to KLplus[SM] (KL+). KL+ provides all of the benefits of KnowledgeLeader, plus full access to Protiviti's suite of online courses.

Protiviti's Governance Portal for Internal Audit

Protiviti's Internal Audit Portal is a web-based audit management system designed to improve the efficiency and effectiveness of your audit department. The Internal Audit Portal is an electronic work paper package that facilitates the audit process from risk assessment through issue tracking. Our advanced reporting engine will provide transparency, real-time status updates and a streamlined audit reporting experience.

Our clients are able to configure the solution to fit their approach and methodology, positioning both small and large internal audit functions to meet their objectives. When combined with our professionals and content, Protiviti will help you create a personalized response to your audit tool needs.

The Internal Audit Portal is an integrated module within the Protiviti Governance Portal that can be used independently or in conjunction with other modules to create a true governance, risk and compliance (GRC) platform. This enterprise solution allows you to leverage frameworks and build a common language and repository that brings internal audit information into a GRC context. Additional modules of the Governance Portal include:

- **Controls Management** – A framework that supports control documentation (e.g., Sarbanes-Oxley), evaluation, documentation and testing.
- **Risk Management** – A framework for assessing inherent, tolerable, and residual risk across defined enterprise categories.
- **Assessment Management** – An integrated survey engine that supports a sustainable self-assessment process across multiple GRC programs and modules of the Governance Portal.
- **Incident Management** – A system that captures actual, near-miss and potential events that can result in operational and financial losses.

For more information, about Protiviti's Governance Portal for Internal Audit, please contact:

Scott Gracyalny
Managing Director,
Risk Technology Solutions
Protiviti Inc.
+1.312.476.6381 (direct)
scott.gracyalny@protiviti.com

Protiviti Internal Audit Practice – Contact Information

Robert B. Hirth Jr.
Executive Vice President – Global Internal Audit
+1.415.402.3621
robert.hirth@protiviti.com

AUSTRALIA
Garran Duncan
+61.3.9948.1205
garran.duncan@protiviti.com.au

BELGIUM
Carl Messemaeckers van de Graaff
+31.20.346.04.00
carl.messemaeckers@protiviti.nl

BRAZIL
Waldemir Bulla
+55.11.5503.2020
waldemir.bulla@protiviti.com.br

CANADA
Carmen Rossiter
+1.647.288.4917
carmen.rossiter@protiviti.com

CHINA
Philip Yau
+86.755.2598.2086, ext. 888
philip.yau@protiviti.com

FRANCE
Francis Miard
+33.1.42.96.22.77
f.miard@protiviti.fr

GERMANY
Michael Klinger
+49.69.963.768.155
michael.klinger@protiviti.de

INDIA
Adithya Bhat
+91.22.6626.3310
adithya.bhat@protiviti.co.in

ITALY
Giacomo Galli
+39.02.6550.6303
giacomo.galli@protiviti.it

JAPAN
Yasumi Taniguchi
+81.3.5219.6600
yasumi.taniguchi@protiviti.jp

MEXICO
Roberto Abad
+52.55.5342.9100
roberto.abad@protiviti.com.mx

THE NETHERLANDS
Carl Messemaeckers van de Graaff
+31.20.346.04.00
carl.messemaeckers@protiviti.nl

SINGAPORE
Philip Moulton
+65.6220.6066
philip.moulton@protiviti.com

SOUTH KOREA
Sang Wook Chun
+82.2.3483.8200
sangwook.chun@protiviti.co.kr

SPAIN
Diego Rodriguez Roldan
+34.91.206.2000
diego.rodriguezroldan@protiviti.es

UNITED KINGDOM
Dene Burke
+44.20.7389.0426
dene.burke@protiviti.co.uk

UNITED STATES
Robert B. Hirth Jr.
+1.415.402.3621
robert.hirth@protiviti.com

THE AMERICAS

UNITED STATES

Alexandria
Atlanta
Baltimore
Boston
Charlotte
Chicago
Cincinnati
Cleveland
Dallas
Denver
Fort Lauderdale
Houston
Kansas City
Los Angeles
Milwaukee
Minneapolis
New York
Orlando
Philadelphia
Phoenix
Pittsburgh
Portland
Richmond
Sacramento
Salt Lake City
San Francisco
Seattle
Silicon Valley/
Santa Clara
Stamford
St. Louis
Tampa
Vienna
Woodbridge

BRAZIL

São Paulo

CANADA

Kitchener-Waterloo
Toronto

MEXICO

Mexico City

PERU

Lima*

VENEZUELA

Caracas*

EUROPE

BELGIUM

Brussels

FRANCE

Paris

GERMANY

Düsseldorf
Frankfurt
Munich

ITALY

Milan
Rome
Turin

THE NETHERLANDS

Amsterdam

SPAIN

Madrid

UNITED KINGDOM

London

MIDDLE EAST

KUWAIT

Kuwait City*

OMAN

Muscat*

UNITED ARAB EMIRATES

Abu Dhabi*
Dubai*

ASIA-PACIFIC

AUSTRALIA

Brisbane
Canberra
Melbourne
Sydney

CHINA

Beijing
Hong Kong
Shanghai
Shenzhen

INDIA

Mumbai
New Delhi

INDONESIA

Jakarta**

JAPAN

Osaka
Tokyo

SINGAPORE

Singapore

SOUTH KOREA

Seoul

* Protiviti Member Firm
** Protiviti Alliance Member

protiviti®
Risk & Business Consulting.
Internal Audit.

PRO-0209-101015