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**