

# PricewaterhouseCoopers 2007 State of the internal audit profession study: Pressures build for continual focus on risk\*



# Table of contents

Overview	4
To enhance organizational risk management, internal audit must embrace ongoing risk monitoring and frequent enterprise-wide risk assessments.	
<hr/>	
Trends	
1. Pressures build for a continual focus on risk.	9
2. Sarbanes-Oxley demands stabilize at a significant level.	22
3. Lack of capacity and capabilities is a top concern.	30
4. Rotational staffing provides a key source of talent.	32
5. Audit report ratings are popular but present challenges for internal audit.	36
6. Other trends and issues from the 2007 survey.	42
<hr/>	
Methodology	46
Appendix	48

# Overview

To enhance organizational risk management, internal audit must embrace ongoing risk monitoring and frequent enterprise-wide risk assessments.

The ongoing migration to a more risk-based approach to internal audit has spawned a natural evolution with respect to the roles and responsibilities of internal audit and the scope of internal audit activities. A decade ago, only a relative handful of internal audit groups were taking a legitimate risk-based approach to the audit-planning process. Today, there is a growing recognition of the strong link between effective risk assessments and effective audit coverage. To strengthen risk management performance, consider the following six imperatives:

1. Adopt a process approach to risk assessment and planning.
2. Supplement annual risk assessments with quarterly or more frequent updates.
3. Leverage your prior assessment results.
4. Align and leverage risk assessments.
5. Seek out the specialized talent you need.
6. Coordinate effectively with other risk management groups.

In the fourth quarter of 2006, PricewaterhouseCoopers conducted its third State of the Profession survey to capture a current view of the internal audit profession. We discovered that the levels of internal audit resources that are needed to comply with Sarbanes-Oxley legislation have stabilized but that it will be difficult to achieve further reductions in resources. We found that chief audit executives (CAEs) are most concerned with finding sufficient talent to meet stakeholder needs, and that rotational staffing is fast becoming the prevalent staffing model for large corporate internal audit groups. And we developed further insight into the pros and cons of CAEs including ratings and opinions in their audit findings and reports.

**Key indicators:**

1. More than 80% of our survey respondents conduct an annual enterprise-wide risk assessment.
2. Multiple enterprise-wide risk assessments are conducted at one third of our responding organizations. Of this group, only 20% consider these assessments to be well aligned.
3. Seven percent of respondents update their annual enterprise-wide risk assessments more than once a month, 2% update monthly, 16% update quarterly, and 11% update semi-annually. The remaining 64% either update their assessments on an ad hoc basis or lack specific update procedures.
4. In the traditional areas of finance, compliance, and operations, survey respondents express high degrees of confidence in their audit risk coverage. In the critical areas of technology, fraud, and strategy, however, respondents are significantly less confident.

5. Nearly a third of our internal audit respondents are responsible for the enterprise risk management function within their organizations.
6. Forty-one percent of our 2007 respondents dedicated half or more of their internal audit resources to Sarbanes-Oxley Section 404 (S404) compliance in 2006, with 21% devoting 75% or more of their resources to S404.
7. Although only 1% of respondents in our last study anticipated the need to devote all of their resources to S404 in 2006, the actual percentage dedicating 100% to S404 last year was five times that number.
8. Collectively, internal auditors in the United States devote a third or more of their time to addressing the requirements of Sarbanes-Oxley. What's more, nearly a third of respondents expect to devote half or more of their internal audit resources to S404 compliance during 2007.
9. Internal audit groups reporting to CFOs devote more time to Sarbanes-Oxley compliance: 46% of respondents who report administratively to their CFOs spent more than 50% of their audit resources on projects relating to Sarbanes-Oxley in 2006, and 69% of those who report administratively to the level below CFO spent more than 50% of their time on compliance with the Act.

10. When asked to assess their primary challenges in the year ahead, 84% of Fortune 500 respondents rated the ability to recruit necessary talent as a medium to high risk (42% medium and 42% high).
11. More than 80% of our Fortune 500 respondents use some form of rotational staffing in their internal audit function.
12. Fifty-six percent of our respondents as a whole—and 63% of our Fortune 500 respondents—said they routinely include ratings on individual findings in their internal audit reports.
13. Eighty-six percent of our total respondents report functionally to the audit committee or the board; 50% of Fortune 500 respondents report administratively to the CFO or the office of the CFO, as do 47% of respondents overall.
14. Forty-three percent of our 2007 respondents reported using some form of “continuous” auditing or monitoring in their audit operations.

# Trends

## 1. Pressures build for a continual focus on risk.

Risk management has attained a sharply higher profile within the internal audit community as internal auditors have sought to enhance both the risk assessments they use to develop and execute their audit plans and the risk management activities they undertake in their organizations. However, a number of divergent and conflicting trends related to risk assessment and risk management were revealed by our 2007 State of the Profession survey, and are raising concerns. At a time when there is growing appreciation for risk assessments and a growing interest in enterprise risk management (ERM) by both management and internal auditors, there are also some troubling issues with regard to the oversight and implementation of risk management.

More than 80% of the internal auditors responding to our survey conduct enterprise-wide risk assessments as part of their annual internal audit planning processes. What's more, nearly a third of respondents indicate that they are responsible for enterprise risk management at their organizations. While ownership of ERM by internal audit may not be the ideal, the survey results show the degree to which companies are beginning to embrace the concept of ERM to improve performance and profitability, optimize resources, ensure effective reporting, and strengthen compliance with laws and regulations. Above all, the survey confirms the need for internal auditors to focus on risk on an ongoing basis, and to update their enterprise-wide risk assessments quarterly, or more frequently.

# Risk assessment survey highlights

## **Annual risk assessments**

More than 80% of the internal auditors responding to our survey conduct an annual enterprise-wide risk assessment.

## **Multiple risk assessments**

One third of responding internal auditors noted that multiple enterprise-wide risk assessments are being conducted within their organizations. Of this total, however, only 20% consider these multiple assessments to be well aligned.

## **Frequency of updates to risk assessments**

Seven percent of respondents update their annual enterprise-wide risk assessments more than once a month, 2% update monthly, 16% update quarterly, and 11% update semi-annually. The remaining 64% either update their assessments on an ad hoc basis or lack specific update procedures.

## **Confidence in risk coverage**

In the traditional areas of finance, compliance, and operations, survey respondents express high degrees of confidence in their audit risk coverage. In the critical areas of technology, fraud, and strategy, however, respondents are significantly less confident.

## **Enterprise risk management responsibility**

Nearly a third of the internal audit respondents are responsible for the ERM function within their organizations.

### **Immaturity in risk management oversight**

Despite the increased emphasis on ERM that has permeated the corporate sector in recent years, the 2007 State of the Profession survey reflects considerable volatility and uncertainty with respect to the roles and responsibilities of internal audit in the risk management arena.

The survey also reveals a decided lack of consistency in the way risk management is practiced within major US companies, specifically how internal audit functions assess risks and take part in risk management processes. At some companies, internal audit oversees risk management; at other organizations, other functions are responsible for risk management or there is no formal risk management oversight whatsoever.

As a result of such inconsistency, the implementation of risk management at many organizations is immature at best and chaotic at worst. This is particularly true at companies where more than one function conducts risk management activities and where the risk assessments do not align strongly with corporate priorities or with each other. One third of responding companies conduct multiple enterprise-wide risk assessments, and of this group, only 20% consider their multiple risk assessments to be well aligned. Our experience indicates that multiple risk assessments that are not aligned effectively can be confusing for audit committees and the board. In some instances, at organizations where multiple risk assessments are conducted, audit committees have gone so far as to direct those responsible for these disparate risk assessments to coordinate their efforts and deliver a joint presentation of results.

## Growing focus on enhancing risk assessments and risk management

According to IIA Standard 2010,<sup>1</sup> internal audit groups should base their audit plans around risk assessments conducted on an annual or more frequent basis, with input from senior management and the board of directors. Given this mandate, annual risk assessments are considered standard operating procedure for the majority of internal audit functions.

When asked who, if anyone, is conducting an annual risk assessment at their companies, 36% of respondents said internal audit, 12% said the chief risk officer or CRO organization, 13% said internal audit and the CRO function jointly, 15% said another business unit within the company, 6% said the company's external auditors, and 18% said no one. On the plus side, 82% of our 2007 respondents report conducting an annual enterprise-wide risk assessment. At the same time, 18% are not conducting such an assessment, a number we found surprisingly high given that the practice is now a global standard for internal audit functions. In addition, some internal auditors would say that the 6% of assessments being conducted by outside auditors should not be attributed to company totals because they are not performed internally. Under that line of thinking, if the 6% attributed to external audit were combined with the 18% of responding companies not conducting annual enterprise-wide risk assessments, you could conclude that nearly a quarter (24%) of the 717 companies responding to our survey had failed to adopt one of the most basic tenets of our profession.

### Frequency of assessment updates

In an ideal world, an internal audit function will conduct an annual enterprise-wide risk assessment and have a robust process to update that assessment on at least a quarterly basis—the second of the two-step approach that, from our perspective, constitutes a leading practice.

When we asked respondents how often they update or revise their risk assessments, we got a mixed response: 7% said they update continuously, which we defined as more frequent than monthly; 2% said monthly; and 15% said quarterly. Thus a quarter of our respondents have achieved best-in-class designations in terms of the frequency of their assessment updates. Of the remaining three fourths of our respondents, 11% said they update semi-annually; 49% said they update as needed, but at no regular interval; and 15% said they do not update their annual risk assessments at all, a figure that drops to 8% for our Fortune 500 respondents. What is most noteworthy about these responses is that only a handful of respondents update continuously while 64% may be doing little or nothing between annual assessments. That certainly leaves room for improvement given the dynamic nature of risk in our world today.

<sup>1</sup> The International Standards for the Professional Practice of Internal Auditing, ©2007, The Institute of Internal Auditors, Altamonte Springs, Fla.

## Multiple risk assessments

To probe the prevalence of multiple risk assessments, we asked survey respondents if more than one group or department within their companies was conducting annual enterprise-wide risk assessments. One third (33%) said yes, and two thirds (67%) said no. We then asked respondents from companies with more than one risk assessment to indicate how well they thought these multiple risk assessments were aligned with each other. The responses: 20% said they are well aligned and developed in close coordination; 50% said they are somewhat aligned, with results coordinated and differences discussed; and 30% said they are not well aligned, with little or no coordination among the parties making the assessments.

In our view, a company is inviting inefficiencies and possibly missing risks if its enterprise-wide risk assessments are not aligned or integrated. The fact that only 20% of our respondents with multiple risk assessments consider those assessments to be well aligned is a major source of frustration to audit committees, which are losing patience with multiple risk assessments that don't say the same thing. Audit committees at these organizations are well advised to direct those conducting the assessments to coordinate their activities and deliver a joint presentation on the results.

## Varying assessment confidence

One of the most striking findings of our survey is the degree to which levels of assessment confidence among internal auditors can vary by area of focus. We asked respondents to characterize their relative levels of confidence in the effectiveness of their audit coverage when dealing with six different types of risk. In the areas of finance, compliance, and operations—sectors that might be characterized as traditional areas of focus for internal audit—respondents expressed high degrees of confidence, but they were significantly less confident when dealing with risk assessments in the areas of technology, fraud, and strategic or business risks. The specific responses, by area, were as follows:

- **Finance**—64% very confident; 33% somewhat confident; 3% not confident
- **Compliance**—49% very confident; 46% somewhat confident; 5% not confident
- **Operations**—43% very confident; 49% somewhat confident; 8% not confident
- **Technology**—33% very confident; 50% somewhat confident; 17% not confident
- **Fraud**—29% very confident; 63% somewhat confident; 8% not confident
- **Strategic/business**—20% very confident; 50% somewhat confident; 30% not confident

## Strong interest in enterprise risk management

According to our survey, 32% of respondents are responsible for ERM at their organizations in addition to their traditional internal audit responsibilities. In one sense, this figure is not surprising, for at major companies in particular, the experience/expertise needed to understand, identify, evaluate, catalog, and monitor risk rests largely with internal audit. At companies where internal audit has overall responsibility for ERM, you also tend to find that there is no chief risk officer or other function charged with risk management.

Our 2007 State of the Profession survey indicates that internal auditors take a fairly basic approach to risk management and that the processes to address risk management are relatively immature. This is a clear indication that the COSO<sup>2</sup> ERM guidelines launched in 2004 have yet to gain significant traction within organizations. The COSO ERM *Framework*,<sup>3</sup> written for COSO by PricewaterhouseCoopers, provides direction for businesses and other organizations seeking to leverage the principles of ERM.<sup>4</sup> It defines enterprise risk management, creates a foundation for mutual understanding of ERM issues, and provides a standard against which organizations can compare their approaches to enterprise risk management. In addition, the COSO ERM *Framework* incorporates the provisions of *Internal Control—Integrated Framework*, developed by COSO in 1992 to help companies assess and enhance their internal control systems.

In business today, you don't often hear internal auditors talking about risk appetites and portfolio risks, or using other language associated with the COSO ERM *Framework*. At the same time, it took a decade for the corporate community to view the COSO internal control framework as an effective means to define and evaluate internal controls.

<sup>2</sup> The Committee of Sponsoring Organizations of the Treadway Commission.

<sup>3</sup> *Enterprise Risk Management—Integrated Framework*.

<sup>4</sup> With the COSO ERM *Framework*, an organization can analyze the effectiveness of its ERM activities by assessing the relationships between the *Framework's* four categories of objectives—strategic, operations, reporting, and compliance—and its ERM components, the elements needed to achieve organizational objectives. COSO's eight key interrelated components of effective ERM are: the internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, and monitoring.

## Enterprise risk management is top priority with multinationals

What we do know now is that risk management is becoming a top-of-mind topic in corporate America. According to PricewaterhouseCoopers' Management Barometer, a quarterly survey of senior executives, 83% of large US-based multinationals place ERM among their top ten priorities. In most (63%) of the businesses surveyed in the fall of 2006, the CEO (26%) or CFO (52%) has primary responsibility for ERM. Of note, when either the CEO or CFO is responsible for enterprise risk management, ERM was found to be positioned even more highly, with 37% of respondents from these companies rating ERM as a top-five corporate priority, versus 20% at companies where a person with a lesser title is primarily responsible.

Despite the unquestioned promise of enterprise risk management, the results of the PwC Management Barometer survey focusing on ERM confirm that senior executives perceive a number of significant challenges in their efforts to leverage ERM's potential. These challenges include difficulty in quantifying risks, a conflict in corporate priorities, and difficulty identifying and/or measuring ERM benefits. Perceived obstacles also include difficulty embedding risk management into different cultures and behaviors, difficulty integrating risk management into business processes, and lack of clarity with respect to risk management roles and responsibilities.

## Benefits of enterprise risk management

As outlined in *Enterprise Risk Management—Integrated Framework*, published by COSO in 2004, ERM provides the foundation for management to deal more effectively with uncertainty and risks and to build value. As a key strategic enabler, ERM can help management:

- **Align its risk appetite and strategy**—With ERM, management can take an entity's risk appetite into consideration when evaluating strategic alternatives, setting related objectives, and developing mechanisms to manage related risks.
- **Enhance its risk-response decisions**—ERM can provide a rigorous framework from which to select alternative responses to risk, from avoidance and reduction to sharing and acceptance.
- **Reduce operational surprises and losses**—ERM can strengthen the ability of management to identify potential events and establish responses, as well as reduce surprises and associated costs or losses.
- **Identify and manage both cross-enterprise and multiple risks**—Every enterprise faces a host of risks, on either a focused or an enterprise-wide basis. With ERM, management is better prepared to develop integrated responses to cross-enterprise or multiple risks.
- **Seize opportunities**—By considering a full range of potential events, management is in a stronger position to identify, pursue, and realize opportunities.
- **Improve capital deployment**—With better risk information, management can more effectively assess capital needs and enhance capital allocation.

### **Six imperatives for more effective risk assessments**

The move to risk-based internal auditing has led to a natural evolution in the scope of internal audit activities. Although only a small number of internal audit groups were taking a significant risk-based approach to auditing a decade ago, the strong link between effective risk assessments and effective audit coverage is widely recognized today. There is also recognition that internal auditors can facilitate a greater understanding of risk management processes and issues among their executive management groups and audit committees.

At the same time, there is a significant gap between high-performing internal audit functions doing many things well and other internal audit groups struggling with day-to-day compliance—which points to the need for many organizations to strengthen their risk management efforts. At nearly a fifth of the organizations involved in our survey, no one is conducting risk assessments. That’s unacceptable, given the work done by the IIA, COSO, and others to pave the way for superior internal audit performance in addressing risks. Internal auditors in the United States need to step up to make better use of their resources, do a better job of informing their audit committees, and avoid duplication of effort.

To strengthen your performance in the risk management arena, consider the following six imperatives:

1. Adopt a process approach to risk assessment and planning

To meet rising stakeholder expectations, you need to keep the audit committee and senior management well informed about your changing risk exposure and positions. This requires a process-driven rather than an event-driven approach to risk assessment, as well as flexible adjustments to your audit plan based on the results of this process-driven approach. You also need to believe that it is a core responsibility of internal audit to maintain an *ongoing focus* on risk and on changes to the organizational risk profile, as opposed to focusing on risk issues only during the annual audit planning process.

2. Supplement annual risk assessments with quarterly or more frequent updates

High-performance auditing requires both an annual risk assessment and regular assessment updates, ideally on a quarterly or more frequent basis. Of our 2007 survey respondents, only a quarter achieved this status. Neither once-a-year risk assessments nor periodic, ad hoc updates are enough to keep up with today's dynamic risk environment. You need to monitor risks on a regular, ongoing basis throughout the year so you will know if a previously identified risk has increased in urgency or if a new risk has become a major concern. With defined risk assessment processes, procedures, and enabling technologies, you will know when and where you need to accelerate or defer your audits. You will also be in a better position to detect and assess emerging risks in critical areas.

3. Leverage your prior assessment results

To achieve high-performance auditing, learn from the past and reach out to key players within your company to strengthen your assessment process. In developing annual risk assessments, 14% of our respondents take a zero-based approach to the assessment process, while 86% consider the prior year's results in their planning. Respondents will also typically seek input from multiple sources to strengthen the assessment process. Last year (2006), 95% of our respondents sought input from senior management, 83% from business unit managers, and 44% from external auditors. What's more, 67% of our 2007 respondents validated the preliminary results of their risk assessments with their CRO or another qualified party.

#### 4. Align and leverage risk assessments

When it comes to dealing with the risks facing an organization, audit committees and senior management groups should hear a consistent message. It is difficult enough to manage risks when you know what they are, but when you must deal with multiple assessments with significant variations, the challenge is compounded. A company should, therefore, have a common risk language or framework, with all areas looking at risk “speaking the same language,” and thus leveraging their risk processes and knowledge. If more than one function at your organization is conducting an enterprise-wide risk assessment, work with the audit committee, senior management, and other players in risk management to develop a consistent, integrated approach.

#### 5. Seek out the specialized talent you need

As the State of the Profession survey suggests, chief audit executives are clearly concerned about their abilities to address strategic or business risks as well as risks regarding fraud and technology. To address these risks effectively, you need to adopt a process-based risk assessment mind-set. And you should tap both internal and external sources to expand your capability sets in the critical areas of business, fraud detection, and technology. Specialized help and views from outside the organization can also assist in identifying emerging issues and risks that might not be apparent to those within the organization.

#### 6. Coordinate effectively with other risk management groups

Our survey shows that coordination and information-sharing between internal audit and other groups with risk management responsibilities is minimal, suggesting significant room for improvement. Only 11% of our respondents claim to have developed a well-implemented process for such coordination, with another 38% handling such matters informally. On a positive note, 41% of internal audit respondents say they are actively working to improve the process.

## A risk management checklist for internal audit

Take a process-based approach to risk assessments and audit planning

- Conduct an enterprise-level risk assessment on at least an annual basis.
- Apply risk-based assessment results to the development of annual audit plans and to planning for individual internal audit engagements.
- Adopt a formal process to update or revise your risk assessments on a quarterly or more frequent basis.
- Update or adjust your audit plan to address the results of the risk assessments.
- Conduct a preliminary risk assessment at the outset of every internal audit engagement.
- Frequently inform your audit committee about internal audit's views of risk and the enterprise's emerging or changing risk positions.

Align strongly with stakeholder expectations

- Clearly align the risk management roles and responsibilities of internal audit with the needs and expectations of your stakeholders and enterprise.
- Initiate a top-down review of your organization's risk management structure, activities, policies, and reporting practices.
- Document your organization's risk profile and management's risk appetite; verify that your organization's risk management structure and processes align well with its risk profile and appetite.
- Assess the effectiveness of your corporate governance processes and practices and identify opportunities to strengthen them with regard to risk management.

## 2. Sarbanes-Oxley demands stabilize at a significant level.

Five years after its passage, the Sarbanes-Oxley Act of 2002 (Sarbanes-Oxley, or “the Act”) continues to be a major preoccupation for internal auditors, despite gradual declines in the level of internal audit resources being consumed by compliance with the Act. At the time of its passage, few members of the business community could have anticipated that this controversial reform legislation would have such an enduring impact on corporate internal audit functions.

Immediately after passage of Sarbanes-Oxley, companies began to devote extraordinary levels of internal audit resources to compliance with the Act. The levels of resources allotted to Sarbanes-Oxley compliance have gone down in succeeding years, but reality continues to confound expectations of large reductions going forward.

A year ago, in the 2006 State of the Profession survey, our respondents once again projected that they would experience significant decreases in the level of internal audit resources dedicated to Sarbanes-Oxley requirements in the year ahead. However, the results of our 2007 survey reveal that the hoped-for significant reductions did not take place. And although respondents are once again projecting an ability to reduce the levels of their resource commitments in the year ahead, these projections are not as optimistic as those of our 2006 respondents.

It appears that the amount of resources allocated to Sarbanes-Oxley has stabilized, but at a level higher than anticipated by many internal audit groups. What’s more, the profession appears to have “hit the wall” in terms of its ability to continue making significant reductions in resources dedicated to compliance with the Act.

For internal auditors, optimism is giving way to reality. We expect that Sarbanes-Oxley will remain a major preoccupation for internal audit functions for years to come. In addition, the ultimate impact of Auditing Standard No. 5 (AS5), a new proposal from the Public Company Accounting Oversight Board (PCAOB), remains to be seen.

In particular, survey respondents recognize that the heavy demands of Section 404<sup>1</sup>—which requires companies to document, evaluate, test, and monitor their internal controls over financial reporting—are here to stay. CAEs are no longer optimistic that these demands will taper off anytime soon. On the plus side, many senior management groups and audit committees appear to be making a permanent commitment to providing internal auditors with the resources needed to achieve effective compliance with the Act.

1 Section 404 of the Sarbanes-Oxley Act of 2002 requires management to develop and monitor procedures and controls for making their required assertion about the adequacy of internal controls over financial reporting. Section 404 also requires attestation of management’s assertion by an external auditor. (Internal Auditing’s Role in Sections 302 and 404 of the US Sarbanes-Oxley Act of 2002, © 2004, The Institute of Internal Auditors, Altamonte Springs, Fla.)

### Resource allocations remain high

In our 2005 State of the Profession survey, more than 70% of reporting companies indicated that Year One compliance with Sarbanes-Oxley required more than half of their internal audit resources. And nearly 50% of our 2006 respondents estimated that they allocated more than half of their internal audit time and resources to Year Two compliance.

For the 2007 survey, 41% of our respondents said they dedicated at least half of their internal audit resources to Section 404 compliance in 2006, with 21% devoting 75% or more of their resources for that purpose. In addition, although only 1% of our 2007 respondents anticipated the need to devote all of their resources to Section 404 in 2006, the actual percentage dedicating 100% of their resources to S404 last year was *five times* that number. Overall, the percentage of internal audit resources being devoted to Section 404 by Fortune 500 respondents is lower than that for respondents overall. But the level of commitment by Fortune 500 companies is significant nonetheless.

When these dramatic percentages are viewed in their entirety, they strongly suggest that internal auditors in the United States are collectively still devoting a third or more of their time and other resources to addressing the requirements of Sarbanes-Oxley.

In our 2007 State of the Profession survey, we asked respondents to estimate the percentage of their resources dedicated to S404 compliance in 2006. Their estimates were as follows:

### Resource allocations to Section 404 compliance in 2006

---

	Respondents overall	Fortune 500 respondents
100%	5%	1%
75%–99%	16%	7%
50%–74%	20%	20%
25%–49%	31%	27%
<25%	28%	45%

When we asked respondents to project what percentage of their internal audit resources they expected to dedicate to Section 404 compliance during 2007, we learned that nearly a third of our overall respondents (32%) anticipate devoting at least half their resources. For our Fortune 500 respondents, the corresponding figure is 21%.

Specific projections for S404 resource demands in 2007 were as follows:

### Projections of 2007 resource allocations to Section 404 compliance

	Respondents overall	Fortune 500 respondents
100%	2%	1%
75%–99%	11%	4%
50%–74%	19%	16%
25%–49%	33%	31%
<25%	35%	48%

### **Internal audit groups reporting to CFOs devote more time to Sarbanes-Oxley compliance**

Based upon our surveys and other observations, there is a strong correlation between the administrative reporting relationship of internal audit and the degree to which a company's internal audit resources are devoted to Sarbanes-Oxley compliance.

In our 2007 survey, only 31% of the internal audit functions reporting administratively to the audit committee or CEO indicated that they dedicated more than 50% of their time to the Act during 2006. By contrast, 46% of those who report administratively to the CFO indicated that they spent more than 50% of their audit resources on projects relating to Sarbanes-Oxley in 2006. Finally, 69% of those who reported administratively to the level below the CFO (i.e., the controller or treasurer) indicated that they spent more than 50% of their time on compliance with the Act last year. Given the disparity of time dedicated to compliance with Sarbanes-Oxley depending on reporting relationships, these survey results naturally beg the question as to who is actually directing the focus and deployment of corporate internal audit resources.

### **Continued strong focus on Section 404**

Much of the time being devoted by internal audit to compliance with Sarbanes-Oxley continues to focus on Section 404 project management. In our 2007 State of the Profession survey, 56% of our respondents reported having such responsibility during the prior year in addition to their other duties. Given that project management is clearly a management responsibility, CAEs with S404 project management responsibilities face a dilemma: How can they provide audit committees with objective assurance that a company's Sarbanes-Oxley processes are being managed effectively when the internal audit function has project responsibility for Sarbanes-Oxley compliance? This is a challenge for hundreds of CAEs and audit committees nationwide.

## Section 404 testing differs by company size

When it comes to providing S404 testing support, there is a division between internal audit and management depending upon company size. At 64% of our responding organizations—a surprisingly high number—internal audit leads the way in S404 testing, which includes process test design and management testing as well as process walk-throughs and process documentation. Among Fortune 500 respondents, the percentage of internal audit groups playing the primary testing role drops to 45%. Conversely, management bears primary responsibility for testing at 55% of our Fortune 500 respondents but at only 36% of our respondents overall. Of note, half of our respondents believe that management should be responsible for testing controls, with internal audit responsible for evaluating control effectiveness.

To follow up, we asked respondents to identify what parties or functions handle most of the S404 testing at their companies. For 34% of our overall respondents, the answer is internal audit (29% for F500 respondents), and for 43% of our respondents, the answer is a combination of internal audit and service-provider personnel (42% at F500 companies). Thus at 77% of our total respondents, and 71% of our Fortune 500 companies, internal audit plays a major role in S404 testing. Among the remaining respondents, 20% use audit personnel outside of internal audit as the primary S404 testers (28% for the F500), while 3% rely on service-provider personnel (1% of the F500).

If internal audit has to assume responsibility for S404 testing, it needs to do what it can to mitigate the additional burden this places on the internal audit function. One way to do so is to leverage the assistance of service providers. On an aggregate basis, nearly half (46%) of our responding organizations pursue this strategy.

We also asked respondents about situations where S404 testing is being conducted under the direction of management. In 58% of such situations, management has always been responsible for Section 404 testing, a number that jumps to 77% for Fortune 500 respondents. At 42% of our respondents, management assumed S404 testing responsibility from internal audit, a figure that drops to 23% for F500 respondents.

We had thought that where management assumed the testing responsibility from internal audit for S404 compliance that internal audit resources were transferred to management in conjunction with this transfer of responsibility. However, this perception was not borne out by the survey results.

### **Ongoing concern: Inability to address other key priorities**

As chief audit executives know all too well, Sarbanes-Oxley has diverted significant resources from risk-based auditing. Many organizations have deferred important aspects of traditional risk-based internal audit plans in order to provide the focus and resources necessary to address compliance with the Act. And although companies have been able to make significant reductions in the levels of internal audit resources devoted to Sarbanes-Oxley, these reductions have not eliminated the risks to internal audit.

The objective of risk-based auditing is to ensure that audit resources are directed toward areas of greatest risk. However, when internal auditors spend too much time evaluating or assessing internal controls over financial reporting, they are more likely to be limited in their ability to execute a comprehensive, risk-based audit program. As a result, their audit coverage could fail to cover the full breadth of an organization's risk profile in an appropriate manner and on a timely basis. What's more, high-risk, non-financial areas are likely to be audited less frequently.

Companies need to recognize the extent to which S404 compliance, in particular, is cannibalizing their resources and, in many cases, leaving important areas unprotected. They need to know that the failure of internal audit to address key strategic, operational, and compliance risk areas can lead to weak corporate governance and operational inefficiencies.

Mandatory requirements from Sarbanes-Oxley and other reform measures will continue to consume significant internal audit resources. Recognizing the finite nature of their resources, CAEs need to work with their audit committees and senior management stakeholders to reassess internal audit priorities and resource allocations. Only by CAEs doing so will companies achieve the kind of comprehensive, risk-based approach to auditing that is needed to address key risks in operations, strategy, technology, and other areas that fall outside the scope of Sarbanes-Oxley.

## Looking beyond Section 404: What you need to do

- Identify areas of high and moderate risk that are part of your internal audit plan but have been deferred or cancelled because of the focus on Section 404 of Sarbanes-Oxley.
- Revisit the budgets, skills, and capabilities you need in order to achieve a comprehensive, balanced, and risk-based approach to auditing.
- Develop a process to advise the audit committee and senior management about emerging risks, and about the actions that internal audit should be taking in response.
- Make sure that the audit committee and senior management are aware of (1) the risks that internal audit is addressing and (2) the risks internal audit is unable to address because of its focus on Section 404. Your goal is to inform the audit committee and senior management about the trade-off in risk coverage associated with internal audit's strong commitment to Sarbanes-Oxley compliance.
- Provide your key stakeholders with summaries of your work from both a strategic and tactical perspective.

### 3. Lack of capacity and capabilities is a top concern.

In recent years, internal audit groups have gained added stature as their roles and responsibilities have expanded in response to the mounting demands of Sarbanes-Oxley and other reform legislation. This greater stature is further enhanced as internal audit's key stakeholders gain a better appreciation for the function's capabilities and strengths. Nevertheless, internal auditors have also been exposed to mounting challenges that threaten their ability to execute their mandate in the risk arena.

In our 2007 survey, we asked respondents to rate potential challenges for internal audit in the year ahead. At a time of increasing demands and expectations, internal audit leaders believe that their greatest challenge is finding enough qualified talent to address the growing and increasingly complex needs of their chief stakeholders. Respondents are also concerned about their ability to address the competing priorities of stakeholders and to identify emerging risks. Surprisingly, budget concerns are reported to be a lesser priority, which suggests that most internal audit groups receive adequate budgetary support from audit committees and executive management.

When asked to assess their primary challenges in the year ahead, 84% of our respondents rated the ability to recruit necessary talent as a medium to high risk (42% medium and 42% high). Along the same lines, 69% of respondents rated the ability to find personnel with the right skills to provide adequate audit coverage as a medium to high risk (48% medium and 21% high), while 68% are worried about finding enough people with IT audit skills (a high risk to 28% of respondents and a medium-rated risk to 40%).<sup>1</sup> Navigating competing stakeholder priorities is also perceived to be a significant challenge, with 42% of respondents rating it a medium risk and 12% rating it a high risk.<sup>2</sup> In addition, internal audit's ability to identify emerging organizational risks is viewed as a noteworthy challenge by 63% of respondents, with 52% labeling it a medium risk and 11% a high risk.

Another reflection of staffing concerns is the percentage of respondents actively recruiting for vacant positions, an issue addressed in our 2005 and 2006 surveys. In our 2007 survey, 43% of our Fortune 500 respondents and 31% of our respondents as a whole reported that they were actively recruiting for auditor positions that had been vacant for six months or more. The 31% overall figure compares with 32% overall for respondents in both our 2005 and 2006 surveys.

<sup>1</sup> The talent-related concerns regard providing satisfactory audit coverage in key areas of specialty, including data analysis, fraud, finance, and technology.

<sup>2</sup> The ability to juggle multiple and often conflicting priorities has become an important competence in today's world of internal audit.

As mentioned, having an adequate budget to address the organization's audit plan is a relatively minor concern to most internal audit leaders, with 87% of respondents characterizing it as a low to medium risk (54% low and 33% medium). Similarly, concerns about unexpected budget cuts stemming from either an economic or a company downturn are minimal, with 75% of respondents according this possibility a low concern, 19% rating it a medium concern, and only 7% calling it a high concern. It was also interesting to note that respondents did not believe that the talent-related challenges identified previously would translate into a significant risk to the delivery of high-quality work. In fact, 97% of the respondents considered the potential loss of credibility linked to the overall quality of work to be a low to medium risk (78% low and 19% medium).

The bottom line for internal audit: You are unlikely to experience budget challenges in the year ahead, but you can expect to have trouble attracting and retaining the mix of talent you need to deliver effectively on stakeholder expectations. You will continue to face stiff competition for audit professionals who can evaluate and test internal controls, assess the adequacy of financial controls, audit complex areas, and address both enterprise-wide risk and governance issues.

To address shortfalls in your human resources and to strengthen your skill sets, capabilities, and productivity, consider leveraging "capacity multipliers," such as strategic co-sourcing, to acquire specialized skills. Also consider tapping third-party internal audit service providers to gain access to particular skill sets, expand your geographic coverage, and provide the flexibility needed to deliver a responsive audit plan.

## 4. Rotational staffing provides a key source of talent.

To a growing extent, leading companies are relying on internal audit as a major source of talent for their lines of business. At the same time, corporate internal audit groups are increasingly turning to rotational staffing models as an effective means to recruit staff from within and outside their companies and to offer these recruits career opportunities in company business units after a two-to-three-year rotation within internal audit. For many corporations, these two strategies provide complementary pathways to much-needed talent in a constrained market.

Rotational staffing has long been a leading practice within the internal audit profession. However, our survey results suggest that it has moved well beyond best-practice status and is fast becoming the prevalent staffing model for large corporate internal audit groups. The experiences offered by internal audit are highly valued by organizations. Moreover, rotational models provide internal audit groups with attractive career paths for recruiting purposes. Yet despite the growth in popularity of rotational models, there appears to be little consensus among survey respondents as to which model works best.

According to our survey, more than 80% of our Fortune 500 respondents have some form of rotational staffing in place that affects either all or significant portions of their internal audit staffs. Of note, 15% of our F500 respondents are dedicated fully to rotational staffing. We also learned that the average length of a rotation is between two and three years, and that most of our respondents tap public accounting firms and other companies for experienced personnel.

Overall, survey results reflect that companies are taking a variety of approaches to rotational staffing and that no particular approach is dominant. Our specific results, by area, are as follows:

- **Staffing model**—When asked to describe their current staffing model for internal audit, 8% of respondents said a pure rotational staffing model (13% for F500 respondents), 43% said a blend of rotational staffing and career positions (57% for the F500), and 49% said that their staffs were made up entirely of career positions, a figure that drops to 30% for F500 respondents.
- **Positions included**—We asked respondents whose models were fully rotational to specify to which positions their rotational models applied. In response, 45% said to all positions, 40% said to all positions with the exception of the CAE, and 15% said to all positions with the exception of the CAE and managers.
- **Approximate rotation length**—
  - 1 year—11%
  - 2 years—38%
  - 3 years—28%
  - 3–5 years—21%
  - Other—2%
- **Potential for career advancement**—When we asked if their staff have the opportunity to move up into audit management at the conclusion of their rotations, 8% of respondents said frequently, 51% said occasionally, and 41% said no, they do not have this opportunity.
- **Sources for recruitment**—When asked where they find recruits to rotate into internal audit (we asked respondents to check all that apply), 28% said colleges and universities, 81% said public accounting firms, 74% said other companies, and 49% said from business units within their own companies. The fact that colleges and universities do not serve as a primary source of recruitment for rotational programs should not come as a surprise. At the conclusion of most rotational programs, internal auditors are typically afforded opportunities to join finance, or other functions in their companies that offer significant responsibility. In most cases, it would not be practical or feasible to offer such positions to staff with only three years of post-college experience.

# Optimizing rotational programs

- An ideal rotational program will have executive-level sponsorship and support outside of internal audit and be viewed as a corporate program as opposed to just an internal audit program. For example, the CEO of one prominent Fortune 100 company personally attends the “graduation” ceremony for internal auditors completing their rotations.
- Ideally, a rotational program will have clearly defined criteria for recruits (i.e., new graduates, experienced hires, and transfers from within the company) and for the skills they are to develop. The program should also include an established process for placing participants in positions within the company at the conclusion of their rotations.
- Rotational programs should have established performance objectives and goals, to measure not only the flow-through of the program but also the successes of the participants after leaving internal audit.
- The ideal duration of a rotation program is about three years. Any shorter, and participants won’t derive sufficient benefit from the experience; any longer, and it begins to resemble a career model.

- High-performance rotational plans are often linked directly to an organization's management development programs or to internal human resource processes that identify high-potential performers so that participation in the internal audit rotation program becomes a sought-after assignment.
- Internal audit functions should also consider establishing shorter-term "guest auditor" programs to recruit subject-matter experts (SMEs) from within the company to conduct specific audits leveraging SME areas of expertise. Such programs can serve as an excellent means of auditioning/recruiting individuals who demonstrate a strong aptitude for internal audit during their guest auditor tenures.
- Finally, safeguards should be designed to ensure that internal audit staff members nearing completion of their rotational tenures are able to carry out their internal audit responsibilities objectively. For example, if an individual has indicated a preference for an assignment to a particular business unit after his or her internal audit tenure (or is being openly recruited or considered for such a position), he or she should probably not be assigned to conduct internal audits of operations in that unit.

## 5. Audit report ratings are popular but present challenges for internal audit.

It is increasingly common for chief audit executives to include ratings and opinions in their audit reports as a means of communicating clearly with audit committees about the relative significance of audit results. Despite the growing popularity of audit ratings and opinions, however, internal auditors continue to struggle with how best to use these communications tools to synthesize findings and overall reports for audit committees and executive management. On the one hand, there are advantages to providing ratings information. On the other hand, there is a lack of consistency in the approaches being taken to convey such information.

### **What is driving the growth in audit ratings?**

Four factors, in particular, are responsible for the increased use of audit ratings:

- First, there is a greater focus on internal audit reports and findings by audit committees, senior management, external auditors, and regulators.
- Second, internal audit stakeholders are requesting more clarity and the prioritization of audit results so that they will know which issues require their immediate attention.
- Third, there is a strong need for chief audit executives to provide audit committees and senior management with internal audit's overall assessment or opinions with respect to organizational controls.
- Fourth, senior management views audits as an excellent source of information to help them understand and assess the relative performance both of business and of the functional units within the organization.

### **Majority of respondents include overall ratings or conclusions**

We asked our survey participants about ratings on individual findings. In response, 56% of them as a whole—and 63% of Fortune 500 respondents—said they routinely include ratings on individual findings in their internal audit reports. Moreover, 69% of respondents include in their reports either summaries or consolidated ratings on individual findings to characterize the overall results of the audit. We also found that 63% of respondents routinely include an overall rating to reflect audit conclusions, a figure that rises to 75% for Fortune 500 respondents.

To gain better insight into how audit ratings are characterized, we asked the respondents who include ratings with their reports to describe how they present their findings. We learned that 57% use a descriptive approach, using language such as *meets expectations* or *needs improvement*; 22% use adjectives such as *strong*, *effective*, or *poor*; 12% use a numerical rating scale; and 9% use some other rating approach.

## The pros and cons of audit ratings

Audit report ratings provide a number of significant benefits. They help senior management and audit committees assess audit results more quickly; they provide the basis for prioritizing follow-up attention from internal audit or the audit committee; and they offer useful comparative information on the severity of issues or trends across an organization. Ratings also facilitate the design and implementation of issues-tracking systems by providing a means to categorize findings. What's more, audit ratings allow internal audit to communicate the potential level of exposure or risk associated with not implementing corrective actions emanating from audit findings.

At the same time, many internal auditors find it counterproductive to include ratings and opinions in their findings and reports. They cite the potential for audit ratings to increase the audit cycle time by extending the reporting process. And they say that audit report ratings can create friction between internal audit and operating units, and make operating unit managers more reluctant to share known control weaknesses with auditors. This discord is exacerbated when audit committees request that managers whose areas of responsibility are the subject of an unsatisfactory report rating meet with the audit committee to explain how they intend to correct the noted deficiencies.

In our 2007 survey, more than half (56%) of respondents reported that audit ratings are, indeed, creating friction and slowing down the audit process at their organizations. They said that company ratings are leading to disagreements with management officials or to frequent or occasional slowdowns in the reporting process. We also learned that more than a third of respondents believe that ratings are being used to determine compensation and bonuses for some members of management, a practice that can create resentment among managers whose areas are not rated satisfactorily. When we asked if company report ratings are used to determine performance ratings, compensation, or bonuses for management, 6% of respondents said frequently and 28% said occasionally.

## Keys to effective audit report ratings

- Identify a rating scheme that fits with the organization culturally, with its control system, and with the objectives of internal audit and management.
- Communicate the rating scheme and its objectives to management and the audit committee to obtain their understanding and support; discourage the use of ratings for punitive actions against management.
- Manage the report distribution and follow-up process (i.e., ensure that ratings reports are routinely distributed to the CEO and audit committee).
- Develop and communicate objective and transparent criteria for assigning audit ratings. In the auditing process, allow management to respond to “draft ratings,” and include their responses in the final report. If proposed audit ratings become a routine source of friction and/or prolong the report-drafting process, consider providing the initial results of the audit to management for review and comment without the proposed rating. Once agreement has been reached on the audit results, provide management with the rating for separate commentary.

## Producing annual opinions on internal controls

Audit committees or management have requested that CAEs periodically provide a summary opinion about their companies' systems of internal accounting controls. In order to comply with those requests, 36% of the CAEs at our responding companies reported issuing an annual, overall opinion on internal controls, and 26% reported issuing an annual, overall opinion on internal controls over financial reporting. Audit report ratings often serve as the building blocks by which these opinions are constructed.

As is the case with audit report ratings, there are both advantages and disadvantages to expressing an opinion on a company's overall system of internal controls. On the plus side, many CAEs believe they are providing a value-added service to management by helping to support certifications for Sections 302 and 404 of Sarbanes-Oxley. In addition, some indicate that they are assisting the audit committee in discharging its fiduciary responsibilities and are contributing to maximizing the efficiency of external auditors.

On the minus side, providing opinions on internal control systems carries certain risks and can create pitfalls. For example, the issuance of an annual opinion by the CAE might inadvertently and inappropriately imply that internal audit either "owns" or "shares ownership" of internal controls with management. In addition, if the CAE's opinion is not appropriately qualified, it can create a false impression of the scope and level of assurance it provides. For example, does the opinion cover the organization's overall system of internal controls as defined by COSO, or does it cover only financial controls related to Sarbanes-Oxley certifications? A particular concern is the question of the relationship between the scope of the audit effort and the opinion issued—that is, does the audit work provide a sufficient basis for the opinion being given? Depending upon the breadth and scope of the annual internal audit plan, the CAE may not be in a position to respond to a request for an overall opinion.

In our view, internal auditors should exercise caution if being asked to provide overall opinions on an organization's system of internal controls. Quite simply, we believe that there can be significant risks and downsides to internal audit issuing such opinions, particularly if management is the party requesting the opinion. A specific concern relates to organizations where management must comply with the requirements of the Sarbanes-Oxley Act. Internal audit should not be placed in a position where it inadvertently assumes any degree of ownership or responsibility for the control system, which is a management responsibility. We suggest that auditors who are asked to issue these annual opinions review carefully the guidance issued by the IIA, "Practical Considerations Regarding Internal Auditing Expressing an Opinion on Internal Control."<sup>1</sup>

<sup>1</sup> Available at [www.theiia.org/download.cfm?file=25663](http://www.theiia.org/download.cfm?file=25663).

## Caveats for internal auditors asked to issue annual opinions

- Reach agreement with management and the audit committee as to the reason the opinion is being requested, its expected use, and the exact definition of the internal control system being addressed.
- Develop effective criteria on which the opinion will be based (e.g., rating audit projects by number of findings, significance of findings, or maturity of controls; using either positive/reasonable assurance or negative/limited assurance in rendering an opinion on the overall system of internal control).
- Develop protocols for communicating annual opinions that clearly delineate the basis for an opinion and any limitations on the scope of internal audit work upon which the opinion was based.
- In the body of the opinion, clearly identify the definition of the control system being addressed, the responsibilities of management, and the scope and timing of the supporting audit activities.
- To the extent possible, provide a disclaimer of opinion or, if the plan provides sufficient coverage for the CAE to form a conclusion, negative assurance (e.g., “nothing came to our attention within the scope of our work that would indicate that controls are not effective”).
- Use objective criteria/language in communicating an opinion.
- Clearly communicate to the audit committee and senior management the basis for your opinion.

## 6. Other trends and issues from the 2007 survey.

### Reporting relationships stabilize at elevated levels

Over the last five years, the reporting levels of internal audit functions have risen steadily. In a 2002 survey conducted by the Institute of Internal Auditors, only 55% of their internal audit respondents said they reported functionally to their audit committee. According to our 2005–2007 State of the Profession surveys, that number has increased more than 30 percentage points in recent years and now appears to be stabilizing.

This year, our 2007 survey participants described their functional and administrative reporting relationships as follows:

- **Functional**—Eighty-nine percent of our Fortune 500 respondents report functionally to the audit committee or board of directors. By comparison, 86% of total respondents report functionally to the audit committee or board, a figure that is down slightly from the 88% recorded in both our 2005 and 2006 surveys.
- **Administrative, to the CEO or president**—Twenty-eight percent of our Fortune 500 respondents report administratively to the CEO or president, as do 31% of total respondents, a figure that is up slightly from the 29% reported by our 2006 respondents.
- **Administrative, to the CFO or the office of the CFO**—Fifty percent of our Fortune 500 respondents report administratively to the CFO or the office of the CFO, as do 47% of our respondents overall, a figure that compares with 49% in 2006.

## Commitments to quality relatively strong within Fortune 500 but weak overall

We asked respondents whether they had initiated an external quality assurance review (QAR) of their internal audit function consistent with the IIA Standards, or if they were planning to initiate one. In response, only 33% of overall respondents reported having conducted a QAR<sup>1</sup> within the past five years, although this percentage increased to 58% for Fortune 500 respondents. Another 12% of our overall respondents, and 13% of our F500 respondents, said that they planned to conduct a QAR by December 31, 2007.<sup>2</sup> Thus 45% of our overall 2007 respondents reported that they had either undergone a QAR at the time surveyed or were scheduled to complete one prior to December 31, 2007, which compares with 49% for our 2006 respondents.<sup>3</sup> Conversely, 26% of our Fortune 500 respondents and 49% of our 2007 respondents overall said that they had not conducted a QAR and had no plans to do so (the 49% overall figure compares with 51% for our 2006 respondents). In our 2007 survey, we received no answer from 6% of our respondents overall or from 2% of our F500 group.

In terms of future plans for QARs, 24% of our overall respondents to our 2007 survey and 16% of our F500 respondents said that they plan to conduct another QAR within three years of their initial QAR. Another 61% said that they would conduct another QAR at or near the five-year deadline, a figure that increases to 68% for the Fortune 500.

When asked to describe their initial QAR experiences, 24% of our total respondents and 25% of our F500 respondents selected *very valuable*, i.e., “yielded significant insight into internal audit’s conformance with IIA Standards (and benchmarks to other internal audit departments).” The majority of our respondents—61% of respondents overall and 65% of the F500—selected *somewhat valuable*, i.e., “we learned a few things that will enhance operations.”

- <sup>1</sup> QARs are considered to be particularly important in management and audit circles. This reflects the enhanced role internal audit departments play today in the risk, control, and governance activities of many major corporations. In addition to confirming compliance with the Standards, a well-designed external assessment will provide benchmarks and measurements that can be used to improve internal audit performance long after the external QAR report is issued. When the IIA unveiled its Standards for the practice of internal audit in 2002, it mandated that internal audit groups conforming to the Standards adopt formal quality assurance and improvement programs that included an external QAR at least once every five years. Although compliance with the IIA Standards is not generally mandated by statutes or regulations, its guidelines are often viewed as mandatory by internal audit leaders.
- <sup>2</sup> Internal audit departments established after January 1, 2002, have until five years from the date they began operations to undergo an initial external QAR.
- <sup>3</sup> In our 2006 State of the Profession survey, 49% of our respondents reported that their internal audit groups had undergone an external QAR at the time surveyed, or were scheduled to complete a QAR prior to December 31, 2006. Fifty-one percent of our 2006 respondents said they were not actively pursuing a QAR.

We also asked respondents to indicate whether they conducted self-assessments of their operations, in keeping with IIA Standard 1311, which requires internal audit to conduct a periodic self-assessment. In response, 28% of our total respondents—but 41% from F500 companies—said they conduct such assessments annually. Another 10% of respondents overall, and 8% from the F500, conduct such assessments every two years. In addition, 14% of our total respondents and 17% from the F500 conduct such self-assessments at least once between external assessments.

### **Continuous auditing continues to generate interest**

Of note, 43% of our 2007 respondents reported using some form of “continuous” auditing or monitoring in their audit operations. Overall, 11% describe their processes as fully operational, which compares with 13% for our 2006 respondents (a smaller group), while 42% of our 2007 Fortune 500 respondents and 32% of our 2007 respondents overall report that their processes are not fully developed. The latter figure represents an improvement from 2006, when 37% of our respondents said their continuous auditing processes were not yet fully functional. Another 38% of our 2007 respondents said they are planning to develop some form of “continuous” auditing or monitoring, while only 18% of this year’s group reported no plans in this area.

Since most continuous auditing is a blend of automated and manual operations, we asked our 2007 respondents to describe their continuous auditing in this context. In response, 8% said their process is or is likely to be fully automated, a significant increase from the 3% of our 2006 survey respondents who claimed to have fully automated processes. Another 81% of our 2007 group said that their continuous auditing processes were part automated and part manual, which compares with 56% for our 2006 respondents. And 11% of our 2007 respondents said that their continuous auditing processes were entirely manual, a sharp decrease from 2006, when 41% of our respondents said that their continuous auditing processes were only manual. The last statistic suggests a significant increase in the application of technology to auditing processes for corporations as a whole.

With respect to their current or planned process frequency, 9% of our 2007 respondents said daily, 7% said weekly, 38% said monthly, and 46% said quarterly. In 2006, the most common continuous auditing “cycle” was also quarterly, with 57% of our respondents falling into this category, while 34% said they focused on monthly monitoring activities and 9% on daily applications of their continuous auditing processes. Of note, we added *weekly* as a frequency option in 2007; it was not included in 2006.

# Methodology

The 2007 State of the Profession survey for internal auditing was conducted in the fourth quarter of 2006 and includes responses from 717 audit managers.

Of the respondents:

- Eighty percent are either chief audit executives or internal audit directors/managers.
- Fifty-nine percent are from companies with \$1 billion or more in revenue.

The survey had four purposes:

1. Capture a snapshot of the internal audit profession.
2. Share insights and observations from PwC experts about the major issues, trends, and changes reshaping internal auditing today.
3. Collect benchmarking data to help organizations compare and contrast their internal audit processes and procedures.
4. Provide a baseline to measure ongoing changes in the profession.

# Appendix

## Appendix I: Risk management roles

The 2007 State of the Profession survey reflects significant confusion with respect to the roles of management, the audit committee, and internal audit in the area of risk management. To help clarify who does what in the risk arena, we've distilled key guidelines from the IIA and the New York Stock Exchange, delineating risk management responsibilities as follows:

- **Management** is responsible for corporate decisions involving risk management. It is management's job to assess risk and oversee a company's enterprise-wide risk management process.
- In its oversight role, the **audit committee** must be familiar with the policies, procedures, guidelines, and processes put in place by management to govern corporate risk management activities. This includes being familiar with major risk exposures and the steps being taken to assess, monitor, and control such exposures.
- It is the job of **internal audit** to report to the audit committee that management is effectively identifying and controlling risk and that the company has a systematic, effective approach to enterprise risk management.

### Guidance from the Institute of Internal Auditors

The IIA's International Standards for the Professional Practice of Internal Auditing (known as the Standards) provide a solid foundation for internal audit in the area of risk management. In terms of broad direction, the IIA Standards state that the primary goal of internal audit is to evaluate and improve the effectiveness of an entity's risk management, control, and governance processes (Standard 1220.A1). Of note, the IIA Standards indicate that when performing consulting services, internal auditors should maintain objectivity and not assume management responsibility.

The IIA Standards also provide the following specific direction:

- **Planning**—Chief audit executives should establish risk-based plans to determine internal audit priorities (IIA Standard 2010).
- **Risk assessments**—Plans of engagement should be based on risk assessments conducted on an annual or more frequent basis, with input from senior management and directors at every stage (IIA Standard 2010.A1).
- **Nature of work**—Internal audit should evaluate and strive to improve risk management, control, and governance processes in a systematic, disciplined manner (IIA Standard 2100).
- **Risk management**—Internal audit should help to identify and evaluate significant exposures to risk and contribute to the improvement of risk management and control systems (IIA Standard 2110).

- **Monitor and evaluate risk**—Internal audit should monitor and evaluate the effectiveness of the organization’s risk management system (IIA Standard 2110.A1). In addition, internal auditors should leverage the results of their assessments to evaluate the adequacy and effectiveness of controls addressing the organization’s governance, operations, and information systems (IIA Standard 2120.A1).

With respect to enterprise-wide risk management, the IIA says the primary role of internal audit is to provide objective assurance to the board of directors on the effectiveness of an organization’s ERM activities. Although management is responsible for making risk management decisions, internal auditors can offer advice and counsel to management in the area of risk management, a role that can include challenging management’s thinking or supporting management’s decisions (see Appendix II).

### **Guidance from the New York Stock Exchange**

Revised corporate governance rules implemented by the New York Stock Exchange in 2004 discuss corporate policies with respect to risk assessment and risk management as well as the requirement for listed companies to have an internal audit function. In a commentary supporting the rules, the NYSE states the following:

“While it is the job of the CEO and senior management to assess and manage the listed company’s exposure to risk, the audit committee must discuss guidelines and policies to govern the process by which this is handled. The audit committee should discuss the listed company’s major financial risk exposures and the steps management has taken to monitor and control such exposures. The audit committee is not required to be the sole body responsible for risk assessment and management, but, as stated above, the committee must discuss guidelines and policies to govern the process by which risk assessment and management is undertaken.”

In additional commentary, the NYSE says that 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,” adding that a listed company may outsource this function to a third-party service provider.

## Appendix II: Internal audit and enterprise risk management—the IIA’s perspective

In 2004, the IIA issued a position paper titled *The Role of Internal Audit in Enterprise-wide Risk Management*, which provides clear guidance for the internal audit profession in the ERM arena. The paper—issued in conjunction with the release of *Enterprise Risk Management—Integrated Framework*, by COSO—suggests ways for internal auditors to maintain the objectivity and independence required by the IIA’s Standards when providing assurance and consulting services.

According to the IIA, the core role of internal audit with respect to ERM is to provide objective assurance to the board of directors on the effectiveness of an organization’s ERM activities. This includes helping to ensure that the organization is managing its key business risks appropriately and is operating its system of internal controls effectively.

Although it’s permissible for internal auditors to advise management in the area of risk management, or to *challenge or support* management’s decisions on risk, the IIA makes it clear that internal auditors *should not be making risk management decisions*. That is the purview of management.

The IIA advises CAEs evaluating a potential ERM activity to consider two key factors: first, whether the activity raises any threats to the desired independence and objectivity of the internal audit function, and second, whether the activity is likely to improve the organization’s risk management, control, and governance processes.

When it comes to ERM activities, the IIA says that internal auditors are permitted to provide assurance on risk management processes and give assurance that risks are being evaluated correctly. It’s also permissible for internal auditors to evaluate risk management processes, to evaluate the reporting of key risks, and to review their management. What’s more, the IIA puts its stamp of approval on internal audit conducting a number of other ERM activities so long as internal auditors take steps to safeguard their independence and objectivity. This expanded group of activities, which the IIA describes as “legitimate internal auditing roles with safeguards,” includes facilitating the identification and evaluation of risks, coaching management in responding to those risks, coordinating ERM activities, consolidating risk reporting, maintaining and developing the ERM framework, championing the establishment of ERM, and developing risk management strategies for board approval.

On the list of practices discouraged for internal audit in the ERM arena, the IIA places taking part in setting the risk appetite, imposing risk management processes, or providing management assurance on risks. Nor should internal audit be making decisions on risk responses, implementing risk responses on behalf of management, or taking accountability for risk management.

## Appendix III: The COSO ERM *Framework*

ERM can help management improve performance and profitability, optimize resources, ensure effective reporting, and strengthen compliance with laws and regulations. In 2004, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) launched its *Enterprise Risk Management—Integrated Framework* to provide direction for businesses and other organizations seeking to leverage the principles of enterprise risk management.

The COSO ERM *Framework* defines ERM, creates a foundation for understanding of ERM issues, and provides a standard against which organizations can compare their approaches to ERM. Written for COSO by PricewaterhouseCoopers, the ERM *Framework* incorporates the provisions of *Internal Control—Integrated Framework*, developed by COSO in 1992 to help companies assess and enhance their internal control systems.

### Addressing four key objectives and eight ERM components

The COSO ERM *Framework* addresses four types of organizational objectives: strategic, operations, reporting, and compliance. With respect to reporting and compliance, the ERM *Framework* provides the means theoretically to provide reasonable assurance of achieving objectives, given that these areas are considered to be within an entity's control. However, the achievement of strategic and operations objectives is often subject to events outside an entity's control. In such cases, the ERM *Framework* can provide reasonable assurance that management, and the board in its oversight role, will receive timely updates of the extent to which the entity is making progress on these objectives.

The COSO ERM *Framework* also identifies eight key interrelated elements, or components, of effective enterprise risk management, as follows:

- **Internal environment**—This includes a company's risk management philosophy and risk appetite as well as how risk is viewed and addressed within the company.
- **Objective setting**—ERM provides a process for management to set objectives that support the entity's mission and are consistent with its risk appetite.
- **Event identification**—Internal and external events affecting the achievement of organizational objectives need to be identified and categorized as either risks or opportunities.

- **Risk assessment**—Risks are analyzed, with their likelihood and impact taken into account, as a basis for determining how they should be managed.
- **Risk response**—Management decides whether to avoid, accept, reduce, or share a given risk, and takes steps to align that risk with the entity’s risk tolerances and risk appetite.
- **Control activities**—Policies and procedures are established and implemented to help ensure that chosen responses to risk are carried out effectively.
- **Information and communication**—Relevant information is identified, captured, and communicated in forms and within time frames that enable people to carry out their responsibilities; communication flows up, down, and across the organization.
- **Monitoring**—ERM systems, processes, and procedures are monitored, modified, and evaluated, as necessary.

The COSO ERM *Framework* enables an organization to analyze the effectiveness of its ERM activities by assessing the relationships between the *Framework’s* four categories of objectives (i.e., what an entity is seeking to achieve) and its ERM components (i.e., the elements needed to achieve the organizational objectives).

### **Assessing the effectiveness of enterprise risk management**

Determining that an entity’s ERM is “effective” depends on whether the eight ERM components are present and functioning effectively. In this sense, the components are also criteria for effective enterprise risk management.

When ERM is determined to be effective in each of the four categories of objectives, an entity’s board of directors and management have reasonable assurance that they understand the extent to which the organization’s strategic and operations objectives are being achieved, that they know the entity’s reporting is reliable, and that the organization is complying with applicable laws and regulations.



For more information, please contact:

Dick Anderson  
Partner  
312.298.4814  
dick.anderson@us.pwc.com

Richard Chambers  
Managing Director  
678.419.7004  
richard.f.chambers@us.pwc.com

Or visit:

[www.pwc.com/internalaudit](http://www.pwc.com/internalaudit)

