

CFO.com

PwC: Internal Auditors May Be Missing Risks

In a report on the internal audit function, PricewaterhouseCoopers finds 18 percent of companies do not assess risk on an annual basis.

[Sarah Johnson](#), CFO.com

May 17, 2007

The major accounting scandals earlier this decade and the Sarbanes-Oxley Act placed a renewed focus on risk management at publicly traded companies. But assessing risk is one task that has fallen by the wayside at some companies. According to a PricewaterhouseCoopers report, 18 percent of companies do not conduct an annual risk assessment.

That could be worrisome for investor advocates who have trusted Sarbox to encourage regular risk assessments from auditors and management — particularly in the wake of recent direction from regulators that Sarbox-mandated reviews should focus on high-risk areas. "If they aren't adequately looking into risks in the areas of finance, compliance, fraud, and technology, how can they be sure their financial statements are fairly presented?" asks Mark Grothe, research analyst at shareholder-advisory firm Glass Lewis. "More broadly, I think these lapses probably indicate poor management teams and ineffectively run companies."

To be sure, Sarbox could actually be to blame for variation among company risk-management practices. The PwC report, which focuses on the state of the internal auditor profession, says that between departments and across the enterprise, more parties have gotten involved in assessing risk and contributing to the company's risk management process. That, says PwC, has led to some confusion and overlapping of responsibilities. One-third of the internal audit managers surveyed said their companies conduct multiple risk assessments across the organization, but the majority do not coordinate their work or results. The effect, says PwC partner Dick Anderson, is inefficient and redundant presentations before audit committees.

Fortunately, observers note, this confusion is tapering as companies get a better handle on their risk management processes and consider adopting a full-blown enterprise-wide risk management system. Since large and midsize companies have a couple of years of Sarbox compliance behind them, CFOs should take a step back and be sure all their board and audit committee members, department heads, and internal auditors are on the same page when it comes to defining areas of risk, suggests the PwC report, which the audit firm released earlier this week.

How the internal audit team assesses and participates in risk management varies within companies. At some, internal auditors are in charge of risk management (a set-up frowned upon by the Institute of Internal Auditors) while other companies lack any formal management oversight of the process. "The implementation of risk management at many organizations is immature at best and chaotic at worst," PwC said in its report. To improve

a company's systems, the CFO or the head of the internal audit team should decide whether the organization understands their key risks, suggests Anderson, and ask the following questions: How are they monitored and mitigated? Who does what? And how should the conclusions be put together?

Dominique Vincenti, chief advocacy officer of the IIA, cautions that enterprise risk management processes do not have to be overly formalized or involve tons of documentation. But they do need to provide the board and top executives the same, big-picture view of the company's stance on risk. To educate other managers and the board about switching to formal risk management plans, finance departments need to factor in the company's culture, operations, systems and values, she says. "[Risk management] needs to be presented in a way that is useful and easily shared among department heads," she said. The IIA recommends that internal auditors not be in charge of risk management, but rather evaluate the board's and CEO's definition of risk management when they audit.

In its report based on feedback from 717 audit managers, PwC recommends that companies adopt a process approach to risk assessment and planning; supplement annual assessments with quarterly or more frequent updates; and coordinate with other risk management groups.