

## Where is the Risk?

Leading audit committees today are recognizing the important—if not imperative—link between effective oversight of financial reporting risk and effective oversight of risk management. As many audit committees are discovering, however, oversight of a company's risk management efforts is no simple matter.

While most audit committees may be comfortable with overseeing financial reporting and related compliance risks, the oversight of nonfinancial risks—operational, strategic, regulatory and others—that could *become* financial reporting risks presents formidable challenges. Often, it is unclear who—whether the audit committee, the full board or another board committee—is responsible for overseeing certain risks; inadequate reporting of risk information can hamper oversight efforts; and lack of a common “risk” vocabulary complicates matters. Considering these and other challenges, it's little surprise that most audit committees today aren't all that comfortable with risk management and risk oversight processes.

Recent surveys conducted by the KPMG Audit Committee Institute (ACI) at roundtables this spring confirm this discomfort. Only one in four of the 2,000-plus directors, audit committee members and senior executives attending the roundtables said they were “very satisfied” that the board and audit committee are effective in overseeing the potentially significant business risks—both financial and nonfinancial—

facing the company. The remainder were only “somewhat satisfied” (51 percent) or said oversight needs to be improved (22 percent).

Perhaps most alarming, a large majority (82 percent) were only “somewhat satisfied” with the information they received regarding risk, or said that such reporting “needs improvement.” And in another ACI poll conducted recently, audit committee members identified “oversight of risk management” as their second-highest priority for 2006.

In some respects, the heightened focus by boards and their audit committees on the oversight of risk management is an outgrowth of Sarbanes-Oxley, with its emphasis on internal controls. From the audit committee's perspective, an effective risk management process is critical to the oversight of the financial reporting process in several ways: A disciplined risk management process can be invaluable to the audit committee by identifying and prioritizing the company's significant financial reporting risks and nonfinancial risks that may have financial reporting implications; it also can help the audit committee ensure that, for each significant risk:

- ◆ The company has appropriate and effective internal controls.
- ◆ Internal and external audit plans appropriately address the risk.
- ◆ The financial statement impact of the risk, if any, is properly recorded or disclosed.
- ◆ Certifications and assertions for Sarbanes-Oxley Sec-

tions 302 and 404, respectively, are appropriate.

The oversight of risk is made more difficult by the absence of a formal risk management process, which is the case today at many companies. While many companies have an “informal” risk management process, in a recent survey conducted by KPMG's 404 Institute, some 40 percent of respondents said their companies were just “investigating the concept” of implementing a formal enterprise risk management program; and only 5 percent indicated their enterprise risk management process was at an “advanced” stage. Likewise, the oversight of risk—by audit committees, boards and other board committees—is widely an evolving practice, often lacking a clear delineation of oversight roles and responsibilities.

Given the breadth, complexity and dynamic nature of risk, as well as the critical link between the oversight of the financial reporting process and the oversight of risk management, we see leading audit committees employing three key practices in their oversight of risk:

- ◆ Reviewing management's processes to identify, prioritize, mitigate and communicate the potentially significant business risks facing the company.
- ◆ Considering the adequacy of management's reports regarding the status of its risk management activities.
- ◆ Ensuring that oversight responsibilities for risk management are appropriately aligned and coordinated among the au-

dit committee, the full board and other board committees. Information flow is increasingly seen as vital to ensuring that risk oversight responsibilities are properly coordinated, and that key risks don't fall through the cracks.

For example, “management risk” is often omitted from the usual portfolio of corporate risks. But it is perhaps the biggest hazard, and minimizing such risk requires every board member's and committee's constant attention.

Management risk comes in two main varieties: the risk that corporate officers lack the competence, skills, resources, or motivation to manage the business, and the risk that they place personal interests above those of the company and its stakeholders.

The way to check for management risk is through focused and ongoing observation and inquiry. This calls for directors, including the audit committee, to ask probing questions and to monitor management performance against business plans.

The bottom line? Audit committees should review their risk oversight processes, including the risk reports provided by management, to ensure they are sufficient to demonstrate that the committee and the board are fulfilling their responsibilities in this area.

---

Kenneth Daly is executive director and Caryn Bocchino is senior manager, KPMG's Audit Committee Institute. The views and opinions are those of the authors and do not necessarily represent the views of KPMG.