Business Insurance www.businessinsurance.com

Sarbanes-Oxley brings opportunity

Ask A Risk Manager, published 6/27/2005

By Christopher E. Mandel

Q: *Why should risk managers care about the Sarbanes-Oxley Act and the compliance efforts of their companies?*

A: As anyone who reads the trade publications knows, there exists no shortage of reports and opinions on the challenges and costs of complying with the federal Sarbanes-Oxley Act, which, stated in the simplest terms, requires public companies to certify for the benefit of their stakeholders the accuracy of their statements as to their financial health.

Each week, it seems, some new source documents the substantial cost and significant impact on the companies that are required to become compliant. Attention has been increased by the convictions of the chief executive officer of WorldCom Inc. and the CEO and chief financial officer of Tyco International Ltd., the first group of executives found to have violated the financial reporting mandates of Sarbanes-Oxley.

Central to the work of achieving compliance is assessing the controls that both directly and indirectly affect the accuracy of a company's financial transactions and the reports on which they are based. While these controls are largely financial in design, they also include many operational, compliance and strategic measures that make up the overall control structure of every company. The financial, operational and compliance controls are the bread and butter of the internal auditor, while the annual audit of the company's financial statements is, of course, of particular concern to the external auditor and the board of directors. The strategic, or business-related, controls and the risks to which they relate are the least understood and the most difficult to document and measure.

And therein lies the traditional connection for risk managers. Just as the controller has been held accountable for financial reporting controls and the compliance head for compliance controls, the traditional risk manager has historically been held accountable for the controls related to a company's many insurable risks, which are typically operational in nature. Take employee injury as an example; most traditional risk managers have been responsible for the risk financing of employee injuries, typically through insurance, as well as for structures that attempt to prevent accidents and to control the cost of losses should they occur. This same construct is true for most other insurable exposures, at least in the higher-performing organizations.

Of course, accountability for the risks throughout an enterprise should normally rest with the party that has the most opportunity to ensure that they are effectively controlled. Many of these controls, though, are often ``owned" by more than one party in today's businesses, making their assessment all the more challenging. That is one process to which today's strategically oriented risk managers can contribute.

But what about all those other risks that aren't necessarily insurable and, in most cases, have not historically come under the charge of the risk manager? They are risks that matter because they can threaten one or more of a company's key objectives and because they could be addressed by controls implemented by an individual within the company structure. Consequently, risk managers should be concerned about these risks. That concern should stem from the need for comprehensive risk management.

As a result, a risk manager must have a direct interest in the effectiveness of all controls. Many of these controls, particularly those of the financial variety, will factor into a Sarbanes-Oxley compliance initiative. And though

compliance with the Sarbanes-Oxley Act stresses financial reporting controls, many operational controls will also be addressed by these efforts.

Although the Sarbanes-Oxley compliance effort is typically led by a company's finance department and/or its internal audit department, the risk manager must be familiar with both of these areas. By developing relationships with key entities and individuals with a stake in risk control, risk managers can plug into the control structure monitoring system to effect some degree of oversight and to develop their own insight as to how well the controls that are in place are functioning. This should be true even if risk managers have no formal process for evaluating noninsurance risks and the controls, processes and objectives that relate to them. Only through a thorough understanding of the company's overall control structure and its relationship to risk and objectives can a risk manager expect to move beyond responsibility that is limited solely to insurable risks and take on a broader accountability for all significant or material risks.

Sarbanes-Oxley compliance efforts have quickly developed into major enterprisewide initiatives. As a result of the priority status and resources they have received, those risk managers who establish their connections to those efforts have an unprecedented opportunity to develop a wider approach to managing risks regardless of insurability.

On the downside, these efforts can involve such detailed assessment that getting too close to them can slow down or even stall a truly holistic approach to risk management. After all, as important as Sarbanes-Oxley compliance has become for all public companies, it is narrowly focused on financial reporting risks and controls and is only a subset of the broader group of significant risks that must be effectively managed in order for companies to meet their key objectives. That being true, it is critical to carefully plan how to ensure that all key risks are appropriately addressed.

So, where should you start? If you're not currently involved in the noninsurable risk control structure of your company, take the initiative to develop relationships with those in charge of key control structures. Get to know your internal auditor and develop the ability to assess the results of his or her audit work, which will clearly indicate the extent to which your company's control structure is effective. After all, your D&O underwriter has a direct stake in that assessment and will expect you, as the risk manager, to be able to articulate it.

The success of risk management at any company is significantly affected by the level of integration and cooperation among its key risk control stakeholders. Each company will populate this group a bit differently, but you should know who its members are and gain their respect and understanding for your interest in the risk control structures they oversee. It will go a long way toward making the contribution of which all risk managers are capable.

Would you like advice from an experienced colleague on a risk management, benefits management or actuarial problem? Three regular features in the Perspective section of Business Insurance can give you some answers.

This month's column on risk management issues is written by Christopher E. Mandel, assistant vp-enterprise risk management at USAA Group in San Antonio, the 2004 Risk Manager of the Year and past president of the Risk & Insurance Management Society Inc.

Address your questions to ASK, Business Insurance, 360 N. Michigan Ave., Chicago, Ill. 60601-3806. Please give us your name, title and employer; however, Business Insurance will consider unsigned letters.