Board Perspectives: Risk Oversight

Gaining Traction With Enterprise Risk Management

Issue 49

Enterprise risk management (ERM) is an enigma. Line up 10 experienced business people and ask them what it is and you'll likely get 10 different answers. While companies may believe they are implementing ERM, what we see in practice often demonstrates a very limited perspective. For example, companies may maintain a list of risks ("enterprise list management") or summarize risk responses as part of an annual review process, leaving us underwhelmed, given the speed of business and the ever-changing and disruptive business environment.

Many senior executives approach the topic of ERM with caution because they don't understand how it would fit within their organization. There is little tolerance for imposing an overlay or appendage onto established processes. The truth is, ERM isn't easy to implement. So, how do organizations succeed in gaining traction with it?

Key Considerations

Many efforts to implement ERM are unfocused, severely resource-constrained, and pushed down so far into the organization that it is difficult to establish their relevance. The near-term results are "starts and stops" and ceaseless discussions to understand what the objectives are. Risk is often an afterthought to strategy and risk management an appendage to performance management. Ultimately, the ERM implementation runs out of steam and fades away. While there is no one-size-fits-all solution, the following design principles will help overcome these issues:

1. **Define the primary objectives of the risk management process.** What do executive management and the board of directors want to accomplish with risk management? The activities of the risk management process typically include the identification, sourcing, measurement, evaluation, mitigation and monitoring of risk. However, the purpose of the process varies from company to company. One company may seek to reduce performance variability to an acceptable level and prevent unwanted surprises. Another company may seek to facilitate taking more risk in the pursuit of value creation opportunities. Still another might want to position itself as an early mover in the marketplace relative to its competitors. The point is, management needs to have a clear view as to what it intends to accomplish through ERM.

2. **Integrate the process with the core business activities.** No matter what the process is, its effectiveness and relevance diminishes greatly if it isn't integrated with what matters. The nature and extent of integration vary across industries and companies, and are highly dependent on management's operating style. The scope of integration could include one or more core management activities such as strategy-setting, annual business planning, performance management and budgeting. Effective integration can result in risk management becoming more aligned with the rhythm of the business so that it can make value-added contributions to the establishment of sustainable competitive advantage and the improvement of business performance over time.

3. **Determine whether the organization's culture will help or obstruct the implementation process to ascertain the extent of needed change.** Even the most well-intentioned risk management process can be compromised if dysfunctional organizational behavior exists and is allowed to fester. If the chief executive officer is not willing to pay attention to the warning signs posted by the risk management function; the reward system is not sufficiently balanced with the long-term interests of shareholders; the board is not asking tough questions about the assumptions and risks underlying the strategy; or risk management is so mired in minutiae that it is not focused sufficiently on strategic issues, it is not likely risk management will have an impact at the crucial moment when a contrarian voice is needed. Every effort should be made to transition to a culture that is conducive to effective risk management. Such a culture encourages open communication, sharing of knowledge and best practices, transparent risk reporting, continuous process improvement, and a strong commitment to ethical and responsible business behavior. Transitioning to such a culture takes time.

4. **Determine the enhancements to infrastructure that are needed.** Given the nature of the organization's risk management process, the core management activities with which that process is to be integrated, and the strengths and limitations of the organization's culture, is the organization's *existing* infrastructure sufficient to get the job done? By infrastructure, we mean the company's policies, internal activities, organizational structure, reporting and systems related to managing risk. If the answer is "yes," then we move on. If the answer is "no," the next question becomes: "What changes are needed?" Changes could include any combination of things, including a risk management policy, more explicit dialogue around risk appetite, a risk management committee, a chief risk officer, improved risk reporting, a crisp delineation of board and management responsibilities, and more reliable systems and data.

5. **Align the analytical risk assessment approach with the unique characteristics of the risks the company faces.** While risk maps, heat maps and other traditional risk assessment approaches may create awareness through a quick overview of risk when a company begins implementing ERM, they can lose their value and grow stale over time as managers struggle to use them as a basis for incorporating actionable steps into the business plan. Why subject risks with different characteristics to the same assessment methodology? For example:

   - Strategic risks warrant the use of a contrarian analysis approach applied to the critical assumptions underlying the strategy.

   - Operational risks require an assessment of the various components along the value chain within which the organization's business model is applied to assess exposure to loss of key suppliers, major customers, and logistics, among other things.

   - Financial risks are more susceptible to the use of measurement tools as they relate to cash flows and market, credit, currency and other related risks.

   - Compliance risks require analysis of the organization's conformance with specific laws, regulations, internal policies and/or contractual arrangements.

   The point is to use the appropriate analytical framework according to the unique characteristics of the risks being assessed.

6. **Assign ownership of the risk assessment process to the managers who are best positioned to achieve expected actionable results.** Engage the appropriate managers who are best positioned to own the risk assessments as well as the appropriate responses to act on the assessment results. For example, ownership will vary for strategic, operational and compliance risks. Holding the appropriate managers accountable for driving and owning the risk responses is fundamental to any effort to integrate risk management into strategy-setting, business planning and performance management.

7. **Support the ERM implementation from the top.** The above design principles define what executives should be looking at when evaluating the role and effectiveness of risk management within the organization. They give way to this last principle: Without support from the top, it's game over.

When implementing ERM, there should be a strong bias toward keeping things as simple as possible and leveraging existing processes, tools and reporting mechanisms.

Questions for Directors

Following are some suggested questions that boards of directors may consider, in the context of the nature of the entity's risks inherent in its operations:

- Is the board satisfied there is a risk management process that provides a common framework for managing risk across the company? Does it make sense to integrate the discipline of risk management with one or more core management processes, such as strategy-setting and business planning?

- Are there cultural issues within the organization that could compromise the effectiveness of risk management?

- Is the infrastructure in place sufficient to accomplish the objectives management and the board wish to achieve with respect to risk management?

- Are the organization's analytics appropriate for the risks it is facing? Is the board receiving the risk reporting it needs to execute its risk oversight responsibilities?

How Protiviti Can Help

Protiviti assists directors and executive management in public and private companies with identifying and managing the organization's key risks. We provide an experienced, unbiased perspective on issues separate from those of company insiders, and an analytical assessment approach aligned with the unique characteristics of the risks the company faces. We assist companies with implementing an enterprisewide approach to managing their risks that is aligned with the rhythm of how the organization is run and managed.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit. Through our network of more than 70 offices in over 20 countries, we have served more than 35 percent of FORTUNE 1000® and FORTUNE Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Protiviti is partnering with the National Association of Corporate Directors (NACD) to publish articles of interest to boardroom executives related to effective or emerging practices on the many aspects of risk oversight. As of January 2013, NACD has been publishing online contributed articles from Protiviti, with the content featured on www.directorship.com/author/jim-deloach/ in the "Blogs & Opinion" section. A compilation of blog posts and articles is maintained and categorized by author's name. Twice per year, the six most recent issues of *Board Perspectives: Risk Oversight* will be consolidated into a printed booklet that will be co-branded with NACD. Protiviti will also post these articles at Protiviti.com.

protiviti®

Risk & Business Consulting.
Internal Audit.