

# CorporateGovernor

Providing vision and advice for management, boards of directors and audit committees Winter 2010

## Is ERM right for your organization?

**Warren Stippich**, Business Advisory Services Partner  
**Bailey Jordan**, Business Advisory Services Partner

In the wake of Wall Street's recent economic upheaval, corporate risk has received unprecedented national exposure, with governance organizations, stock exchanges, the media, ratings agencies and stakeholders sharpening their focus on enterprise risk management (ERM) and its role within companies today.



As the leading approach to managing and optimizing risks, ERM determines how much uncertainty is acceptable within an organization, providing companies with a strategic risk analysis that cuts across business units and departments and considers end-to-end processes. By adopting ERM, a company gains the ability to align its risk “appetite” and tolerance with business strategy. As a result, management can better manage risk “opportunistically”—they can identify events that could have an adverse effect, determine whether the benefits outweigh the risks and develop an action plan to manage them. In other words, proper risk management allows organizations to examine and evaluate opportunities and create value by taking risks carefully.

By adopting ERM, a company gains the ability to align its risk “appetite” and tolerance with business strategy.

### In this issue

- 1 Is ERM right for your organization?
- 4 Conflict-of-interest internal audit

With risk management making headlines, discussions regarding ERM implementation have gained momentum as boards pressure management to ensure that unanticipated surprises and systemic risks are few and that those uncertainties are handled appropriately. Despite this push, management is often skeptical of ERM's benefits in light of its perceived implementation challenges and the mixed messages of its success.

[continued>](#)

## Is ERM right for your organization? (continued)

There are various ERM frameworks that define the essential components and provide guidance:

- The Committee of Sponsoring Organizations of the Treadway Commission (COSO), **Enterprise Risk Management — Integrated Framework** (2004)
- Joint Australian/New Zealand Standard, **AS/NZS 4360:2004, Risk management** (August 2004)
- International Organization for Standardization, **ISO 31000:2009 Risk management — Principles and guidelines** (November 2009)

North Carolina State University in partnership with the American Institute of Certified Public Accountants recently addressed this issue in their *Report on the Current State of Enterprise Risk Oversight*, which surveyed approximately 700 companies on the topic of ERM. According to the study, 44 percent of respondents had no ERM process in place and no plans to implement such a system. It's clear from these results that there are many organizations where management still questions ERM's value.

Participants whose organizations had not implemented an ERM process were asked to provide their rationale for this decision (respondents could list more than one reason). The most common responses were competing priorities (61 percent) and insufficient resources (60 percent), followed by lack of perceived value (48 percent). Other responses included lack of board or senior executive ERM leadership (38 percent) and the perception that ERM adds bureaucracy (37 percent).

These results raise the question, is “full-blown” ERM right for every organization? Many may argue that the broad-scale implementation of ERM does not make sense for organizations with a simple business model, low headcount, few locations or a small number of products or services. However, for those companies that have rejected the idea of a formal ERM initiative, there are a number of ways they can still benefit from embodying an ERM approach without the perceived investment of money and resources.

What many companies may not realize is that they are already executing components of ERM without calling it a formal program – complying with laws, identifying and managing risks, conducting internal audits and assessing controls. Accordingly, companies that are hesitant to create an official ERM program should first examine their current risk management activities and take stock of those processes already in place.

Furthermore, ERM can be modified to meet an organization's needs, taking into account its size, structure, objectives, culture, risk profile, industry and financial position. With this in mind, organizations should consider implementing a more manageable “bite-sized” program that still utilizes the basic concepts of ERM, but is executable in phases, focuses only on the important risks and utilizes existing people and processes. A company may even consider developing a pilot program within a single risk area, as a means of reducing startup costs and limiting resource use.

For those considering establishing an ERM program at any level, here are some points to keep in mind:

### 1. Start at the top

Critical to the development of ERM is program leadership, which should begin at the top of an organization with executive management and cascade down into a company's business units. In addition, the assembly of a risk management committee may be beneficial, ensuring the appropriate individuals know what is expected of them throughout the process.

### 2. Develop a manageable “risk universe”

Once leadership has been determined, management should conduct an enterprise risk assessment to identify the organization's most critical risks and determine the risk universe. Taking into account the company's strategic objectives, operations, control environment and inherent risk, an enterprise risk assessment should examine the following risk areas, categorized in four broad, simple perspectives:

- **Financial risks:** Cash flow, types of investments and their safety, credit, impaired assets, inflation and deflation. Of particular importance are areas where accounting irregularities, financial restatements or fraud may occur.
- **Legal and regulatory risks:** Identify, quantify and manage litigation exposure and claims, whether civil or criminal or contractually driven.
- **Operational risks:** Information technology, improper payments, outsourced services and demand forecasting, as well as those specific to the company and industry.
- **Strategic risks:** Partnerships, technology innovation, unrealized merger/integration synergies, talent and succession planning, product/service innovation and new revenue streams.

continued>

## Is ERM right for your organization? (continued)

It is important to note that defining risk at too granular a level is a common pitfall for many organizations. To aid in this process, companies may choose to conduct brainstorming sessions as a means of identifying and ranking the top risks where they can get a good “bang for their buck,” including those areas that cross governance or business units.

### 3. Create an action plan that builds on the company's capabilities

After finalizing the risk universe, companies should create an action plan that clearly defines and prioritizes each risk and identifies activities for managing these risks effectively. The key is to keep this effort as simple as possible. A company should first look at its existing business processes, rather than inventing new activities, to create a risk management inventory that identifies functions or processes that are often already in place:

- SOX compliance efforts
- Management self assessments
- Internal audit function
- Established reporting process
- Any relevant technologies



### ERM under the radar

If your organization is hesitant to enter into a full-blown ERM initiative, here are five steps that can keep you moving in the right direction in terms of risk management:

1. Determine the risk tracking and measuring activities already taking place.
2. Document those risk tracking and measuring activities.
3. Explore enhancing the program.
4. Identify another name that more appropriately captures this activity.
5. Start small: Implement a pilot program to begin the dialogue of risk identification, tracking and measuring in your company.

### 4. Evaluate risk management activities with the company's resources and needs in mind

After evaluating its existing processes, management must then decide how much added capacity – if any – is needed to achieve the company's risk management objectives, by performing a gap analysis of its current and desired capabilities. Management may also need to weigh the expected costs of improving its capabilities against the benefits, choosing to implement only those activities of most value. This process should be ongoing, whereby changes, threats and potential obstacles are addressed on a regular basis. In addition, even if a program is working well, an organization should continue to review its practices, evaluating what works and what doesn't and making adjustments accordingly.

For many organizations, it is easy to understand how ERM could potentially add value, yet assigning the time, resources and capital to create such an initiative is often difficult. Whether or not ERM is currently on your company's to-do list, it is important to remember that ERM is achievable when focus and discipline are applied – building on what works, enhancing what is already in place and standardizing wherever possible.

Call the activity whatever you want. The point is that most companies are already doing something to identify, track and measure risk. By starting small and taking a top-down, cross-functional approach, ERM becomes less of a burden and more of a benefit, helping to provide your organization with a means of leveraging risks for greater performance, build a foundation for competitive advantage and ultimately establish itself as a market leader. •

# Cutting-edge governance, risk and compliance

## Conflict-of-interest internal audit

**Warren Stippich**, Business Advisory Services Partner

### Reviewing the effectiveness of your organization's processes for addressing conflicts of interest

Whether you are a U.S. SEC registrant complying with Sarbanes-Oxley requirements<sup>1</sup>, a private company, or a not-for-profit<sup>2</sup>, you will want to implement a conflict-of-interest policy, as well as audit the policy periodically to ensure effectiveness and compliance. The Institute of Internal Auditors defines a conflict of interest in its *International Professional Practices Framework Standards Glossary* as “Any relationship that is, or appears to be, not in the best interest of the organization. A conflict of interest would prejudice an individual’s ability to perform his or her duties and responsibilities objectively.” The conflict resides in a situation, not in an individual’s actions. So whether the conflict is real, potential or perceived, it must be managed.

To address this issue, many organizations have implemented conflict-of-interest policies. They differ for each organization, but they typically give employees explicit guidelines both on ethical behavior and on situations to avoid. Employees are usually asked to complete an annual questionnaire in which they certify that they have read and understand the policy and the penalties for noncompliance, disclose any conflicts, and promise to report any violations if they arise.

While implementing a policy provides a formal process for managing conflicts of interest, an organization shouldn’t stop there; it needs to monitor adherence to the policy. It is important to include conflicts of interest in any internal audit risk universe. The internal audit department — or an outside service provider — can help audit an organization’s conflict-of-interest practices in a number of ways:

#### In this issue

1 Is ERM right for your organization?

4 Conflict-of-interest internal audit

- Verifying that all employees and other persons of interest are circularized and have responded
- Examining the organization’s conflict-of-interest policy and related documentation
- Conducting interviews with relevant staff based on their knowledge of the processes and their involvement in applying the requirements of the conflict-of-interest policy
- Analyzing procedures for identification, assessment and mitigation of conflicts of interest
- Reviewing confidential reports maintained for all employees

continued>

**While implementing a policy provides a formal process for managing conflicts of interest, an organization shouldn’t stop there; it needs to monitor adherence to the policy.**

<sup>1</sup> For SEC registrants, the SOX requirements to demonstrate strong internal control drive an annual conflict check. Refer to Section 402 for additional information regarding conflict-of-interest disclosures.

<sup>2</sup> Organizations risk losing tax-exempt status if they do not guard against the conflicts of interest prohibited in 26 U.S.C. § 503.

## Conflict-of-interest internal audit (continued)

For the conflict-of-interest audit, each organization will have a checklist specific to its industry and entity structure, but some considerations are common to all sectors:

- Who are the owners of the conflict-of-interest program, do they have the right level of authority to enforce, and do they keep the policy up to date?
- Are circularization procedures followed? Is a lack of response handled properly?
- Are satisfactory procedures in place to prevent or resolve conflict-of-interest situations?
- Are proper guidelines provided to employees, and are those employees encouraged to identify and report conflicts of interest?
- Are sanctions for violations documented? Enforced?
- Are reported conflicts addressed appropriately, as set forth by management and the board?
- Does the organization report conflicts to the audit committee?
- Are stakeholders aware of the results of the program?
- Are there flaws in the program that leave it vulnerable to unreported conflicts?



An organization that inadequately addresses its conflicts of interest will risk reputational harm, noncompliance with legal requirements and perhaps even sanctions. Forward-thinking business leaders will recognize the importance of instituting clear processes to help ensure conflicts of interest are properly managed, as well as investing the time and resources needed to audit the effectiveness of the program. •

### About the newsletter

*CorporateGovernor* is published by Grant Thornton LLP. The people in the independent firms of Grant Thornton International Ltd provide personalized attention and the highest quality service to public and private clients in more than 100 countries. Grant Thornton LLP is the U.S. member firm of Grant Thornton International Ltd, one of the six global audit, tax and advisory organizations. Grant Thornton International Ltd and its member firms are not a worldwide partnership, as each member firm is a separate and distinct legal entity.

For additional information on the issues discussed in this newsletter, consult your Grant Thornton client-services partner.

### Contact information

Warren Stippich  
Partner  
Business Advisory Services  
Warren.Stippich@gt.com

Editor: Emily Ford, editors@gt.com

Content in this publication is not intended to answer specific questions or suggest suitability of action in a particular case. For additional information on the issues discussed, consult a Grant Thornton client-service partner.

© Grant Thornton LLP  
All rights reserved  
U.S. member firm of Grant Thornton  
International Ltd

www.GrantThornton.com