Crowe Horwath™

October 2009
Enterprise Risk Management

Enterprise Risk Management:

A Practical Plan to Get Going Now

Many companies have an idea, albeit vague, about enterprise risk management (ERM). But few have made real progress in planning or actual implementation. What is the holdup? A practical five-step approach can help companies get their arms around ERM … and begin to realize the benefits of integrated risk management.

Summary

Section 404 of the *Sarbanes-Oxley Act* proved to be an arduous process for many public companies, yet these requirements cover only a slice of the total risks facing businesses. A much wider range of factors – including strategic, operations, and compliance risks – lies outside of the financial reporting and internal controls areas of Section 404. Any of the wide spectrum of business risks can also damage a company's reputation, result in significant liability, and lead to substantial loss of business value, if not a company's demise.

Boards of directors have become increasingly aware of the need to manage the wider range of risks across the enterprise. They are looking for ways to meet their fiduciary responsibilities, manage their own personal liability, and improve the business. They are asking about and, in some cases, pushing strongly for a more coordinated and comprehensive process of managing risks – enterprise risk management, in other words.

Business leaders, however, are frequently at a loss on how to get started or how to make meaningful progress. They may question how ERM differs from the way they currently manage the business. A "core ERM project" is a practical way to take advantage of what is currently being done in the organization and move forward while managing costs out of the starting blocks.

The starting point is to identify the effectiveness of risk-related activities the organization has already put into place. Gaps are then identified and prioritized, thereby making significant progress on the journey to a more integrated, efficient, and value-driven approach to risk management.

Trends

ERM has been discussed for more than a decade, yet rarely implemented. In the mid-1990s, the Economist Intelligence Unit created an extensive ERM framework. Professional associations, from internal audit groups to audit committee members and chief financial officers, have discussed the subject at conferences, in papers, and in trade publications. Often, the discussion has remained largely academic or not actionable.

There is a genuine need for ERM, as business failures and scandals in recent years have illustrated. In complex businesses, it is unreasonable to expect senior executives to fully understand the risks, and the interrelationships of the risks that their people are taking, without the use of improved tools and better methods.

In an era of unprecedented emphasis on risk management, complacency is simply not an option. In addition to the Sarbanes-Oxley legislation passed in 2002, regulatory agencies and stock exchanges have new rules placing greater emphasis on risk assessment. High-profile accusations of corruption – involving civil litigation as well as criminal trials – continue to work their way through the courts and are covered extensively by the media. Less dramatic, but certainly of no less concern to stakeholders, is the loss in value that organizations have experienced because they did not manage key business risks appropriately. The end of scrutiny is nowhere in sight.

Challenges

In many organizations, risks are being managed but frequently in haphazard and fragmented ways. Many companies lose sight of the big picture and do not sufficiently link risk management activities to their business strategies.

Some risks are being identified and managed, but only with limited coordination. Other key risks are off the radar screen. Many activities are restricted to a controls-based or regulatory-compliance approach with individual requirements being managed too narrowly. There is minimal or no coordination to take advantage of value available in aggregating these

compliance risk management activities within an effective risk management approach.

The consequences of fragmented approaches can result in substantial write-offs and lackluster performance. The challenge most organizations face is getting beyond the ERM "talking stage," understanding what is already being done across the many different activities under way in the organization, and making significant headway on the ERM journey.

Benefits

The benefits of ERM can include:

- Promoting a broader understanding of risks;
- Putting in place a process to highlight the key risks, what is being done, and by whom;
- Bringing to light emerging risks earlier;
- Enabling organizational alignment to manage the risks and control the cost of compliance; and
- Allowing organizations to take on and effectively manage risks that their competitors cannot.

In addition, a successful ERM program will strengthen corporate governance, which tends to increase the confidence of stakeholders, including regulators.

Gaps

Risks to companies can be categorized in strategic, operational, reporting, and compliance areas – the four objectives of the integrated model introduced in 2004 by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission.

COSO's visual model for ERM resembles a complex Rubik's Cube,® and is daunting to many businesspeople. In addition to the four risk objectives mentioned, there are eight stages in the COSO ERM integrated framework.

The eight stages represent what is needed to achieve each of the objectives (strategic, operational, reporting, and compliance). Reading from top to bottom, the eight components start with "Internal Environment" and conclude with "Monitoring," and there is a clear sequence of activities; some of the interim stages include "Risk Assessment" and "Risk Response."

The remaining visible side of the cube outlines different levels of the organization. The categorization starts at the broadest level, the entity (or entire enterprise) and proceeds to a subsidiary level. This face of the model is designed to be tailored to each business depending on organizational structure.

Judging from the complexity of the COSO ERM model, the accompanying framework, and separate volume for application techniques, implementing ERM using this model as a starting point will not happen in most organizations, unless they have huge resources and flawless project management skills.

Solution

ERM is a worthy goal for all businesses, regardless of size. Risk management activities need to be tied to strategy and ultimately built into everyday business processes.

Making noteworthy progress on this journey does not require throwing the proverbial baby out with the bathwater. The following five-step project plan enables organizations to identify and coordinate activities they already have begun, identify risks not adequately managed, close gaps, and move forward.

The steps of this five-point plan are, in short, organizing your team, establishing a framework, assessing risks, inventorying current risk-response activities, and closing the gaps.

Leveraging existing knowledge and programs will go a long way to helping reduce the effort in getting started. For example, internal audit, the Sarbanes-Oxley 404 team, the compliance officer, IT security and privacy, or the insurance group, have already conducted some type of risk assessment.

Step 1: Organize the Effort
Assemble a project team, steering committee, and adopt a charter.

To start on the right foot, it is important to assemble the right people and agree on timelines and objectives. Organizing requires assembling a steering committee to oversee the project, a project team to do the primary work, and a charter to guide what will be done, when, and by whom.

Steering Committee. ERM processes need to be built with stakeholders in mind and designed to suit the needs of the organization. Since ERM is ultimately strategic in nature, it will never succeed without support from the chief executive officer and other C-suite officers. High-

level executives who could be recruited for this committee include the chief financial officer, general counsel, chief operating officer, and internal audit director.

Project Team. The group driving the process needs knowledge of business operations (not only the financials) and risk assessment skills. The more complex the business, the more operations people need to be on the project team. Ideally, the team leader should be someone who understands risk assessment.

Project Charter. This document clearly establishes the objectives – what the project team plans to deliver and in what time frame. Although ERM is a process, the charter recognizes that this is a project with a defined time span and deliverables that will recommend best ways to move forward.

Step 2: Establish a Framework Around Risk
Establish a model but keep it simple.

The COSO ERM model is comprehensive and useful, particularly for large organizations with huge resources. Many companies, however, need a simplified approach to get – started one that works from a basic and logical model: plan, do, check. The "planning" stage requires risk assessment, the "doing" stage involves developing a strategy for implementation, and the "checking" phase means monitoring processes for risk management.

A common understanding of key terms is necessary so committee members are on the same page when it comes to comprehending risk, risk management, and enterprise risk management. ERM remains an amorphous concept. Thus, it must be demystified. Some discussion of key terms is essential to move forward.

Risk. Inherent in any business venture, risk can never be eradicated. It is an opportunity for financial gain, as well as a hindrance to achieving business goals.

Risk management. In some minds, risk management means insurance. But it is a much broader concept. Risks can be categorized as strategic, operational, compliance, and reporting. Risk management is an organization's strategic response to risk.

ERM. Enterprise risk management enables organizations to identify and manage all significant risks in an integrated way. ERM covers a broad portfolio of risk. Risk assessments are firmly rooted in an understanding of the business, customers, and management's strategic objectives.

A common language enables efficient communication and minimizes the likelihood of misunderstandings. The training needed to ensure consistency will lead to improved "buy-in" from all groups affected. Likely byproducts will be a broader understanding of risk throughout the organization and wider acceptance of individual and departmental responsibilities for risk management.

Step 3: Risk Assessment – The Top 10
Avoid getting lost in the details. Think broadly about risk.

Rather than thinking in narrow terms, the largest risk your organization faces is not achieving its overall business objectives. These objectives emerge from the strategic direction set at the highest levels of the organization.

In a nod to David Letterman's famous top 10 lists, identify what the top 10 risks to your organization could be. Of course the list would not be funny, but confining it to 10 key risks (or five, or 15, depending on your organization) will keep your project team focused on the big picture rather than being mired in details.

One way to get your project team thinking more broadly about risk is to think about the needs and wishes of various stakeholder groups: customers, employees, regulators, management, shareholders, etc. What kinds of things could happen to disappoint members of these groups? You might expect to identify a universe of 30 to 50 risks, but you will need to prioritize.

This stage requires not only identification of key risks, but understanding where risks reside in the organization and weighing their significance. No list of top 10 risks will be the same for any two organizations. For some companies, Food and Drug Administration compliance risks are immensely important. Others may face bigger risks when it comes to commodity pricing. It is up to the project team to collaborate across the enterprise and come up with a list of key risks.

Step 4: Inventory Current Risk-response Activities

A high-level review assesses what your organization is already doing.

Most organizations are already doing a good deal of risk management, but the processes are isolated and fragmented. Risks related to internal controls over financial reporting, for example, are under scrutiny for public companies because of Sarbanes-Oxley compliance. Credit risks are managed centrally in many organizations, while human resources risks may be left to each business unit. This is the stage to inquire and document how much your organization is already doing to manage risk. Your project team will need to interview key people and ask questions in an open-ended way:

- How do you think about risk?
- When someone says "risk" what do you think?
- To which risks are you responsible for responding?
- How do you coordinate your risk mitigation or compliance activities with others in the organization?

Likely candidates to interview include the controller, chief financial officer, chief executive officer, heads of business units, general counsel, the director of human resources, compliance director (if your organization has one), head of quality, head of safety, credit risk director, and external auditor.

Avoid asking leading questions, but be aware of reactive versus proactive approaches. For example, is the person in charge of environmental risk merely carrying out someone else's orders or looking for new risk exposures? Establish a dialogue that brings out the reality of risk management activity without suggesting what it should be.

Developing ERM does not require discontinuation of existing risk activities and starting from scratch. Instead, you can build on existing activities that have proven value.

Step 5: Identify Gaps and Prioritize

Compare your inventory of current risk responses to the top 10 priorities.

Now that you know the top 10 risks that can impede achievement of your organization's business objectives, along with the risk-response activities currently being conducted, you can compare the two lists. Which risks are being adequately managed? Which are missing from the radar screen? Where is an initiative already in place to better understand and manage risks?

Once the gaps in risk response have been identified, the next step is to develop an approach to close the gaps. This begins with prioritizing which gaps have the greatest potential to derail achievement of your business objectives. Which would require the greatest deployment of human or financial capital? Which ones would demand outside resources? Which ones could be accomplished in the shortest time?

Many elements of your organization's existing structure may be sufficient and will be retained, but significant gaps will probably be found. These may be in risk management leadership, risk assessment methodology, specific technical skills, common processes, or technology capabilities. Internal cultural biases or paradigms may need to be changed as well.

Weighing the urgency and resources required, organizations then can develop specific strategies to close the most critical gaps. While keeping the desired end result in mind, each of the strategies can be slotted into an implementation plan, complete with action steps and a timeline. A process will need to be established for ongoing reporting of the progress to mitigate the risks, as well as periodic reassessment of the top 10 risks being tracked.

This stage may require additional information and interviews. If you have not adequately assessed a top 10 risk, for example, you probably do not fully understand the source of the risk, the probability of its happening, and the magnitude if it does occur.

Discuss ways to move forward with members of the steering committee, and let members of this group direct you to the appropriate people for answers.

Also, be alert for new risks, whether arising from the environment, regulatory changes, competitors, or new products.

Step 5 needs to include recommendations guiding the organization to improve ongoing risk management processes. Decisions will need to be made on how to best manage a risk and where it should be managed. Will you centralize certain activities, or embed them in specific processes or business units?

Conclusion

ERM is a multiyear journey. A well-defined and supported core ERM project, however, enables an organization to "jump start" the process, rather than delaying moving forward because the concept seems grandiose, costly, and unworkable. Delaying further on ERM very likely will mean losing ground to competitors.

Organizations are well advised to take stock of existing risk assessment as well as risk-response activities and build on them. At the end of the project, your steering committee and project team will realize the value of implementing the COSO ERM model and continuing the ERM journey. You will now be able to fold compliance activities, Sarbanes-Oxley processes, and other risk-response activities into your framework to keep it current and relevant. You will be in the position, and have the buy-in, to coordinate risk management activities across functions and departments.

The substantial project management, team-building, and risk assessment efforts needed to carry out a successful core ERM project are worth the investment and consistent focus. ERM enables better alignment between risk management and business strategy. It enables you to understand your organization's risk profile, maintaining an appropriate balance between risk and performance. ERM can lead to a competitive advantage over peers with a less disciplined approach to mastering risk.

Contact Us

Rick Julien is a partner specializing in risk management with Crowe Horwath LLP in the Oak Brook, Ill., office. He can be reached at 630.586.5280 or rick.julien@crowehorwath.com.

Todd Richards is a partner specializing in risk management with Crowe Horwath LLP in the Oak Brook, Ill., office. He can be reached at 630.586.5195 or todd.richards@crowehorwath.com.

Jonathan Marks is a partner specializing in risk management with Crowe Horwath LLP in the New York office. He can be reached at 212.692.3727 or jonathan.marks@crowehorwath.com.

About Crowe

Crowe Horwath LLP is one of the largest public accounting and consulting firms in the United States. Under its core purpose of Building Value with Values,® Crowe assists clients in reaching their goals through assurance, financial advisory, performance, risk consulting, and tax services. Crowe professionals provide public and private company clients with thought leadership in many sectors, including financial and diversified financial services, healthcare, government, private equity sponsored, inventory-based, retail, not-for-profit, higher education, and food and commodities. With 25 offices and more than 2,500 personnel, Crowe is recognized by many organizations as one of the country's best places to work. Crowe serves clients worldwide as a leading independent member of Crowe Horwath International.

www.crowehorwath.com

MOHAWK windpower

When printed by Crowe Horwath LLP, this piece is printed on Mohawk Color Copy Premium, which is manufactured entirely with Green-e certified wind-generated electricity.

RISK9030C