What is Enterprise risk management?

2016

Mark S. Beasley
Deloitte Professor of ERM and Director of the ERM Initiative
North Carolina State University

NC STATE Poole College of Management
Enterprise Risk Management Initiative

2801 Founders Drive
Raleigh, NC 27695
919.513.0901 | www.erm.ncsu.edu

What is Enterprise Risk Management?

Mark S. Beasley
Deloitte Professor of ERM and Director of the ERM Initiative

All organizations have to manage risks in order to stay in business. In fact, most would say that managing risks is just a normal part of running a business. So, if risk management is already occurring in these organizations, what's the point of "enterprise risk management" (also known as "ERM")?

Let's Start by Looking at Traditional Risk Management

Business leaders manage risks and they have done so for decades. Thus, calls for enterprise risk management aren't suggesting that organizations haven't been managing risks. Instead, proponents of ERM are suggesting that there may be benefits from thinking differently about how the enterprise manages risks affecting the business.

Traditionally, organizations manage risks by placing responsibilities on business unit leaders to manage risks within their areas of responsibility. For example, the Chief Technology Officer (CTO) is responsible for managing risks related to the organization's information technology (IT) operations, the Treasurer is responsible for managing risks related to financing and cash flow, the Chief Operating Officer is responsible for managing production and distribution, and the Chief Marketing Officer is responsible for sales and customer relationships, and so on. Each of these functional leaders is charged with managing risks related to their key areas of responsibility. This traditional approach to risk management is often referred to as silo or stove-pipe risk management whereby each silo leader is responsible for managing or elevating risks within their silo as shown in Figure 1 below.

Figure 1

Limitations with Traditional Approaches to Risk Management

While assigning functional experts responsibility for managing risks related to their business unit makes good sense, this traditional approach to risk management has limitations, which may mean there are significant risks on the horizon that may go undetected by management and that might affect the organization. Let's explore a few those limitations.

Limitation #1: There may be risks that "fall between the siloes" that none of the silo leaders can see. Risks don't follow management's organizational chart and, as a result, they can emerge anywhere in the business. As a result, a risk may be on the horizon that does not capture the attention of any of the silo leaders causing that risk to go unnoticed until it triggers a catastrophic risk event. For example, none of the silo leaders may be paying attention to demographic shifts occurring in the marketplace whereby population shifts towards large urban areas is happening at a faster pace than anticipated. Unfortunately, this oversight may drastically impact the strategy of a retail organization that continues to look for real estate locations in outlying suburbs or more rural areas surrounding smaller cities.

Limitation #2: Some risks affect multiple siloes in different ways. So, while a silo leader might recognize a potential risk, he or she might not realize the significance of that risk to other aspects of the business. A risk that seems relatively innocuous for one business unit, might actually have a significant cumulative effect on the organization if it were to occur and impact several business functions simultaneously. For example, the head of compliance may be aware of new proposed regulations that will apply to businesses operating in Brazil. Unfortunately, the head of compliance discounts these potential regulatory changes given the fact that the company currently only does business in North America and Europe. What the head of compliance doesn't understand is that a key element of the strategic plan involves entering into joint venture partnerships with entities doing business in Brazil and Argentina, and the head of strategic planning is not aware of these proposed regulations.

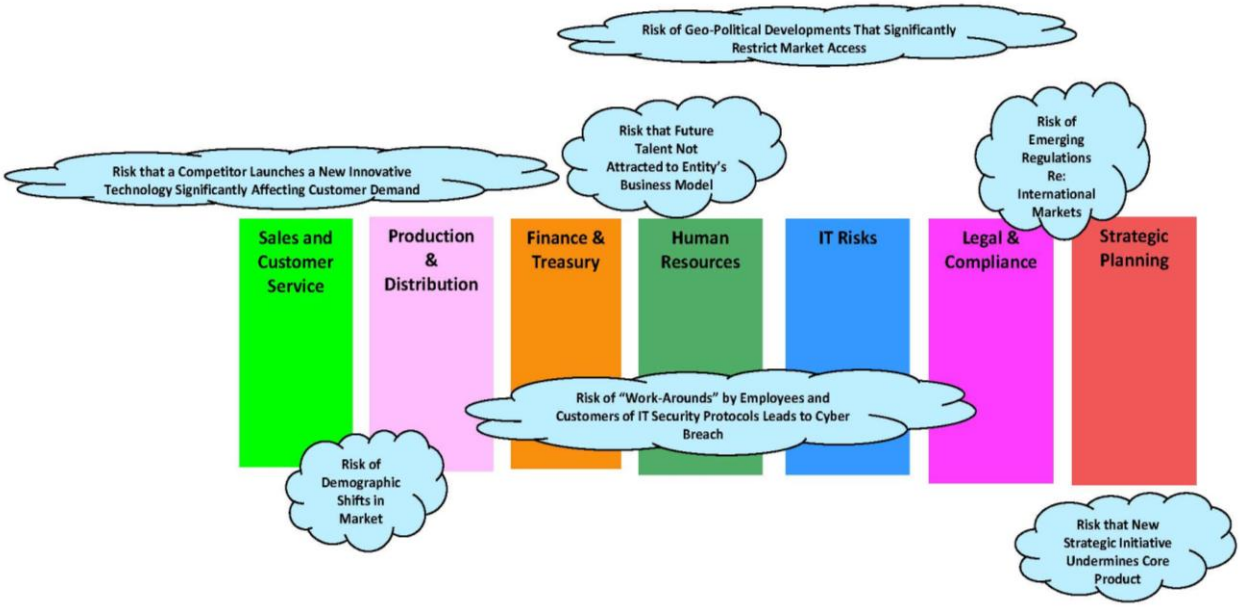
Limitation #3: Third, in a traditional approach to risk management, individual silo owners may not understand how an individual response to a particular risk might impact other aspects of a business. In that situation, a silo owner might rationally make a decision to respond in a particular manner to a certain risk affecting his or her silo, but in doing so that response may trigger a significant risk in another part of the business. For example, in response to growing concerns about cyber risks, the IT function may tighten IT security protocols but in doing so, employees and customers find the new protocols confusing and frustrating, which may lead to costly "work-arounds" or even the loss of business.

Limitation #4: So often the focus of traditional risk management has an internal lens to identifying and responding to risks. That is, management focuses on risks related to internal operations inside the walls of the organization with minimal focus on risks that might emerge externally from outside the business. For example, an entity may not be monitoring a competitor's move to develop a new technology that has the potential to significantly disrupt how products are used by consumers.

Limitation #5: Despite the fact that most business leaders understand the fundamental connection of "risk and return", most businesses are struggling to connect their efforts in risk management to strategic planning. For example, the development and execution of the entity's strategic plan may not give adequate consideration to risks because the leaders of traditional risk management functions within the organization have not been involved in the process.

The result? There can be a wide array of risks on the horizon that management's traditional approach to risk management fails to see, as illustrated by Figure 2. Unfortunately, some organizations fail to recognize these limitations in their approach to risk management before it is too late.

Figure 2



Embracing Enterprise Risk Management (ERM)

Over the last decade or so, a number of business leaders have recognized these potential risk management shortcomings and have begun to embrace the concept of enterprise risk management as a way to strengthen their organization's risk oversight. They have realized that waiting until the risk event occurs is too late for effectively addressing significant risks and they have proactively embraced ERM as a business process to enhance how they manage risks to the enterprise.

The objective of enterprise risk management is to develop a holistic, portfolio view of the most significant risks to the achievement of the entity's most important objectives. The "e" in ERM signals that ERM seeks to create a top-down, enterprise view of all the significant risks that might impact the business. In other words, ERM attempts to create a basket of all types of risks that might have an impact – both positively and negatively – on the viability of the business.

Leadership of ERM

Given the goal of ERM is to create this top-down, enterprise view of risks to the entity, responsibility for setting the tone and leadership for ERM resides with executive management and the board of directors. They are the ones who have the enterprise view of the organization and they are viewed as being ultimately responsible for understanding, managing, and monitoring the most significant risks affecting the enterprise.

Top management is responsible for designing and implementing the enterprise risk management process for the organization. They are the ones to determine what process should be in place and how it should function, and they are the ones tasked with keeping the process active and alive. The board of director's role is to provide risk oversight by (1) understanding and approving management's

ERM process and (2) overseeing the risks identified by the ERM process to ensure management's risk-taking actions are within the stakeholders' appetite for risk taking. (Check out our thought paper, ***Strengthening Enterprise Risk Management for Strategic Advantage***, issued in partnership with COSO, that focuses on areas where the board of directors and management can work together to improve the board's risk oversight responsibilities and ultimately enhance the entity's strategic value.[1]

Elements of an ERM Process

Because risks constantly emerge and evolve, it is important to understand that ERM is an ongoing process. Unfortunately, some view ERM as a project that has a beginning and an end. While the initial launch of an ERM process might require aspects of project management, the benefits of ERM are only realized when management thinks of ERM as a process that must be active and alive, with ongoing updates and improvements.

The diagram in Figure 3 illustrates the core elements of an ERM process. Before looking at the details, it is important to focus on the oval shape to the figure and the arrows that connect the individual components that comprise ERM. The circular, clockwise flow of the diagram reinforces the ongoing nature of ERM. Once management begins ERM, they are on a constant journey to regularly identify, assess, respond to, and monitor risks related to the organization's core business model.

Figure 3

Positioning ERM for Strategic Value

Because ERM seeks to provide information about risks affecting the organization's achievement of its core objectives, the starting point of an ERM process begins with gaining an understanding of what currently drives value for the business and what's in the strategic plan that represents new value drivers for the business. To ensure that the ERM process is helping management keep an eye on internal or external events that might trigger risk opportunities or threats to the business, a

[1] Visit our website – http://www.erm.ncsu.edu – to download this and the other thought papers highlighted in this document.

strategically integrated ERM process begins with a rich understanding of what's most important for the business' short-term and long-term success.

Let's consider a public-traded company. A primary objective for most publically traded companies is to grow shareholder value. In that context, ERM should begin by considering what currently drives shareholder value for the business (e.g., what are the entity's key products, what gives the entity a competitive advantage, what are the unique operations that allow the entity to deliver products and services, etc.). These might be thought of as the entity's current "crown jewels". In addition to thinking about the entity's crown jewels, ERM also begins with an understanding of the organization's plans for growing value through new strategic initiatives outlined in the strategic plan (e.g., entry into new geographic markets, launch of a new product, or the acquisition of a competitor, etc.). You might find our thought paper, ***Integration of ERM with Strategy***, helpful given it contains three case study illustrations of how organizations have successfully integrated their ERM efforts with their value creating initiatives.

With this rich understanding of the current and future drivers of value for the enterprise, management is now in a position to move through the ERM process by next having management focus on identifying risks that might impact the continued success of each of the key value drivers. How might risks emerge that impact a "crown jewel" or how might risks emerge that impede the successful launch of a new strategic initiative? Using this strategic lens as the foundation for identifying risks helps keep management's ERM focus on risks that are most important to the short-term and long-term viability of the enterprise.

With knowledge of the most significant risk on the horizon for the entity, management then seeks to evaluate whether the current manner in which the entity is managing those risks is sufficient and effective. In some cases, management may determine that they and the board are willing to accept a risk while for other risks they seek to respond in ways to reduce or avoid the potential risk exposure.

The Focus is on All Types of Risks

Sometimes this emphasis on identifying risks to the strategies causes some to erroneously conclude that ERM is only focused on "strategic risks" and not concerned with operational, compliance, or reporting risks. That's not the case. Rather, when deploying a strategic lens as the point of focus to identify risks, the goal is to think about any kind of risk – strategic, operational, compliance, reporting, or whatever kind of risk – that might impact the strategic success of the enterprise. As a result, when ERM is focused on identifying, assessing, managing, and monitoring risks to the viability of the enterprise, the ERM process is positioned to be an important strategic tool where risk management and strategy leadership are integrated. It also helps remove management's "silo-blinders" from the risk management process by encouraging management to individually and collectively think of any and all types of risks that might impact the entity's strategic success.

Output of an ERM Process

The goal of an ERM process is to generate an understanding of the top risks that management collectively believes are the current most critical risks to the strategic success of the enterprise. Most organizations prioritize what management believes to be the top 10 (or so) risks to the enterprise (see our thought paper, ***Survey of Risk Assessment Practices***, that highlights a number of different approaches organizations take to prioritize their most important risks on the horizon. Generally, the

presentation of the top 10 risks to the board focuses on key risk themes, with more granular details monitored by management. For example, a key risk theme for a business might be the attraction and retention of key employees. That risk issue may be discussed by the board of directors at a high level, while management focuses on the unique challenges of attracting and retaining talent in specific areas of the organization (e.g., IT, sales, operations, etc.).

Monitoring Top Risks with Key Risk Indicators (KRIs)

While the core output of an ERM process is the prioritization of an entity's most important risks and how the entity is managing those risks, an ERM process also emphasizes the importance of keeping a close eye on those risks through the use of key risk indicators (KRIs). Organizations are increasingly enhancing their management dashboard systems through the inclusion of key risk indicators (KRIs) linked to each of the entity's top risks identified through an ERM process. These KRI metrics help management and the board keep an eye on risk trends over time. Check out our thought paper, ***Developing Key Risk Indicators to Strengthen Enterprise Risk Management***, issued in partnership with COSO for techniques to develop effective KRIs.

Conclusion

Given the speed of change in the global business environment, the volume and complexity of risks affecting an enterprise are increasing at a rapid pace. At the same time, expectations for more effective risk oversight by boards of directors and senior executives are growing. Together these suggest that organizations may need to take a serious look at whether the risk management approach being used is capable of proactively versus reactively managing the risks affecting their overall strategic success. Enterprise risk management (ERM) is becoming a widely embraced business paradigm for accomplishing more effective risk oversight.

Interested in Learning More About ERM?

As business leaders realize the objectives of ERM and seek to enhance their risk management processes to achieve these objectives, they often are seeking additional information about tactical approaches for effectively doing so in a cost-effective manner. The ERM Initiative in the Poole College of Management at North Carolina State University may be a helpful resource through the articles, thought papers, and other resources archived on its website or through its ERM Roundtable and Executive Education offerings. Each year, we survey organizations about the current state of their ERM related practices. Check out our most recent report, ***The State of Risk Oversight Report: An Overview of Enterprise Risk Management Practices***.

Visit **www.erm.ncsu.edu** to learn more.

Mark S. Beasley, CPA, Ph.D., *is the Deloitte Professor of Enterprise Risk Management and Director of the ERM Initiative at NC State University. He specializes in the study of enterprise risk management, corporate governance, financial statement fraud, and the financial reporting process. He completed over seven years of service as a board member of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and has served on other national-level task forces related to risk management issues. He advises boards and senior executive teams on risk governance issues, is a frequent speaker at national and international levels, and has published over 90 articles, research monographs, books, and other thought-related publications. He earned his Ph.D. at Michigan State University.*