COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Strengthening Enterprise Risk Management for Strategic Advantage

www.coso.org

Many senior executives and their organization's board of directors are working to strengthen risk oversight so that they are better informed about emerging risk exposures, particularly those impacting strategy. COSO is issuing this thought paper to highlight key elements of enterprise risk management for board and senior executive consideration as they re-examine their existing approaches to risk oversight.

Strengthening Enterprise Risk Management for Strategic Advantage

Overview

The recent financial crisis is leading to renewed focus on how senior executives approach risk management and the role of their boards of directors in risk oversight. COSO is issuing this thought paper to foster dialogue among senior executives and their boards about ways to strengthen risk management in their organizations. We begin with a review of the environment that is generating calls for organizations to re-examine their risk management practices. We then highlight four specific areas where senior management can work with its board to enhance the board's risk oversight capabilities, which are further developed in the next four sections of this paper.

I. **Discuss Risk Management Philosophy and Risk Appetite.** Unless the board and management fully understand the level of risk that the organization is willing and able to take in the pursuit of value creation, it will be difficult for the board to effectively fulfill its risk oversight role. We outline our thoughts about the importance of management and the board achieving a shared understanding of the organization's risk philosophy and appetite as they seek to accomplish key organizational objectives.

II. **Understand Risk Management Practices.** For some organizations, risk management is ad hoc, informal, and implicit, leaving executives and boards with an incomplete view of the entity's top risk exposures. We provide an overview of key considerations for leaders seeking an enterprise view of risks in relation to the objectives they seek to achieve.

III. **Review Portfolio Risks in Relation to Risk Appetite.** Ultimately, management and the board need an understanding of the entity's portfolio of top risk exposures affecting entity objectives so that they can determine whether it is in line with the stakeholder's appetite for risk. We provide some perspectives on how senior executives might develop this enterprise-wide focus and provide relevant risk exposure information to the board for review.

IV. **Be Apprised of the Most Significant Risks and Related Responses.** Because risks are constantly evolving, a goal of risk management processes is to provide timely and robust information about risks arising across the organization. As management designs and implements key performance information, we encourage them to proactively include key risk indicators identifying emerging risks that may ultimately impact the achievement of key objectives.

COSO hopes this thought paper will serve as a basis for introspection about current approaches to risk management and be a catalyst for management to strengthen risk management for the purpose of enhancing the board's risk oversight capabilities and the organization's strategic value. We encourage boards and management to turn to COSO's ***Enterprise Risk Management— Integrated Framework*** for in-depth discussion of core components of enterprise risk management.

COSO, 2009

Opportunities for Improvement

Times of economic crisis often generate significant discussion and debate surrounding risk management in all types of organizations, with particular emphasis on the role of the board of directors in strategic risk oversight. Due to the widely-held perception that some organizations encounter risks for which they are not adequately prepared, boards, along with other parties, are often under increased focus during such times.

The complexity of business transactions, advances in technology, globalization, speed of product cycles, and the overall pace of change continue to increase the volume and complexities of risks facing organizations. There is a perception that some senior executives and their boards could be more aware of the risks they are taking, and could do more to prepare for potential downside risks. It is well recognized that organizations must take risks in order to add stakeholder value; however, there is growing interest in senior executive teams having more robust risk management capabilities in place that strengthen the board's risk oversight practices.

We continue to see an increased focus on risk management practices, particularly the effectiveness of board risk oversight efforts. This emphasis on risk oversight has been building for a number of years. The New York Stock Exchange's *2004 Final Corporate Governance Rules* require audit committees of listed corporations to discuss risk assessment and risk management policies. In 2008, credit rating agencies, such as Standard and Poor's, began assessing the enterprise risk management processes of rated firms across many industries as part of their corporate credit ratings analysis. We are seeing signals from some regulatory bodies suggesting that there may be new regulatory requirements or new interpretations of existing requirements placed on boards, and correspondingly on senior management, regarding risk oversight processes.

Comments from U.S. Securities and Exchange Commission (SEC) Chairman Mary Schapiro, speaking before the Council of Institutional Investors in April 2009, suggests new regulations may be

> *".....I want to make sure that shareholders fully understand how compensation structures and practices drive an executive's risk-taking.*
>
> *The Commission will be considering whether greater disclosure is needed about how a company — **and the company's board in particular** — manages risks, both generally and in the context of setting compensation. I do not anticipate that we will seek to mandate any particular form of oversight; not only is this really beyond the Commission's traditional disclosure role, but it would suggest that there is a one-size-fits-all approach to risk management.*
>
> *Instead, I have asked our staff to develop a proposal for Commission consideration that looks to providing investors, and the market, with better insight into how each company and each board addresses these vital tasks."*
>
> *Mary Schapiro, SEC Chairman*
> *April 2009*

emerging for greater disclosures about risk oversight practices of management and boards of public companies. In July 2009, an initial set of proposed rules were released by the SEC that would expand proxy disclosure information about the overall impact of compensation policies on the registrant's risk taking and the role of the board in the company's risk management practices. The SEC is also considering the need for potential new rules related to expanding disclosures about risk management processes in registrant quarterly and annual filings.

Legislation has also been introduced in Congress that would mandate the creation of board risk committees. In addition, the U.S. Treasury Department is considering regulatory reforms that would require compensation committees of public financial institutions to review and disclose strategies for aligning compensation with sound risk management. While the Treasury Department's focus has been on financial institutions, the link between compensation structures and risk-taking has implications for all organizations. Similar focus on board risk oversight is emerging outside the U.S., as evidenced by calls for materially increased board-level engagement in high-level risk oversight included in a July 2009 report on bank corporate governance commissioned by the Prime Minister of the United Kingdom.

In response to these emerging issues, some organizations are creating new positions to lead risk management efforts (e.g., creation of the CRO—chief risk officer—position). However, mere changes in the organizational chart alone may be insufficient to effectively manage risks as an integrated business process designed to achieve strategic goals and preserve and enhance stakeholder value.

Re-Examining Existing Risk Management

The 2008 financial crisis, coupled with global integration and the rapidity of change, has highlighted the benefits of more sophisticated risk management practices among senior executive leadership and improved risk oversight on the part of boards of directors for some organizations. Rapidly changing economic and market conditions give rise to unusual changes in risks for many organizations. Reliance primarily on historical experience in assessing risk exposures can leave some organizations ill-prepared to respond to a rapidly shifting economic environment. As a result, many senior executives and their boards are recognizing benefits of strengthening the integration of strategy development activities with a richer understanding of associated risks. Senior executive teams are considering whether there is a need to increase their level of investment in processes to quickly identify emerging risks affecting core objectives, given the realities of a rapidly evolving economic, market, and regulatory climate.

Attention has centered on executive compensation arrangements due to concern that some of those arrangements may have inadvertently encouraged excessive risk-taking by rewarding strong performance without appropriately taking into consideration the risks that were assumed in achieving that performance. For some, the scales may have tipped too far in the emphasis on performance without due consideration of risks. Going forward, boards are closely examining how compensation arrangements balance a focus on achieving key performance goals without exposing the organization to unintended risks. In fact, the SEC's proposed rules announced in July 2009

would require management to increase its disclosures of information that describe the overall impact of compensation policies on risk-taking.

Management is frequently being asked to provide their boards with more information regarding key risk exposures affecting the organization's objectives, including emerging strategic risks. In order to discharge their responsibility for risk oversight, boards are beginning to insist that management provide them reports on these risks with linkage to how they impact organization objectives and that agenda time be allocated to the discussion of key risk exposures affecting the achievement of key objectives. Boards are also increasingly engaged in overseeing management's monitoring processes to consider whether the risks assumed in pursuit of performance objectives are understood throughout the organization and remain within established limits. And, they are seeking information that sheds insight on how management's responses to existing risks might have long-term impact on the organization's achievement of long-term strategies and objectives.

Responding with an Enterprise View of Risk Management

How can senior executive teams strengthen risk management in a way that is both strategic and value-adding? COSO believes that implementation of enterprise risk management (ERM) provides the opportunity to achieve a robust and holistic top-down view of key risks facing an organization, and to manage those risks strategically to increase the likelihood that organizational objectives are achieved. Committed to improving organizational performance through better integration of strategy, risk management, control, and governance, COSO issued its ***Enterprise Risk Management—Integrated Framework*** to help boards and management understand an enterprise-wide approach to risk management. That framework is based on identified leading practices and the development of consistent terminology and approaches that can be used by many organizations in meeting their objectives. Recognizing that there is no one size fits all approach to ERM, COSO's framework highlights principles and elements of ERM as defined below:

> ***Enterprise risk management is a process, effected by the entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within the risk appetite, to provide reasonable assurance regarding the achievement of objectives.***
>
> ***COSO's Enterprise Risk Management – Integrated Framework (2004)***

Roles of the Board and Senior Management

As articulated in COSO's definition of ERM, an entity's board of directors plays a critical role in overseeing how management approaches enterprise-wide risk management. Because management is accountable to the board of directors, the board's focus on effective risk oversight is critical to setting the tone and culture towards effective risk management through strategy setting, formulating high-level objectives, and approving broad-based resource allocations.

Of course, the board's ability to effectively oversee an entity's risks starts with a rich understanding of the strategies and objectives the organization seeks to achieve. COSO's ***Enterprise Risk Management—Integrated Framework*** builds upon that kind of foundation to highlight four areas where the board can work with management to provide appropriate risk oversight related to those strategies and objectives:

- **Discuss risk management philosophy and risk appetite.** Risk appetite is the amount of risk, broadly defined, that an organization is willing to accept in pursuit of stakeholder value. All organizations encounter risks in pursuit of their goals, both long-term and short-term. Boards play a vital role in articulating a sense of their risk management philosophy and their willingness to accept risks, especially those risks that may be seen as outside the norm for the business and industry. Because boards represent the views and desires of the organization's key stakeholders, a critical starting point for risk management is for management and the board to develop a shared understanding of the organization's risk management philosophy and overall appetite for risk as they establish organizational strategies and objectives.

- **Understand enterprise risk management practices.** Management can review its existing risk management processes with the board and the board can then challenge management to demonstrate the effectiveness of those processes in identifying, assessing, and managing the organization's most significant enterprise-wide risk exposures likely to affect the achievement of the organization's objectives.

- **Review portfolio of risks in relation to risk appetite.** Effective board oversight of risks is contingent on the ability of the board to understand and assess the interaction of the organization's strategies and objectives with key risk exposures to determine whether those exposures are within the stakeholder's overall appetite for risk taking. Board agenda time and information packets that integrate strategy and operational initiatives with enterprise-wide risk exposures strengthen the ability of boards to gain comfort that risk exposures are consistent with overall stakeholder appetite for risk.

- **Be apprised of the most significant risks and related responses.** Risks are constantly evolving as the organization strives to achieve its objectives, creating a high demand for robust risk information. Regular updating by management (at all levels of the organization) of key risk indicators that are linked to objectives is critical to enhancing board oversight of key risk exposures for preservation and enhancement of stakeholder value.

The next sections of this thought paper build upon these four focus areas to provide more detail on the key responsibilities of the board of directors regarding risk oversight and the support needed from senior executives and others throughout the organization to strengthen risk management in all types of organizations.

I. Discuss Risk Management Philosophy and Risk Appetite

An entity's internal environment and the culture of the organization have a direct impact on the entity's risk management philosophy. That philosophy is reflected in the ways risks are considered in the development of the entity's high-level strategy and objectives and how those risks are considered in day-to-day operations to achieve those strategies and objectives. In order to provide ongoing risk oversight, board members require a rich understanding of the organization's risk philosophy, which allows them to consider whether the philosophy is consistent with stakeholder expectations for the entity and to adjust that philosophy to stakeholder expectations when it is misaligned. Indeed, it could be argued that prospective board members should fully consider the organization's risk philosophy as they evaluate joining the board.

An entity's risk management philosophy may be articulated explicitly in a policy document, or it may be merely reflected in the organization's culture, or the "way it gets things done." It is often helpful to have a well-developed risk philosophy that is understood and shared throughout the organization. Determining whether there is consistency in risk management philosophy across an organization can be difficult for board members, and even for senior management. Some firms use employee surveys or other tools to gauge the level of commitment to the risk management philosophy and the consistency of that commitment across the organization.

An entity's risk management philosophy and its risk appetite are closely related. Like risk management philosophy, a rich understanding of the stakeholder's overall appetite for risk-taking can serve to guide management and employees in their decision-making about strategies and objectives. Risk appetite, however, is more difficult to clearly and fully articulate than a risk management philosophy. Some entities struggle with defining levels of risk they are willing to accept in the pursuit of stakeholder value.

Identifying an Organization's Risk Appetite

As difficult as the process of describing risk appetite may be, it is critical that management fully share its view of the entity's appetite for risk and that the board evaluate whether that risk appetite has been set at the appropriate level in light of stakeholder expectations. Risk appetite will be a key consideration in objective setting and strategy selection. If an organization is setting very aggressive goals, then it should have an appetite for a commensurate level of risk. Conversely, if the organization is very risk averse, i.e., has a low appetite for risks, then one would expect that organization to set more conservative goals. Similarly, as boards consider specific strategies, they should determine whether that strategy falls within or aligns with the organization's risk appetite.

Unless the board fully understands the level of risk that management is willing and able to take in the pursuit of value, it will be difficult for the board to effectively fulfill its risk oversight responsibilities.

The nature of a firm's risk appetite will also be a key factor in dictating what constitutes effective risk management processes, so unless the board fully understands the level of risk that the

organization is willing and able to take in the pursuit of value, it will be difficult for the board to effectively fulfill its risk oversight responsibilities. In fact, financial and economic crises sometimes indicate that some boards may not fully appreciate the risks being taken by management, and if boards better understand those risks, they may be in better position to limit risk-taking that is well beyond an identified stakeholder appetite for risk.

In describing risk appetite, it is important to recognize that appetite can be articulated either qualitatively or quantitatively, and may be expressed in terms of ranges rather than exact amounts. As a starting point, management may consider those strategies that the entity would not be interested in pursuing due to the risk involved or the level of risk relative to the potential returns. For example, some companies might say that they will not enter international markets, or will not enter certain countries because they believe those activities are too risky. Others may believe that it is necessary to take those risks in order to achieve long-term success. Many of these types of discussions are occurring in strategy setting meetings as organizations chart their future direction.

By debating these boundaries of what the organization will and will not do, management is starting to articulate a risk appetite. Another way for entities to explore their appetite for risks is to go through a process of considering the impacts of past events and the reactions of key stakeholders such as shareholders, creditors, customers, employees, and regulators to gain some perspective of risks acceptable or not to key stakeholders. It may also be helpful to consider in a similar way hypothetical events that could occur in the future. Several key questions can be posed for discussion to solicit the viewpoints of senior executives and board members on the appropriate risk levels for the entity. For example:

- *Do shareholders want us to pursue high risk/high return businesses, or do they prefer a more conservative, predictable business profile?*
- *What is our desired credit rating?*
- *What is our desired confidence level for paying dividends?*
- *How much of our budget can we subject to potential loss?*
- *How much earnings volatility are we prepared to accept?*
- *Are there specific risks we are not prepared to accept?*
- *What is our willingness to consider growth through acquisitions?*
- *What is our willingness to experience damage to our reputation or brand?*
- *To what extent are we willing to expand our product, customer, or geographic coverage?*
- *What amount of risk are we willing to accept on new initiatives to achieve a specified target (e.g., 15% return on investment)?*

There are a number of key considerations to collectively take into account in developing an entity's risk appetite. Management benefits greatly by having a good understanding of its existing risk portfolio; that is, the categories and concentrations of risk inherent in its existing business as well as its capabilities relative to managing those risks. If an organization is particularly effective in managing certain types of risks, then it may be willing to take on more risk in that category. On the other hand, if the organization has a high concentration of risk in a particular area, then it may not have any appetite for taking on more risk in that area. Some entities may find that, through the

process of identifying and assessing risks to develop a thorough understanding of their risk portfolio, they have already exceeded their appetite for risk in certain categories, and may need to take additional steps to respond to those risks.

If the organization has a high concentration of risk in a particular area, then it may not have any appetite for taking on more risk in that area.

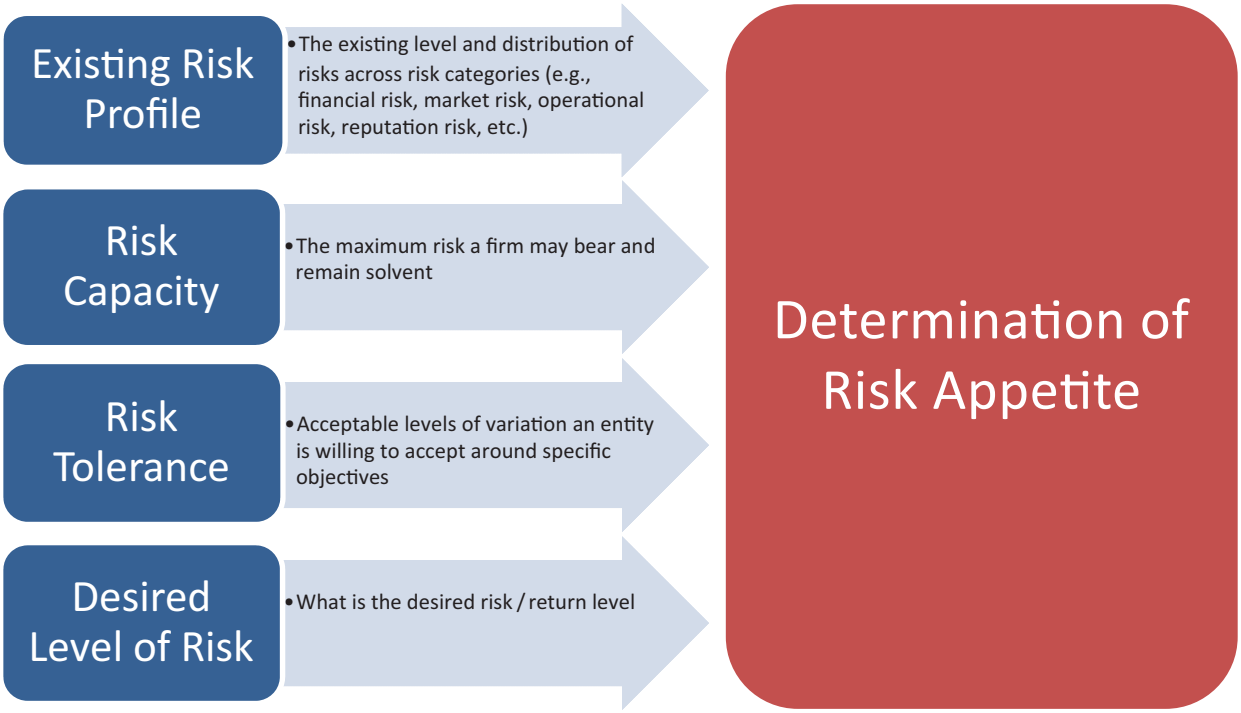
Another consideration when developing an organization's risk appetite involves an evaluation of the entity's risk capacity. Risk capacity refers to the maximum potential impact of a risk event that the firm could withstand and remain a going concern. Risk capacity is usually stated in terms of capital, liquid assets, or borrowing capacity. Risk appetite should not exceed an entity's risk capacity, and in fact, in most cases, appetite will be well below capacity.

An entity should also consider its risk tolerances, which are levels of variation the entity is willing to accept around specific objectives. Frequently, the terms risk appetite and risk tolerance are used interchangeably, although they represent related, but different concepts. Risk appetite is a broad-based description of the desired level of risk that an entity will take in pursuit of its mission. Risk tolerance reflects the acceptable variation in outcomes related to specific performance measures linked to objectives the entity seeks to achieve. So to determine risk tolerances, an entity needs to look at outcome measures of its key objectives, such as revenue growth, market share, customer satisfaction, or earnings per share, and consider what range of outcomes above and below the target would be acceptable. For example, an entity that has set a target of a customer satisfaction rating of 90% may tolerate a range of outcomes between 88% and 95%. This entity would not have an appetite for risks that could put its performance levels below 88%.

Most importantly, an entity should consider its stakeholders' overall desire for risk. Even if none of the other considerations significantly limit an organization's risk appetite, stakeholders may have conservative return expectations and a very low appetite for risk-taking. That would directly impact the articulation of risk appetite for the board and management.

Management often benefits from describing its risk appetite within each of its main categories of risk. For example, consider a company that is evaluating a new service offering that would involve providing ancillary services to existing customers using outsourced labor. One major benefit of this offering is that its start-up capital requirements are negligible. If the company has only defined its risk appetite in terms of the capital it is willing to put at risk in a new venture, this proposal may well move forward without consideration of the potential risks to the firm's reputation when it uses outsourced labor that it may not be able to fully control. If the company has articulated its appetite for reputational risk, then it should have some assurance that reputation risk issues will receive due consideration in the evaluation of the proposal.

Elements of Risk Appetite



The limiting factor in ultimately determining an entity's risk appetite could be any one of the four elements. Target levels of earnings per share, capital, or net operating cash flows are frequently used to express risk appetite for the board and management. For many organizations, there is a desire to avoid volatility in earnings, and therefore the tolerance levels for earnings per share results above or below target will serve to reflect an entity's risk appetite.

When describing risk appetite within different categories of risk, it may be desirable to use either quantitative or qualitative definitions. Where risk can be measured quantitatively, it can be relatively easy to hone in on the entity's comfort zone relative to the risks it takes on. But, often risk appetite is best defined qualitatively, such as high, moderate, or low. While qualitative measures may be less precise, they will still provide valuable guidance in assessing appropriate levels of risk taking.

Articulation of risk appetite will provide clarity over the risks the entity is willing to assume and allows consistent communications regarding strategy and risk management to different stakeholders and to employees throughout an organization. It sets the boundaries for the entity, linking strategy setting, target setting, and risk management processes. Having open discussions between senior management and the board of directors around risk appetite will help to avoid surprises and will form the basis for the development of strategies and objectives in the context of strengthened entity-wide risk management processes.

II. Understand Risk Management Practices

Any organization that is in existence today is performing some form of risk management—mere survival suggests that some degree of risk oversight is in place. The challenge for organizations, however, is that the process for managing the complex portfolio of risks can often be ad hoc and informal, leading to an incomplete understanding of the entity's top risk exposures affecting key objectives, including a lack of understanding of strategic risks. When risk management is underdeveloped, the concepts surrounding "risk" and "risk management" may be ill-defined leaving management with little basis but to assume that its leaders are in agreement about what constitutes risk for the organization, and that those risks are well understood across the organization and being managed to acceptable levels. Boards of directors can be left wondering whether the organization's risk management processes are effectively identifying the organization's key risk exposures affecting key strategies and objectives.

The recent crisis is causing some boards to re-examine their approach to risk oversight. Boards are turning to management with questions like:

- *"What are management's processes for identifying, assessing, and managing top risk exposures?"*
- *"How does management's process for managing risks consider whether risks being taken in the pursuit of objectives are effectively monitored to be sure they are within acceptable levels?"*
- *"What processes does management have in place to identify emerging risks affecting objectives and the related changes in risk prioritization in a rapidly changing environment?"*
- *"How is management monitoring key risks related to core strategic objectives?"*

In some organizations, management's responses to these questions are difficult to provide because there is minimal structure or definition as to how the organization approaches risk oversight.

Realizing Benefits of Changes in Risk Management and Board Oversight

Attention placed on risk management and the role of the board in risk oversight is leading to reminders about the importance of the fundamental relationship between risk and reward. As they consider how this risk/reward relationship is managed, boards are realizing that the level of management's investment in infrastructure and formal processes for managing and monitoring the return side of the risk/return relationship is fairly robust. In most situations, management has designed and implemented complex and sophisticated processes to identify, measure, and monitor performance through a variety of systems, processes, and tools. Examples of the level of investment in the return side infrastructure include formal processes and procedures surrounding strategic planning, forecasting tools and modeling, and financial reporting and accounting systems, among others. So, the level of management's investment in monitoring the return side of performance is often explicit, formal, and complex.

Risk vs. Reward

Thought Question: ***What is the level of investment in monitoring both sides of this relationship?***

In contrast, the level of management's investment in infrastructure and formal processes for managing and monitoring the risk side of the relationship can sometimes be underdeveloped and relatively immature. A lack of defined risk management processes can leave management in a position that requires them to implicitly assume that key business unit leaders across the organization are in agreement about how risk is defined for the organization, that leaders have self-identified effective methods for tracking risks for their areas of responsibility, that they understand the organization's objectives for risk management, including how risk management integrates with the organization's strategy, and that management (and the board) have reached consensus about the organization's top risk exposures. In some instances these issues are never discussed among management and the board, leaving risk management across the organization relatively informal and implicit.

Re-Examining Existing Risk Management Approaches

Senior executive teams and boards are considering whether existing levels of investment in risk management are adequate. In some organizations, the existing processes for managing risks have been ineffective in identifying on a consistent basis key risk exposures affecting the achievement of the entity's objectives.

While many traditional approaches to managing certain types of risk (e.g., insurance, legal, compliance, regulatory, etc.) are important and performed competently in most organizations, at times these risks are being managed in isolation with little consistency as to how risks are identified, assessed, managed, and communicated to senior leadership and the board. The result is that risk management processes can be left to the discretion of risk specialists with information about certain risk exposures who then communicate those exposures on an unstructured or reactive basis. As a result, boards and senior executives may be left with an incomplete understanding of the organization's top risk exposures and other functions within the enterprise can be unaware of how other risk exposures may be correlated with risks they encounter within their unit.

In some organizations existing processes for managing risks may be ineffective in identifying on a consistent basis key risk exposures affecting the achievement of the entity's objectives.

Incorporating Core ERM Principles to Strengthen Risk Management

Some senior executives are exploring ways to strengthen their risk management processes by embracing an enterprise risk management approach. To understand the core elements of ERM, we recommend COSO's ***Enterprise Risk Management—Integrated Framework***, which outlines key principles and concepts of enterprise-wide risk management.

COSO's definition of ERM (see earlier sidebar) summarizes several important elements of effective enterprise risk management. Each of these elements warrants consideration by management, with oversight from the board, as organizations seek to strengthen their enterprise risk management activities.

ERM is a process that is ongoing and flowing throughout the entity. Some business leaders misunderstand the concept of ERM and falsely view ERM as a fad, a project to be completed, a technology to be installed, or a new business unit or function to be created and funded. While ERM may involve some of these characteristics, the more important aspect of enterprise risk management is the need to design and implement a set of actions that can be continuously and iteratively applied throughout the enterprise as management and business unit leaders run the business.

For organizations where the approach to risk management is unstructured, ad hoc, or implicit, management may be challenged in its ability to effectively demonstrate to the board of directors and other key stakeholders that such processes are able to be continuously and consistently applied across the enterprise. Thus, boards of directors and other key stakeholders may not be easily persuaded that risks are being effectively managed on an enterprise-wide basis.

In our dynamic world, risks constantly change thereby requiring organizations to modify their objectives and strategies on an ongoing basis. In such an environment, it is naive to think that effective risk oversight can occur when the underlying risk management activities are unstructured, static, or separate from how the organization conducts its core business. Rather, proactive approaches to risk management include processes and activities that are intertwined within an organization's core activities so that risk management is performed on an ongoing, consistent basis by employees throughout an organization. That way, risk management becomes an integrated core activity that is applied continuously as the enterprise conducts its business and executes its strategy. Boards are looking to management to build an approach that leads to this integrated process view where risk management is ingrained in the everyday operation of the business.

In our dynamic world, risks are constantly changing thereby requiring organizations to modify their objectives and strategies on an ongoing basis.

ERM is effected by people at every level of the organization. Financial crises unfortunately often highlight that existing approaches to risk management in some organizations fail because they assign risk management to specific functions or activities that manage certain categories of risk, with little coordination across those risk functions as to how risks are managed and how they might interact to affect the enterprise as a whole. Education and training about risk management processes is sometimes lacking for personnel outside those functions or activities, causing others across the enterprise to not feel a sense of ownership for risk management within their areas of responsibility. In some cases, that leads to failure in identifying key risks affecting the enterprise. ERM, when viewed as part of an organization's key business processes and culture, helps to break down silos of risk management in an organization and instills a new "culture of cross-functional communication."

An enterprise-wide view of risk management is built upon the premise that ERM is effected by people ranging from the board and senior management to many other personnel across the enterprise. Similar to how an organization's strategies have to be developed and applied by people across an organization, an effective enterprise-wide perspective for risk management also requires the engagement of people spanning the organization. Because risks affect multiple aspects of an

organization and arise from both internal and external risk drivers, effective ERM is generally not accomplished by assigning risk management to isolated or independent persons or functions within the organization without the involvement of other personnel across the enterprise. Rather, an enterprise view of risk management usually benefits greatly from judgment and decisions made by individuals bringing a diverse range of knowledge, experiences, and perspectives to the ERM process. Thus, training opportunities focused on risk management processes may be necessary for people throughout the organization.

ERM is to be applied in strategy setting. Some individuals, upon first learning about an ERM approach to risk management, perceive it to be merely a compliance or bureaucratic exercise done separately from other activities to satisfy the expectations imposed by those within or outside the enterprise. That kind of viewpoint fails to see how ERM creates strategic advantage. Thus, risk management and strategy-setting activities are often viewed as separate and distinct, with risk management sometimes stigmatized as being a non-value adding, compliance, or regulatory function with no visible or clearly articulated connection to the organization's strategy. Unfortunately, to some extent the Sarbanes-Oxley legislation passed in 2002 exacerbated the notion of risk as being of a financial nature only when in reality sources of risk are much broader in terms of potential impact on an organization's business objectives and strategic goals.

Because risk and return are inseparable concepts, an ERM approach to risk management integrates management's processes for selecting the organization's strategies and objectives with their risk management activities. As emphasized in COSO's ERM definition, ERM is to be applied in strategy setting with an ultimate goal of contributing to the achievement of the entity's objectives. Thus, ERM is by definition designed to be strategic and value-adding.

Example Mapping of Strategies and Top Risk Exposures

	Strategic Initiative #1	Strategic Initiative #2	Strategic Initiative #3	…
Top Risk Exposures				x
Risk Exposure #1		x		
Risk Exposure #2		x		
Risk Exposure #3	x			x
…			x	

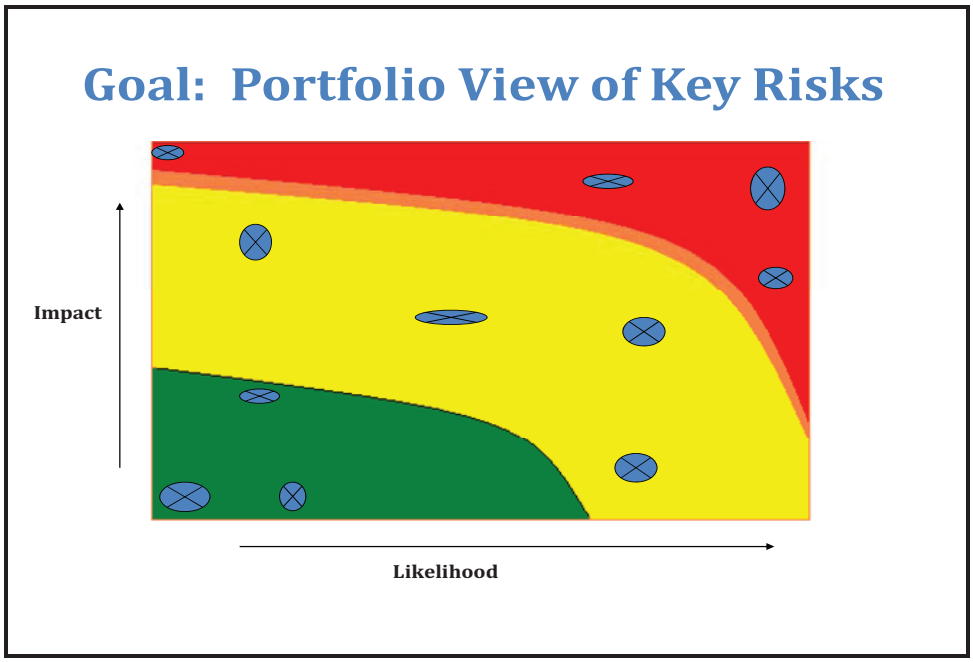
In fulfilling oversight roles related to strategic leadership and corporate governance, boards are seeking information provided by management that links an organization's key risk exposures with its core strategies and objectives. Developing an understanding of the linkages between top risk exposures and key strategies and objectives can help both management and the board to strengthen the value proposition for risk management and risk oversight by identifying where risks are overlapping within an individual strategy and where certain risks may affect multiple strategies.

III. Review Portfolio of Risks in Relation to Risk Appetite

By definition, *enterprise* risk management is designed to be deployed on an enterprise-wide basis. Value-generating activities are performed throughout the organization, with every level and unit of the organization charged with responsibilities for achieving specific objectives. Correspondingly, potential events can emerge at any level or unit that may affect the achievement of objectives at the business unit level or for the enterprise as a whole. As a result, ERM is designed to be applied across the enterprise, with a goal of creating an entity-level portfolio view of risk.

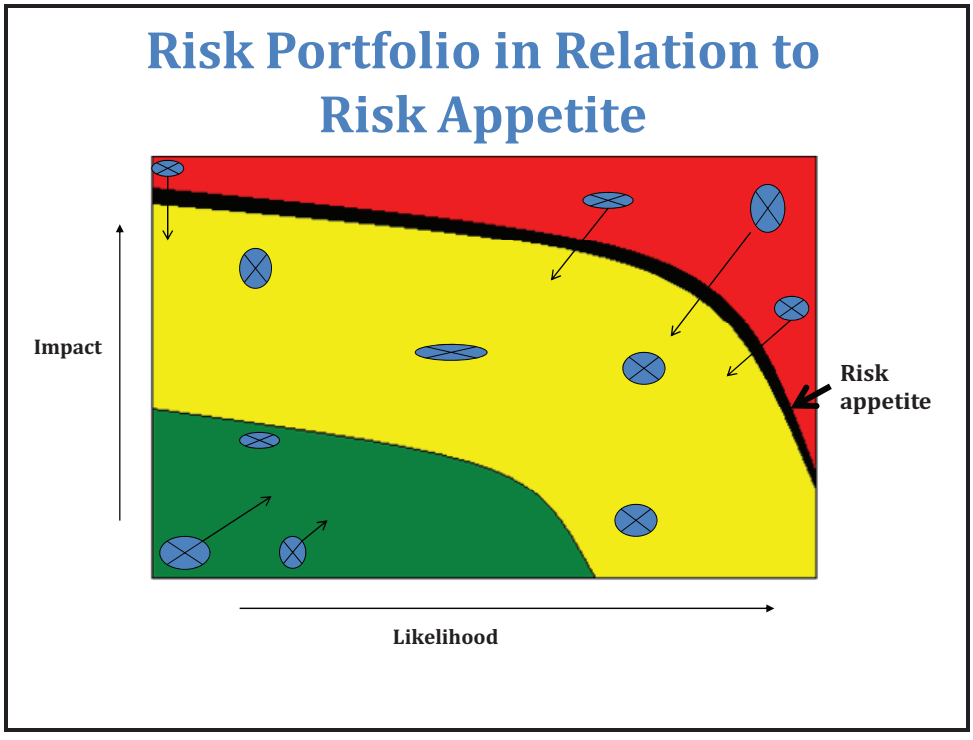
Risk management processes that capture risk information from each level of the organization aid in the creation of a composite view of key risk exposures for presentation by management and discussion with the board. A portfolio view of risks informs management and the board about concentrations of risks affecting specific strategies or overlapping risk exposures for the enterprise and helps in the prioritization of the enterprise's top risk exposures based on assessments of risk probabilities and impact to the organization. Discussion between the board and senior management about the organization's top risk exposures can help them stay focused on those risks with the greatest potential for impact on stakeholder value.

Heat maps (see an example below) are one type of tool that can provide an effective visualization that can help target board and senior management discussion on those risk issues critical to the organization. Other tools exist that can help management and the board understand the portfolio of key risk exposures. The use of such tools should be tempered by the realization that many of the risk events that played a significant role in prior financial crises are best characterized as low likelihood/frequency, but extremely high impact occurrences. These so-called "tail events" or "black swans" have proved to be extremely worthy of board attention and oversight.



Ultimately, board oversight is benefited by having a portfolio view of the organization's key risk exposures affecting the achievement of entity objectives so that it can view key risk exposures in the context of the entity's overall appetite for risks as it pursues those objectives. By balancing risk exposures with the entity's overall appetite for risks, management and the board are able to align the organization's activities to achieve objectives with the underlying risks that are attached to those activities. In some cases, that alignment may lead to adjustments in strategic initiatives to bring those activities more in line with the entity's overall appetite for risks.

In some instances, boards and senior management will identify a need to respond to certain risks in order to reduce their probability of occurrence or potential impact. At the same time, they may identify other areas where the organization's current responses are reducing risks too much, thereby minimizing potential returns for the organization. In those instances, the board and senior management may decide to increase the relative risk exposure to capture the potential for better returns, while staying well within the overall risk appetite. The graphic below attempts to convey that risk appetite may be non-linear in nature. That is, for some organizations, the potential impact (e.g., losses) of certain events is simply not tolerable—even at remote levels of likelihood. The black band depiction of the risk appetite also reflects that risk appetite may not be defined with complete precision.



By building risk management approaches on these foundational elements, management teams can increase their confidence that potential events are identified and managed on a timely basis to be within the organization's risk appetite so that the odds are improved that the organization's objectives are achieved.

IV. Be Apprised on the Most Significant Risks and Related Responses

Two important elements of a well-functioning ERM process are the free-flow of risk information throughout the organization (including the board of directors) and the monitoring of the risk management process to maintain confidence in its ability to develop and deliver relevant risk data about organizational objectives. This section discusses these two key elements from the perspective of both the board of directors, in its oversight role, and the senior management team of the organization, in discharging its responsibility to effectively manage the enterprise. Boards require relevant and timely information concerning key risks that is captured by the risk reporting system to oversee the efficacy of the organization's risk management approach. As well, senior management teams are recognizing the benefit from the broad perspectives that independent members of the board can offer with respect to emerging risks that have been identified and discussed in other organizations in which they are employed or serve in a similar board capacity.

Boards, in their role as independent overseers, cannot be expected to participate in the day-to-day management of risks encountered by the organizations they serve. The role of the board is to oversee whether the risk management processes designed and implemented by senior management and risk management professionals employed by the organization act in concert with the organization's strategic vision and overall risk appetite, as articulated by the board and executed by the senior management team. As well, the board can strive to understand whether they believe adequate attention is being paid to the development of a culture of risk-aware decision-making throughout the organization.

The organization's ERM system should function to bring to the board's attention the most significant risks affecting entity objectives and allow the board to understand and evaluate how these risks may be correlated, the manner in which they may affect the enterprise, and management's mitigation or response strategies.

An ERM system brings to the board's attention the most significant risks affecting entity objectives and allows the board to understand how these risks may be correlated, the manner in which they may affect the enterprise, and management's mitigation or response strategies. It is critically important for board members to have sufficient experience, training and knowledge of the business and objectives it seeks to achieve in order to meaningfully discuss the risks that the organization encounters. Some boards are increasing investments in and opportunities for director education to assist board members in developing a fundamental grasp of ERM concepts and risk management techniques. As seats on the board open due to retirements or the creation of additional directorships, the board may consider aggressively recruiting new members with directly relevant industry expertise and, if possible, a background that includes risk management experience. In fact, the SEC's proposed rules announced in July 2009 expand proxy disclosure requirements to include information about individual director risk management experience as part of the director nomination process.

The ability of the board to effectively perform its oversight role is critically dependent upon the unimpeded flow of information between the directors, senior management, and the risk management professionals in the organization. If the board is unsure whether it is receiving adequate information to allow directors to effectively discharge their risk oversight responsibility or the board is unsure whether management has sufficient information to execute risk mitigation strategies, the board may consider addressing different data needs with management. Examples of the types of information that may be warranted for board review include:

- *External and internal risk environment conditions faced by the organization,*
- *Key material risk exposures that have been identified,*
- *Methodology employed to assess and prioritize risks,*
- *Treatment strategies and assignment of accountabilities for key risks,*
- *Status of implementation efforts for risk management procedures and infrastructure, and*
- *Strengths and weaknesses of the overall ERM process*.

The Development and Use of Key Risk Indicators

Key risk indicators (KRIs) are metrics used by some organizations to provide an early signal of increasing risk exposure in various areas of the organization. In some instances, they may be little more than key ratios that the board and senior management track as indicators of evolving problems, which signal that corrective or mitigating actions need to be taken. Other times, they may be more elaborate, involving the aggregation of several individual risk indicators into a multi-dimensional risk score about emerging potential risk exposures. KRIs are typically derived from specific events or root causes, identified internally or externally, that can prevent achievement of performance goals. Examples can include items such as the introduction of a new product by a competitor, a strike at a supplier's plant, proposed changes in the regulatory environment, or input-price changes.

The development of KRIs that provide relevant and timely information to both the board and senior management plays a significant role in effective risk oversight.

The development of KRIs that can provide relevant and timely information to both the board and senior management is a significant component of effective risk oversight. Effective KRIs often result when they are developed by teams that include the professional risk management staff and business unit managers with a deep understanding of the operational processes subject to potential risks. Ideally, these KRIs are developed in concert with strategic plans for individual business units and can then incorporate acceptable deviations from plan that fall within the overall risk appetite of the organization.

It is also important to consider the frequency of reporting KRI's. The appropriate time horizon is dependent upon the primary user of a specific KRI. For operational managers, real-time reporting may be necessary. For senior management, where a compilation of KRIs that highlights potential deviations from organization-level targets is the likely goal, a less frequent (e.g., weekly) status report may be sufficient. At the board level, the reporting is often aggregated to allow for a more

strategic evaluation of the data. It is important to remember that a KRI does not manage or treat risk, and can lead to a false sense of security if poorly designed. Ideally, active assessment of the "predictive-ability" of each KRI is an ongoing facet of the organization's ERM process.

Elements of Well-Designed Key Risk Indicators (KRIs)

While risk oversight is ultimately a responsibility of the full board, boards often delegate primary responsibility for overseeing management's risk management processes and related identification of key risk exposures to a committee of the board. Often that delegation is to the audit committee. In doing so, boards are delegating oversight of management's risk management processes to the audit committee, but sharing with the full board oversight of outcomes (risk exposures) identified by that process. For example, risk exposures that are mitigated by internal controls might be overseen by the audit committee while risk exposures that affect the strategy of the organization are a full board responsibility.

If the board chooses to delegate primary risk oversight responsibility to a committee of the board, that committee should consider meeting in executive sessions with the designated ERM leader in a manner analogous to the audit committee and its regular sessions with the company's internal auditor, and with senior management in connection with CEO and CFO certifications of the financial statements. Senior risk managers as well as the senior executive team need to be comfortable in informing the board or relevant committee of rapidly emerging risk exposures that require the immediate attention of the board. Reporting channels that are open at all times strengthen board risk oversight capabilities. Regular reporting to the full board by the board committee charged with primary risk oversight helps keep the full board apprised of important changes in the organization's approach to risk management, its risk profile or exposure to key risks as signaled by well-designed KRIs that link risk exposures and objectives.

Conclusions

Despite growing interest in strengthening enterprise risk management, recently published research conducted by the ERM Initiative at NC State University (see *Report on the Current State of Enterprise Risk Oversight* (2009) at www.erm.ncsu.edu) suggests that the current state of enterprise-wide risk management across a wide spectrum of organizations may be immature. Executives in many of the organizations participating in that research study reported that they have not yet fully embraced the need for a top-down, enterprise-wide perspective of risk management.

Results from this research, and from COSO's own observations of the current state of risk management capabilities, lead us to believe that there are significant benefits that could be realized by having senior executives and boards give careful consideration to existing risk management processes in light of perceived increases in the volume and complexity of risks and operational surprises being experienced by many organizations. That, coupled with a self-described aversion to risk by some entities, is likely to spawn greater focus on improving existing risk management processes and the board's risk oversight.

This thought paper . . . is intended to help foster new dialogue between boards and senior executive leadership as they partner to more fully develop their organization's resiliency to risk.

This thought paper highlights key elements of enterprise risk management for senior executive consideration as they begin to re-examine existing approaches to risk management. It is intended to help foster new dialogue between boards and senior executives as they partner to more fully develop their organization's resiliency to risk and management's abilities to identify opportunities to take appropriate risks for competitive and strategic benefit.

As organizations strive to develop ERM processes into more mature business operating models, boards and management will need to be patient. Immediate success is rare—ERM must be viewed as a long-term cultural change and realistic expectations must be established for its implementation and evolution. There is, unfortunately, no "off-the-shelf" solution for organizations seeking to launch an effective enterprise-wide approach to risk management and oversight. Rather, there are numerous approaches to accomplishing an enterprise view of risks that organizations can tailor to fit their specific needs.

An executive summary of COSO's ***Enterprise Risk Management—Integrated Framework*** provides an overview of the key principles for effective enterprise risk management and is available for free download at www.coso.org. More detailed guidance, including examples about effective implementation of key ERM principles, is contained in the full two-volume set. COSO's objectives are to improve organizational performance through better integration of strategy, risk management, control, and governance. Our Frameworks are based on identified leading practices and the development of consistent terminology and approaches that can be used by many organizations in meeting their objectives. We hope that our ERM Framework will help in that journey to enhancing long-term stakeholder value.

COSO—The Committee of Sponsoring Organizations of the Treadway Commission

Board Members

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a voluntary private-sector organization comprised of the following organizations dedicated to guiding executive management and governance participants towards the establishment of more effective, efficient, and ethical business operations on a global basis. It sponsors and disseminates frameworks and guidance based on in-depth research, analysis, and best practices.

American Accounting Association
American Institute of Certified Public Accountants
Financial Executives International
Institute of Management Accountants
The Institute of Internal Auditors

ERM Initiative at North Carolina State University

Author Team

Mark S. Beasley
Deloitte Professor of Enterprise Risk Management

Bonnie V. Hancock
Executive Director, ERM Initiative

Bruce C. Branson
Associate Director, ERM Initiative

The ERM Initiative at North Carolina State University is pioneering thought-leadership about the emergent discipline of enterprise risk management, with a particular focus on the integration of ERM in strategy planning and governance. The ERM Initiative conducts outreach to business professionals through executive education and its internet portal (www.erm.ncsu.edu); research, advancing knowledge and understanding of ERM issues; and undergraduate and graduate business education for the next generation of business executives.

COMMITTEE OF SPONSORING
ORGANIZATIONS OF THE TREADWAY COMMISSION

www.coso.org