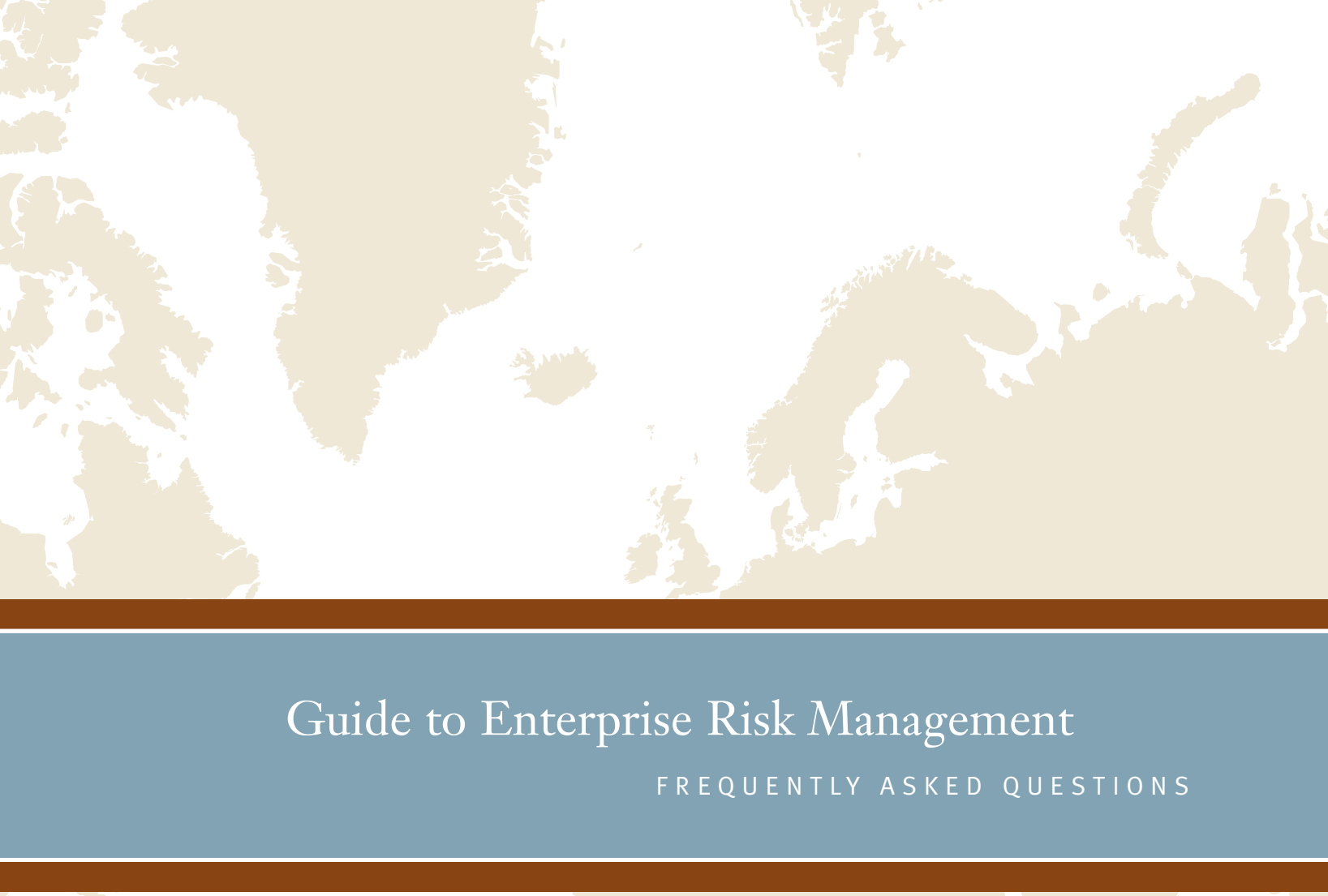


Guide to Enterprise Risk Management

FREQUENTLY ASKED QUESTIONS

protiviti®
Independent Risk Consulting

Business Risk | Technology Risk | Internal Audit

Guide to Enterprise Risk Management: Frequently Asked Questions

Table of Contents (continued)

Table of Contents (continued)

Table of Contents (continued)

Getting Started – Set the Foundation

Table of Contents (continued)

Table of Contents (continued)

Building a Compelling Business Case

Making it Happen

Relevance to Sarbanes-Oxley Compliance

Table of Contents (continued)

Introduction

In today's challenging global economy, business opportunities and risks are constantly changing. There is a need for identifying, assessing, managing and monitoring the organization's business opportunities and risks. The question is: How does an organization take practical steps to link opportunities and risks when managing the business? And further: What does this have to do with risk management?

In August 2004, the Treadway Commission's Committee of Sponsoring Organizations (COSO) issued its Enterprise Risk Management – Integrated Framework after completing a developmental project spanning a three-year period. The framework, which includes an executive summary and application techniques, expands on the previously issued Internal Control – Integrated Framework to provide a more robust and extensive focus on enterprise risk management (ERM). As explained in the foreword to the framework: "While [the framework] is not intended to and does not replace the internal control framework, but rather incorporates the internal control framework within it, companies may decide to look to this enterprise risk management framework both to satisfy their internal control needs and to move toward a fuller risk management process."

At Protiviti, we believe that ERM implementation should be integrated with strategy-setting. ERM redefines the value proposition of risk management by elevating its focus from the tactical to the strategic. ERM is about designing and implementing capabilities for managing the risks that matter. The greater the gaps in the current state and the desired future state of the organization's risk management capabilities, the greater the need for ERM infrastructure to facilitate the advancement of risk management capabilities over time. COSO's new framework provides criteria against which companies can benchmark their risk management practices and processes. The framework provides a common language that fosters communication among executives, directors, auditors and advisors, and we encourage everyone with an interest in implementing ERM to read and understand it.

Many are asking questions about the value proposition of ERM and practical steps on how to implement it. While we do not have all the answers, we attempt to address in this publication some of the most commonly asked questions with respect to ERM. This publication is designed to answer your questions without making you wade through material with which you are already familiar. It often refers to the COSO framework, which readers can obtain at **www.coso.org**. It offers ideas, suggestions and insights to executives responsible for ERM implementation. It is intended for use as a reference tool rather than as a book to be read from cover to cover. It is supplemented by Issue 6 of Volume 2 of *The Bulletin*, "Enterprise Risk Management: Practical Implementation Advice," which provides an overview for C-level executives and directors and is available at **www.protiviti.com**.

As companies gain more experience with implementing ERM, we expect to update this publication from time to time. If we do so, we will post information at **www.protiviti.com**. Protiviti periodically publishes ERM performer profiles on KnowledgeLeader℠ to provide ERM case examples and plans to publish a book including such profiles from time to time.

This publication is neither intended to be a legal analysis nor a detailed "cookbook" of steps to take in every situation. Accordingly, companies should seek out appropriate advisors for counsel on specific questions as they evaluate their unique circumstances.

Protiviti Inc.
January 2006

THE FUNDAMENTALS

1. What is Enterprise Risk Management (ERM)?

COSO defines ERM as *"a process, effected by an 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 its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."* This definition is broad for a reason. It reflects certain fundamental concepts, each of which is discussed on pages 5 through 9 of the COSO ERM framework. As summarized on page 5 of the framework, "enterprise risk management is:

- A process, ongoing and flowing through an entity
- Effected by people at every level of an organization
- Applied in strategy-setting
- Applied across the enterprise, at every level and unit, and includes taking an entity-level portfolio view of risk
- Designed to identify potential events affecting the entity and manage risk within its risk appetite
- Able to provide reasonable assurance to an entity's management and board
- Geared to the achievement of objectives in one or more separate but overlapping categories – it is "a means to an end, not an end in itself."

ERM is about establishing the oversight, control and discipline to drive continuous improvement of an entity's risk management capabilities in a changing operating environment. It advances the maturity of the enterprise's capabilities around managing its priority risks. Before a company can assert it is applying ERM, it must address ALL of the above concepts embodied in COSO's definition.

2. Why implement ERM?

Using the ERM definition articulated in Question 1, the overriding objective for implementing ERM is to provide reasonable assurance to an entity's management and board that the entity's business objectives are achieved. On pages 1 through 4 of the framework, COSO states that ERM assists management with aligning risk appetite and strategy, enhancing risk response decisions, reducing operational surprises and losses, identifying and managing cross-enterprise risks, providing integrated responses to multiple risks, seizing opportunities and improving deployment of capital. We agree with COSO's point of view and will further discuss it in this publication.

We believe there are six fundamental reasons for implementing ERM. Each serves to help elevate risk management to a strategic level. The six reasons are:

(1) *Reduce unacceptable performance variability*: ERM assists management with (a) evaluating the likelihood and impact of major events and (b) developing responses to either prevent those events from occurring or manage their impact on the entity if they do occur. Most companies focus on traditional risks that have been known for some time. Few companies have a systematic process for anticipating new and emerging risks. Therefore, many companies often learn of critical risks too late or by accident, spawning the "fire fighting" and crisis management which drains resources and creates new vulnerabilities. The strategic lens of ERM broadens the traditional risk management focus on low-probability and catastrophic risks to a more expansive view on reducing the risk of erosion of critical sources of enterprise value. ERM assists management with improving the consistency of operating performance by increasing the emphasis on reducing earnings volatility, avoiding earnings-related surprises, and managing key performance indicator (KPI) shortfalls. ERM improves the management of increasing risk mitigation costs and the success rate of achieving business objectives.

(2) *Align and integrate varying views of risk management:* There are many silos within organizations with a point of view on managing risk, e.g., treasury, insurable risk, EH&S, IT, and within business units. Silo mentality inhibits efficient allocation of resources and management of common risks, enterprisewide. When there are multiple functions managing multiple risks, there is a need for a common framework. For example, some organizations are:

- Assessing the need for a chief risk officer (CRO), including that individual's role, authority and reporting lines
- Integrating risk management into critical management activities, e.g., strategy-setting, business planning, capital expenditure and M&A due diligence and integration processes
- Linking risk management to more efficient capital allocation and risk transfer decisions
- Increasing transparency by developing quantitative and qualitative measures of risks and risk management performance
- Aggregating common risk exposures across multiple business units with the objective of understanding the greatest threats to enterprise value and formulating an integrated risk response

(3) *Build confidence of investment community and stakeholders:* As institutional investors, rating agencies and regulators talk more about the importance of risk management in their assessments of companies, management may be requested to disclose and comment on the organization's capabilities for understanding and managing risk to enable stakeholders to make informal assessments as to whether returns are adequate in relation to the risks undertaken. As companies increase the transparency of their risks and risk management capabilities, and improve the maturity of their capabilities around managing critical risks, management will be able to articulate more effectively how well they are handling existing and emerging industry issues.

(4) *Enhance corporate governance:* ERM and corporate governance are inextricably linked. Each augments the other. ERM strengthens board oversight, forces an assessment of existing senior management-level oversight structures, clarifies risk management roles and responsibilities, sets risk management authorities and boundaries, and effectively communicates risk responses in support of key business objectives. All of these activities are germane to good governance. By the same token, effective governance sets the tone for (a) understanding risks and risk management capabilities and (b) aligning risk appetite with the entity's opportunity-seeking behavior. Directors often ask, "What are the risks, how are they managed and how do you know?"

(5) *Successfully respond to a changing business environment:* As the business environment continues to change and the pace of change accelerates, organizations must become better at identifying, prioritizing and planning for risk. ERM assists management with evaluating the assumptions underlying the existing business model, the effectiveness of the strategies around executing that model, and the information available for decision-making. ERM drives management to identify alternative future scenarios, evaluate the likelihood and severity of those scenarios, identify priority risks and improve the organization's capabilities around managing those risks. As the environment changes, new risks emerge and are escalated in a timely manner for action and possible disclosure. These activities impact resource allocation for the organization as a whole.

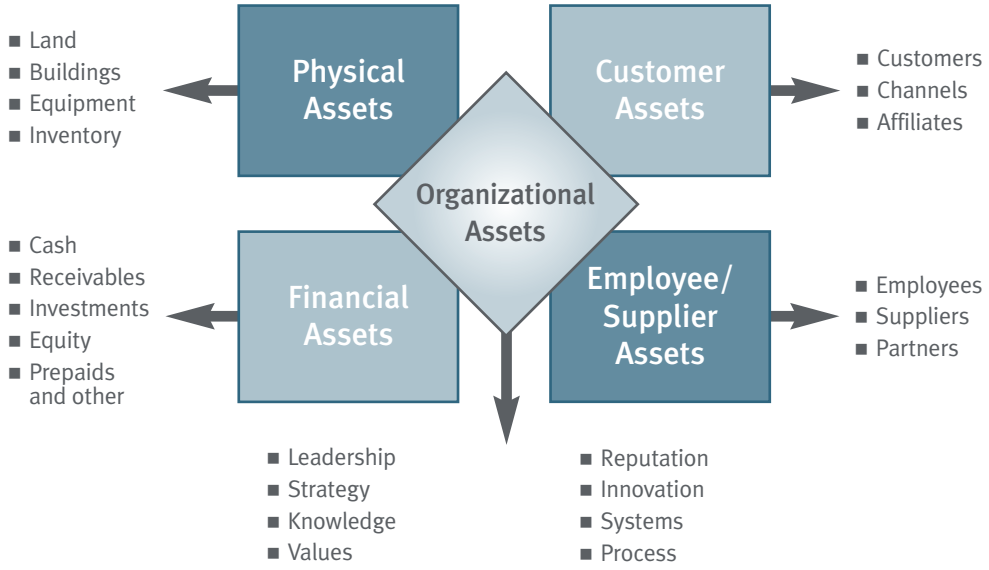
(6) *Align strategy and corporate culture:* ERM helps management create risk awareness and an open, positive culture with respect to risk and risk management. In such an environment, individuals can raise issues without fear of retribution. With respect to matters of enterprisewide importance, ERM often centralizes policy-setting and creates focus, discipline and control. It clarifies the distinction between risk-taking and risk-avoidance behaviors, improves tools for quantifying risk exposures, increases accountability for managing risks across the enterprise and facilitates timely identification of changes in an entity's risk profile. ERM encourages balance in both the entrepreneurial activities and control activities of the organization, so that neither one is too disproportionately strong relative to the other.

3. How does the scope of ERM compare to existing risk management approaches?

Traditional risk management approaches are focused on protecting the tangible assets reported on a company's balance sheet and the related contractual rights and obligations. The emphasis of ERM, however, is on enhancing business strategy. The scope and application of ERM is much broader than protecting physical and financial assets. With an ERM approach, the scope of risk management is *enterprisewide* and the application of risk management is targeted to *enhancing as well as protecting* the unique combination of *tangible and intangible assets* comprising the organization's business model. This point of view is consistent with COSO's assertion that ERM is applied both across the enterprise and in strategy-setting.

With market capitalizations often significantly exceeding historical balance sheet values, the application of risk management to intangible assets is critically important. Just as potential future events can affect the value of tangible physical and financial assets, so, too, can they affect the value of key intangible assets, e.g., customer assets, employee/supplier assets and organizational assets such as the entity's distinctive brands, differentiating strategies, innovative processes and proprietary systems. This is the essence of what ERM contributes to the organization – the elevation of risk management to a strategic level by broadening its application to ALL sources of value, not just physical and financial ones.

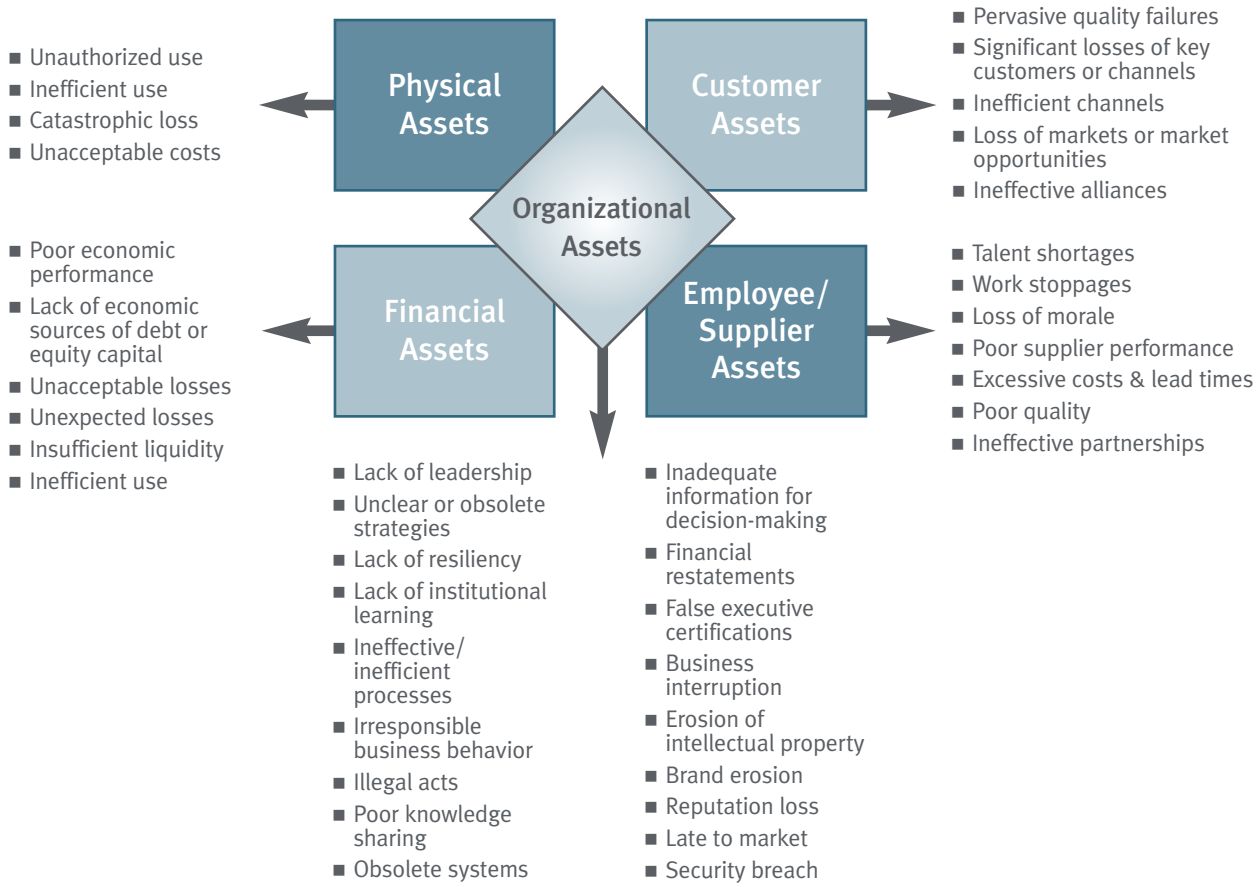
The five broad categories of assets representing sources of value, and examples within each category, are illustrated below[1]:



These five asset categories include sources of value underlying an organization's business strategy. By placing the emphasis on strategy-setting, ERM transitions risk management from a discipline of avoiding and hedging bets to a differentiating skill for enhancing and protecting enterprise value as management seeks to make the best bets in the pursuit of new opportunities for growth and returns. ERM invigorates opportunity-seeking behavior by helping managers become confident in their understanding of the risks and in the capabilities at hand within the organization to manage those risks.

[1] *Cracking the Value Code: See What Matters, Invest in What Matters and Manage What Matters in the New Economy*, Richard E. S. Boulton, Barry D. Libert and Steve M. Samek, HarperCollins, 2000.

The risk assessment process can lead to more comprehensive risk responses when management identifies potential future events that could affect each category of assets critical to the execution of the enterprise's business model. The schematic below illustrates categories of potential future events that might be considered during a risk assessment:



An enterprise's sources of value, whether tangible or intangible, are inherent in its business model. They are affected by sources of uncertainty which must be understood and managed as an organization works to achieve its performance objectives. They may be external or internal. For example, *environment risks* are uncertainties arising in the external environment affecting the viability of the enterprise's business model. *Process risks* are uncertainties affecting the execution of the business model, and therefore often arise internally within the organization's business processes. Because inadequate knowledge and information breeds more uncertainty, *information for decision-making risks* are uncertainties affecting the relevance and reliability of information supporting management's decisions to protect and enhance enterprise value. These three broad categories – environment, process and information for decision-making – provide the basis for understanding the sources of uncertainty in any business. As Question 75 illustrates, these risk categories include many subcategories of potential future events which could become the focal point for assessing risk and formulating appropriate risk responses.

In summary, uncertainty about the future creates risk and ERM broadens the focus of risk management to all significant sources of enterprise value. By understanding the key external and internal variables contributing to uncertainty in a business and monitoring trends in those variables over time, management can more effectively run the business and realize the potential of the enterprise's business model. The following table provides examples of observable events to illustrate this point.

ASSET CATEGORY	EXAMPLES OF EXPOSURES	SOME ILLUSTRATIVE VARIABLES FOR EVALUATING UNCERTAINTY
Physical	Physical facilities	Catastrophic occurrence probability of: - Maximum possible loss - Maximum foreseeable loss - Normal loss
	Production throughput	Defects occurrence probability Changes in backlog
Financial	Net monetary assets	Change in interest, exchange and inflation rates
	Business plan cash flow	Change in interest, exchange and inflation rates
	Total accounts receivable	Customer default probability
	Commodity holdings	Changes in oil, metals, power and other prices
	Equity holdings	Changes in stock prices
Customer	Customer base	Change in service quality index
	Revenue streams	Change in competitor pricing Returns occurrence probability
Employee/Supplier	Employee group	Change in change readiness index Health and safety incidents occurrence probability
	Strategic suppliers	Change in just-in-time performance ratings Change in quality ratings Change in raw materials prices
Organization	Brand image	Change in ability to deliver on brand promise
	Differentiating strategy	Change in quality, time and cost performance relative to competitors Change in customer expectations and wants
	Innovative processes	New technological innovations that obsolete existing process capabilities

For any of the key variables noted above that are relevant to a business, there are potential future events that provide the context for assessing and managing risk. An underlying principle in strategy-setting further illustrates this context: The greater the dispersion of possible future events or outcomes, the higher the organization's level of exposure to uncertain returns. An organization's sensitivity to risk is a function of (1) the significance of its exposures to change and future events, (2) the likelihood of those changes and future events occurring and (3) its ability to manage the business implications should any combination of those possible future changes and events occur. The organization's ERM infrastructure facilitates the advancement of risk management capabilities to provide better knowledge and information about the enterprise's key variables (or risks) and its capabilities around managing the effects of changes in those variables (or risks).

4. What is the value proposition for implementing ERM?

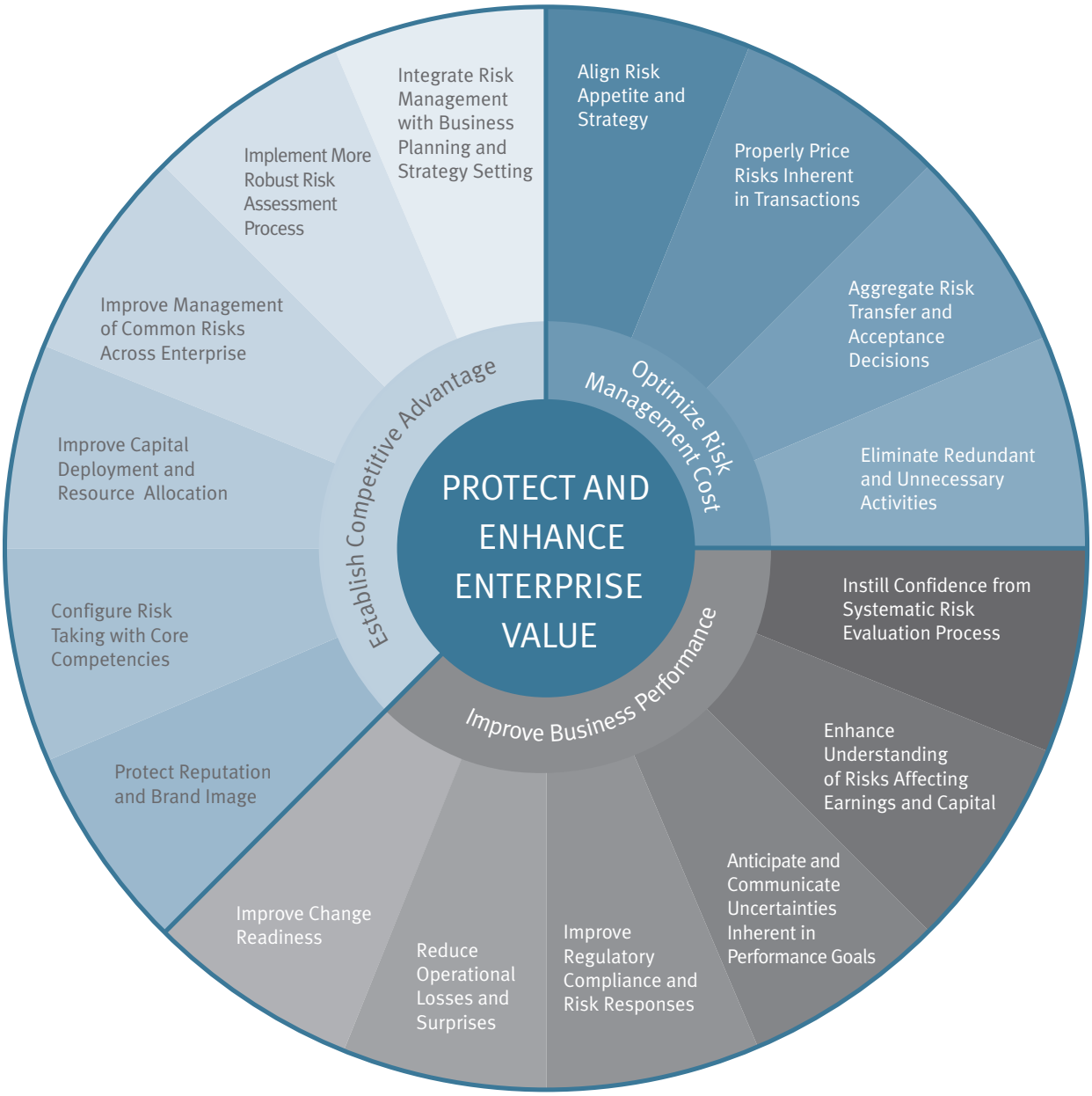
Directors and CEOs face many challenges. They must focus their organizations to capitalize on emerging opportunities. They must continually invest scarce resources in the pursuit of promising – though uncertain – business activities. They must manage the business in the face of constantly changing circumstances. And as they do all of these things, they must simultaneously be in a position to provide assurance to investors, directors and other stakeholders that their organizations know how to protect and enhance enterprise value. Amid constantly changing risk profiles, directors and CEOs need a higher level of performance from every discipline within the organization, including risk management.

ERM will help directors and CEOs meet these challenges by establishing the oversight, control and discipline to drive continuous improvement of an entity's risk management capabilities in a changing

operating environment. ERM redefines the value proposition of risk management by providing an organization with the processes and tools it needs to become more anticipatory and effective at evaluating, embracing and managing the uncertainties it faces as it creates sustainable value for stakeholders. By continuously improving the risk management capabilities that really matter to the successful execution of the business model, ERM elevates risk management to a strategic level.

As ERM is deployed to advance the maturity of the organization's capabilities for managing the priority risks, it helps management to successfully enhance as well as protect enterprise value in three ways. First, ERM focuses on establishing sustainable competitive advantage. Second, it optimizes the cost of managing risk. And third, it helps management improve business performance. These contributions redefine the value proposition of risk management to a business.

The following schematic illustrates the value proposition of ERM:



The above illustrative points are discussed throughout this book.

These valued-added contributions from ERM lead to possibly the greatest single benefit risk management provides for the success of a business: Instill greater confidence in the board, CEO and executive management. These stakeholders need to know that risks and opportunities are systematically identified, rigorously analyzed and cost-effectively managed on an enterprisewide basis, in a manner consistent with the enterprise's risk appetite and business model for creating value. Under ERM, executives are more knowledgeable of the risks inherent in their operations. They understand the process by which risks are identified, assign risk ownership in a timely fashion and ensure that risk responses are formulated timely and monitored effectively. They also bring to bear systematic risk assessment techniques to new risk-taking ventures. They insist that business plans incorporate a focus on risk, so that they will be more substantive and robust. In summary, in an ERM environment the assumptions underlying the business model are periodically challenged and, if necessary, refined in a dynamic cycle of continuous improvement and change.

It is vital to understand that the above articulation is generic. Because a generic value proposition is not sufficient to drive senior management decisions to invest in ERM infrastructure, it must be supplemented with a more granular articulation made possible by an enterprise risk assessment and a gap analysis around the entity's existing capabilities for managing its priority risks. As explained in our response to Question 85, the greater the gap between the current state and the desired future state of the organization's risk management capabilities, the greater the need for ERM infrastructure to facilitate the advancement of those capabilities over time. This understanding improves the specificity of the ERM value proposition, making it more compelling.

In summary, an effectively functioning ERM infrastructure can become one of the root differentiators between mere survivors and industry pacesetters. Beyond delivering the above benefits, redefining the value proposition of risk management will add to the CEO's storyline with stakeholders in today's demanding environment. An ERM infrastructure stimulates and reinforces desired behaviors within the organization consistent with its business objectives, strategies and performance goals. An ERM approach differentiates the firm's business model and helps to build its image and reputation with customers, suppliers, employees and the capital markets, all of which are keys to sustaining a successful business.

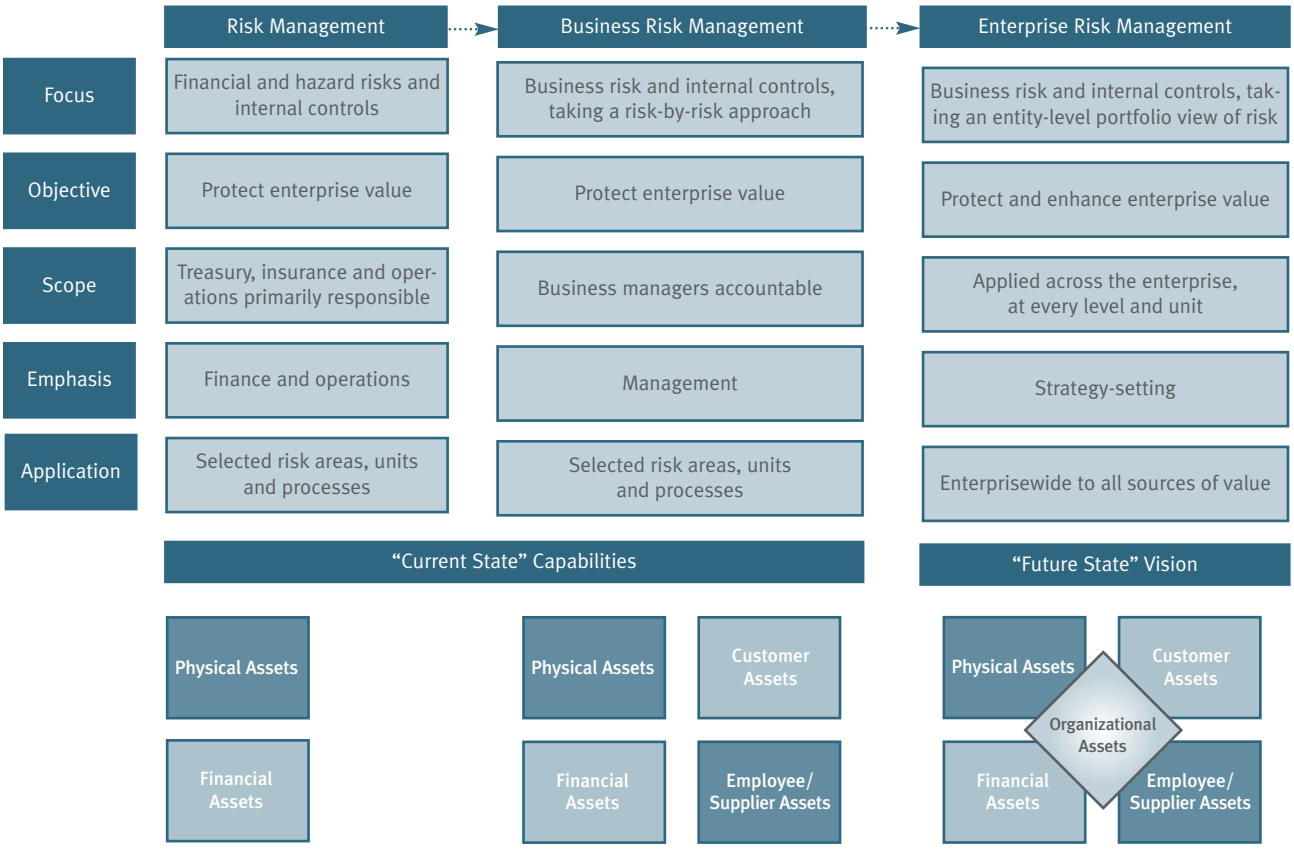
5. Which companies are implementing ERM?

Few, if any, companies can claim they have fully implemented ERM, as defined by COSO. For most companies, the chasm between the traditional risk management model and ERM, as discussed in Question 6, is simply too overwhelming to address. For example, the COSO definition (see Question 1) states that ERM is "applied … across the enterprise." A comprehensive, enterprisewide focus on managing risk is a high implementation standard for most companies because of the behavioral changes required to overcome the conventional management of risk in silos, which companies have had in place for a long time. For that reason, in recent years ERM has been pursued more by visionary organizations than by the mainstream of companies.

ERM is a "best-of-breed" approach consisting of different techniques that different companies have implemented in different ways. Institutions in financial services are probably furthest along based on the capabilities they have put in place to manage market and credit risks across the enterprise. However, even those institutions have a ways to go to address operational risk enterprisewide.

6. If companies are not implementing ERM, then what are they doing?

Most companies are applying the traditional risk management model in their business, which makes ERM a "future goal state," as the following schematic illustrates:



The evolution from the traditional risk management model to ERM noted above is not easy. Under traditional risk management approaches, the process is fragmented, risk is viewed as a negative (something to be avoided), reactive and ad hoc behavior is accepted, and the risk management activity is transaction-oriented (or cost based), narrowly focused and functionally-driven. Under ERM, as defined by COSO, the process is integrated, risk is also viewed as a positive (recognizing that successful companies must take on risks when seizing opportunities), proactive behavior is expected, and the risk management activity is strategic (or value-based), broadly focused and process-driven.

The traditional risk management model is focused on managing uncertainties around physical and financial assets. ERM is focused on the enterprise's entire asset portfolio, including its intangible assets such as its customer assets, its employee and supplier assets, and such organizational assets as its differentiating strategies, distinctive brands, innovative processes and proprietary systems. Very few companies have implemented a truly enterprisewide approach in all aspects of the business. Companies at the early stages of developing their ERM infrastructure often lay a foundation with a common language, a risk management oversight structure and an enterprisewide risk assessment process. A few companies have evolved toward more advanced stages, such as institutions in the financial services industry managing market and credit risks. Some companies apply ERM in specific units, such as in a trading unit's management of commodity price risk on an enterprisewide basis.

7. Who is responsible for ERM?

Because the emphasis is on strategy-setting, ownership begins at the top of the organization with executive management and cascades downward into the organization to unit and functional managers. Questions 39 through 45 discuss the role of executive management. The board of directors provides oversight (the role of directors is discussed in Questions 46 through 49). In addition, there is the chief risk officer (or equivalent executive), whose role is discussed in Questions 50 through 52. There may also be one or more risk management committees, depending on the nature and complexity of the risks and the need for cross-functional and cross-unit coordination. Questions 53 through 57 explain the respective roles of these executives in the context of the risk management oversight structure.

8. What are the steps companies can take immediately to implement ERM?

There are steps that any organization can take beginning tomorrow morning. We will illustrate them in this book. For example, organizations can:

- Adopt a common risk language. See Question 75.
- Conduct an enterprise risk assessment to identify and prioritize the organization's critical risks. Refer to Questions 69 through 84.
- Perform a gap analysis of the current and desired capabilities around managing the critical risks. Refer to Questions 110 and 111.
- Articulate the risk management vision, goals and objectives (see Questions 64 and 65), along with a compelling value proposition (refer to Questions 4 and 134 through 136) to provide the economic justification for going forward.
- Advance the risk management capability of the organization for one or two critical risks, i.e., start with a risk area where senior management knows improvements are needed to successfully execute the business strategy.

While there are other possible steps, the above are an excellent beginning and provide a simplified view for getting started with ERM implementation. It is also important to inventory what has already been done and to achieve visible early successes. The key is to keep the effort simple and focused by integrating the ERM-related activities into the business strategy and plan.

9. Is ERM applicable to smaller and less complex organizations?

All organizations face business risk, regardless of size. Organizations ignore risk at their own peril. No organization can afford to stand pat with its existing risk management capabilities; therefore, every organization should evaluate how it can improve its risk management. The COSO framework is useful for this purpose because its gives each organization a framework with criteria against which to compare its existing risk management capabilities. COSO points out on page 13 of its published framework:

> While some small and mid-size entities may implement component[s of ERM] differently than large ones, they still can have effective enterprise risk management. The methodology … is likely to be less formal and less structured in smaller entities than in larger ones, but the basic concepts should be present in every entity.

10. Why have companies that have tried to implement ERM failed in their efforts?

Few companies have implemented ERM, as defined by COSO. For example, the COSO definition makes clear that application of ERM must be "across the enterprise, at every level and unit, and includes taking an entity-level portfolio view of risk." Unless the ERM implementation is applied uniformly across the company

and is a holistic and comprehensive focus on all key business risks, it is not truly enterprisewide. Furthermore, unless the ERM implementation is tightly linked to the assessment and formulation of business strategy, it is not meeting the COSO requirements. While some companies have begun their journey to implement ERM, few of them have completed it.

11. Does implementation of ERM ensure the success of a business?

ERM does not guarantee the success of a business. It provides better information to managers and a more robust process for them to deploy, but does not necessarily transform a poor manager into a good manager. COSO points out that "limitations result from the realities that human judgment in decision-making can be faulty, decisions on responding to risk and establishing controls need to consider the relative costs and benefits, breakdowns can occur because of human failures such as simple errors or mistakes, controls can be circumvented because of human failures such as simple errors or mistakes, controls can be circumvented through collusion by two or more people, and management has the ability to override enterprise risk management decisions." The COSO definition also refers to "reasonable assurance." According to COSO, "reasonable assurance reflects the notion that uncertainty and risk relate to the future, which no one can predict with precision." In addition, COSO states on page 8 of the framework:

> Reasonable assurance does not imply that enterprise risk management frequently will fail. … The cumulative effect of risk responses that satisfy multiple objectives and the multipurpose nature of internal controls reduce the risk that an entity may not achieve its objectives. … However, an uncontrollable event, a mistake, or an improper reporting incident can occur. In other words, even effective enterprise risk management can experience a failure. Reasonable assurance is not absolute assurance.

12. What is the difference between ERM and management?

ERM is an integral part of managing an organization, but does not drive everything management does. COSO states that "[m]any judgments applied in management's decision-making and related management actions, while part of the management process, are not part of enterprise risk management." COSO provides several examples on page 14 of the framework. For example, management's choices as to the relevant business objectives, the specific risk responses and the allocation of entity resources are management decisions and are not part of ERM. That said, risk management is neither an afterthought nor an appendage to the existing management activities of the core business. In an ERM environment, risk management is effectively integrated with strategy-setting, business planning, performance measurement and other business disciplines.

13. What does it mean to "implement ERM"?

We believe the ERM implementation should emphasize strategy-setting. As explained in our response to Question 85, the application depends on each organization's priority risks (defined in the context of its business strategy) and the gaps around managing those risks. ERM is not a "one-size-fits-all" solution on a shelf. Management must decide the nature of the ERM solution based on the organization's size, objectives, strategy, structure, culture, management style, risk profile, industry, competitive environment and financial wherewithal. According to COSO, these and other factors affect how the ERM framework is applied.

Implementing ERM requires that management take the following steps:

(a) Identify and understand the organization's priority risks to provide a context.

(b) Use the COSO framework to define the current state of the organization's risk management capabilities.

(c) Use the COSO framework to define the desired future state of the organization's risk management capabilities.

(d) Analyze and articulate the size of the gap between (b) and (c) and the nature of the improvements needed to close the gap, which is a function of (i) the organization's existing capabilities and experience and (ii) management's desire to improve and outperform.

(e) Based on the analysis in (d), develop a business case for addressing the gap to provide the economic justification for the overall effort to implement the ERM infrastructure improvements.

(f) Organize a plan that advances the desired ERM infrastructure capabilities and address change issues associated with executing the plan.

(g) Provide the oversight and facilitation necessary to ensure effective integration and coordination of the overall effort.

See our response to Question 85 for further advice on getting started.

COSO states that ERM is "a means to an end, not an end in itself." The trend towards ERM recognizes that risks are complex and interrelated, and the business environment isn't getting any simpler. Therefore, there are significant benefits that can be achieved from evaluating and managing risk on a comprehensive enterprisewide basis. The process of implementing ERM is fundamentally a process of education, building awareness, developing buy-in and ultimately assigning accountability and accepting ownership. Because risks will continue to change and evolve as the global marketplace changes and evolves, implementing ERM should be viewed as a commitment to continuous improvement as opposed to an event.

14. Generally, how long does it take to implement ERM?

It is fashionable to view business initiatives as discrete activities with clear objectives and well-defined timetables. While ERM is certainly no exception from the standpoint of applying project management discipline, it is much more than a project. ERM is a journey, meaning it is a growth process in which the organization integrates risk management with strategy-setting to improve the effectiveness of its risk management capabilities over time.

The length of time required to implement ERM varies, depending on the current state of the organization's risk management, its desired future state and the extent to which it is willing to dedicate resources to improve risk management capabilities. In addition, because ERM requires an open environment conducive to effective communications about risks and risk management up, down and across the enterprise, cultural issues may exist for many organizations to overcome. For example, ERM requires an elimination of barriers – functional or departmental – so that a truly holistic, integrated, proactive, forward-looking and process-oriented approach is taken to manage all key business risks and opportunities – not just financial ones. If there are significant change management issues to address, the period of time to implement ERM will be extended. While there are concrete things any organization can do that will make an impact within 12 months, we estimate that most organizations will require from three to five years to accomplish their objectives in fully implementing their ERM solution.

15. Is there any way to benchmark the level of investment required to implement ERM?

As noted in the responses to Questions 13 and 14, it is difficult to generalize on the required investment. One reason for this is that the current and desired states vary for different companies. ERM is also the responsibility of every key individual within the organization. COSO states that ERM "is affected by an entity's board of directors, management and other personnel." It is integral to what they do. Managing an organization and managing risk should be inextricably linked. Therefore, management must decide the nature of the ERM solution based on the organization's facts and circumstances. With the point of origin and the point of destination varying by company, each organization's approach will have its own distinctive elements.

One effective way to determine the level of investment is to compare the organization's existing risk management to a framework (such as the COSO framework) and, using that comparison as a context, empower a group of senior executives to define the role of risk management in the organization. Based on this assessment, the level of investment can be priced based on the people, tools and other resources required to implement the desired ERM infrastructure. Our response to Question 85 provides additional context for gauging the level of investment by pointing to the need to begin with an enterprise risk assessment and a gap analysis around managing the organization's critical risks.

16. Don't successfully run companies already apply ERM?

We would expect that successfully run companies are applying many aspects of ERM infrastructure. It is indeed difficult to succeed without identifying, formally assessing, responding to, controlling and monitoring risk. However, we suggest that few companies on the planet can say with certainty that their risk management practices need no further improvement. The message is not about what companies are currently doing, but about what companies should do to enhance or improve their risk management capabilities as the operating environment changes. The COSO framework provides criteria by which companies can evaluate their risk management practices.

Businesses have always faced a variety of risks, but these are times when the pace of change and the resulting consequences to a business seem to be greater than ever. Some examples:

- Globalization has increased exposure to international events. Rarely do country borders insulate companies from such events. The price of energy is a case in point.
- The need for increased efficiency, innovation and differentiation, while always relevant, has escalated in importance as companies seek new ways to differentiate themselves.
- While competitor risk continues to be a priority, the cost of strategic error is rising in the global marketplace. Financial markets are more volatile than ever. Obsolete business models create a losing hand in the game. And, even if the business model is the right one to establish sustainable advantage, it is a winner only if the organization is able to execute it effectively.
- Understanding and responding to customer wants remains the key in this demanding era of increasingly focused niche markets. Failure to keep pace can result in rapid erosion of market share.
- Outsourcing has become so commonplace, questions arise about clarifying the retention and transfer of risk.
- Unfortunately, we now know the unthinkable can happen. The events of September 11, 2001 have changed how we think about business interruption risk.
- Due to the highly publicized public reporting fiascos and high demands on certifying officers, financial reporting is now a significant risk area as companies focus on the sustainability of their disclosure process and internal control structure.

Today, these and other risks are driving a continually changing risk profile that not only has financial implications, but also strategic and operational impacts. As executives examine the risks their companies face today, they will see a different profile than what they saw even a few years ago. And, more importantly, they can expect to see even different risks just a few years from now. That is why an enterprise risk assessment process is so critical.

It all comes down to this: It isn't the strongest or the smartest that will survive and prosper in the global economy – it's the organizations that can best adapt to change. As markets and customers change, business models change. As the competitive landscape changes, business strategies change. Furthermore, unless the ERM implementation is tightly linked to the assessment and formulation of business strategy, it is not realizing its full potential. That is why even companies that have achieved excellence in risk management should periodically evaluate the effectiveness of their risk management capabilities.

17. How long has ERM been around and why is there a renewed focus on it?

The concepts and theories underlying ERM, namely a portfolio view of risk, have been around a long time. The application of these concepts and theories has emerged in financial institutions and world-class corporate treasuries as they apply at-risk frameworks, capital attribution techniques and other measurement methodologies to the management of market risk and credit risk. However, market developments in recent years have made it clear that volatility isn't just a currency, interest rate or equity security risk anymore.

Customer preferences, competitor product offerings, labor markets and technology are all changing with increasing frequency, with their behavior resembling that of the financial markets. Even the life cycles of organizational business models are compressing. Change is no longer linear, but exponential. Successful companies must innovate and deliver total solutions that create new sources of value for their customers or markets or they will lose ground to nimbler, more creative rivals.

Never-ending innovation also gives rise to new risks that should be evaluated frequently. This way of thinking makes business strategy a fluent, dynamic process, with risk management augmenting that process. This increasing pace of change and recognition that change is a proactive way of life, coupled with increasingly effective risk identification, measurement, reporting and planning techniques, have caused companies to take a closer look at the state of their risk management.

In the past, the gap between the traditional risk management model and ERM, as explained in Question 6, was just too wide for most companies to address. However, compliance with Sarbanes-Oxley has laid a foundation for implementing ERM capabilities that did not previously exist. Companies that have implemented improved disclosure processes and internal control over financial reporting (ICFR) should take a closer look at how they can expand these capabilities to encompass other critical business activities, because the chasm is not as great as it once was due to the ongoing compliance effort required by Sarbanes-Oxley. The COSO Enterprise Risk Management – Integrated Framework provides the criteria to assist management in evaluating what needs to be done. That framework encompasses the COSO Internal Control – Integrated Framework used by many companies to assess the effectiveness of their ICFR.

18. What percentage of public companies currently have an ERM process or system?

The short answer is that the COSO framework provides the criteria needed to address this question. Until the framework gets more traction in the marketplace and companies can benchmark their risk management against the framework to assess where they stand, we won't know the complete answer to this question. However, there are some insights from which we can infer where companies currently stand:

- A Global CEO Survey published by PricewaterhouseCoopers (PwC) in 2004 indicated that 39 percent of 1,400 CEOs strongly agreed that ERM was a priority. While this group of CEOs (described by PwC as "strongly committed" CEOs) reported benefits from ERM, PwC's survey reports that 53 percent of them agree they have the enterprise information they need, 42 percent integrate ERM with strategic planning, 29 percent report the use of quantification to the greatest extent possible, 27 percent integrate ERM across all functions and units, and only 20 percent report that everyone understands his or her accountability relating to risk management. By contrast, the remaining CEOs (those not as strongly committed to ERM, according to the survey) report significantly lower percentages on these and other related questions.

- In our research over the last 10 years, we have deployed several surveys (with the latest study in the fall of 2005) to inquire about the level of confidence senior executives have in their organization's risk management. In every case, around 60 percent of the senior executives reporting indicated that they lacked high confidence that their organization's risk management capabilities were effective in identifying and managing all potentially significant business risks. Our experience indicates that this lack of confidence is caused by the absence of a systematic process for engaging appropriate executives in identifying and prioritizing risk enterprisewide. Deciding what to do and how to do it only comes after the vital risks are on management's screen through an effective enterprise risk assessment process.

- The lack of transparency also extends to the board of directors. In a McKinsey study involving 200 directors representing over 500 boards, released just before the Sarbanes-Oxley Act was enacted into law, 36 percent of the directors indicated that their boards did not understand the company's major risks. Approximately 40 percent of directors indicated that they lacked knowledge as to how to effectively identify, safeguard and plan for risk. The study also found that nonfinancial risk received only "anecdotal treatment" in the boardroom. No wonder management is getting more questions from directors about their company's risks and risk management.

19. Is there an example of effective ERM as it is applied in practice?

The COSO Application Techniques provide examples of the methods utilized by different companies at various levels of the organization in applying ERM principles. Readers familiar with the framework will find the material useful as examples.

20. How does the application of ERM vary by industry?

On page 3 of the Application Techniques, COSO states that "because of the array of available approaches and choices, even similar organizations implement enterprise risk management differently – whether applying the framework's concepts and principles for the first time or considering whether their existing enterprise risk management process, which may have been developed ad hoc over time, is truly effective." The industry within which a company operates is noted by COSO as one of the attributes that will "affect how the framework's concepts and principles are most effectively and efficiently applied." The nature of the industry will drive the nature of the risks and the risk management practices the organization adopts to manage those risks. For example, a bank will focus on managing market and credit risk to a greater extent than other institutions because the assumption of those risks is the essence of its business model. A pharmaceutical company will focus on managing its research and development pipeline because that is the lifeline to its future revenue streams. A utility will manage conformance risks in a nuclear power facility because that is the key to its reputation and future viability. Regardless of the industry, however, the components of the framework – as defined by COSO – still apply.

21. Are there any organizations that need not implement ERM?

Every successful organization faces risk. As articulated by COSO, ERM is a process for dealing with risks and opportunities. Executive management in most organizations, regardless of industry sector, is focused on investment and return, on opportunity and reward and on competitive advantage and growth. That's why ERM is vital to success – it assists managers in gaining confidence that they understand the organization's risks and have the capabilities in place to manage those risks.

Every successful organization takes risks. Every choice management makes to act or not to act affects the organization's risk profile. ERM can assist management in developing a differentiating skill in selecting the best bets for a company to make, given the competitive, regulatory and other forces in the external environment. This enhanced skill invigorates opportunity-seeking behavior.

Every successful organization responds to risk. Executive management must run the business amid changing market realities. They must carefully evaluate risk and reward as they channel resources to the best opportunities, consistent with the organization's risk appetite. They must confidently assure investors and other stakeholders that their organization is effectively managing risk while thriving in the global marketplace. As if that isn't enough, in the face of Sarbanes-Oxley, the CEO and CFO as certifying officers must be champions of transparent public reporting. Responding to these and other risks inherent in the business model is what successful organizations do.

An ERM infrastructure will help executives and directors meet these challenges. As discussed in Question 23, this assertion applies to both public and private companies.

22. What are the regulatory mandates for implementing ERM?

While there are no explicit regulatory requirements mandating use of the COSO Enterprise Risk Management – Integrated Framework at the present time, regulatory developments have created an environment in which companies would benefit from ERM. COSO pointed out that, like other factors defining the external environment, regulation itself creates uncertainty.

In the United States, Sarbanes-Oxley has commanded the headlines from its passage in July 2002 up to the time this publication was released to print. While the focus of Sarbanes-Oxley is limited to the reliability of

financial reporting, we believe that companies would benefit from an ERM process focused on identifying the enterprise's critical risks for timely action and disclosure. There are also other developments in the United States, such as the USA PATRIOT Act requiring "know your customer" anti-money laundering regulations and the Gramm-Leach-Bliley Act requiring financial institutions to safeguard and preserve privacy of "non-public" customer information. According to the New York Stock Exchange (NYSE) listing requirements, the audit committee charter must require the committee to discuss policies with respect to risk assessment and risk management. The NYSE also mandates an internal audit function with the purpose of providing management and the audit committee with ongoing assessments of the company's risk management processes and system of internal control. While not required, ERM would facilitate compliance with these requirements through an infrastructure and process which strengthens the enterprise's focus on simultaneously protecting and enhancing enterprise value.

Outside the United States, the KonTrag legislation in Germany requires large companies to establish risk management supervisory systems and report controls information to shareholders. Firms listed on the London Stock Exchange and incorporated in the United Kingdom are required to report to shareholders on a set of defined principles relating to corporate governance (known as the Combined Code, and supported with guidance provided by the Turnbull Report). The new Basel Capital Accord, issued by the Basel Committee on Banking Supervision, requires financial institutions to report on operational risk. Again, an ERM process would facilitate compliance with these requirements. In addition, Sarbanes-Oxley type legislation continues to arise in countries outside the United States.

23. Are standards for implementing ERM different for private and public companies?

The COSO framework applies to all organizations, large and small, public and private. The methods used to apply the components of the framework may vary depending on the organization's size, objectives, strategy, structure, culture, management style, risk profile, industry, competitive environment and financial wherewithal.

24. Must companies have sophisticated processes in all areas of risk management to realize the benefits of ERM?

The COSO framework does not require sophistication in risk management. It is unnecessary to deploy the most advanced techniques for all risks. Few organizations have the resources to do that, and there isn't a compelling business case for doing so. Sophistication is a function of (a) the nature of the risks faced by an organization, i.e., their complexity, volatility, pervasiveness and susceptibility to measurement, and (b) the availability of practical solutions that the entity can put into practice. When evaluating the desired risk management capabilities in a specific risk area or areas, the issue is not about deploying the most sophisticated processes, competencies, technology and knowledge – it is about selecting the most appropriate processes, competencies, technology and knowledge. This is a management decision. And that decision should be made in the context of the strategy-setting process.

For each individual risk or group of related risks, management must evaluate the current state of the organization's risk management capabilities. At that point, management must decide how much added capability is needed to achieve the entity's risk management objectives. Further, management must address the expected costs and benefits of improving the organization's capabilities. The goal is to identify the entity's most pressing exposures and uncertainties and to focus improvement activities on the elements of ERM infrastructure needed to manage those exposures and uncertainties more effectively.

THE COSO ENTERPRISE RISK MANAGEMENT— INTEGRATED FRAMEWORK

25. What is COSO?

COSO stands for "Committee of Sponsoring Organizations" and is a voluntary private-sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal controls and corporate governance. COSO was originally formed in 1985 to sponsor the National Commission on

Fraudulent Financial Reporting, an independent private sector initiative often referred to as the Treadway Commission. The Commission studied the causal factors that can lead to fraudulent financial reporting and developed recommendations for public companies and their independent auditors, for the Securities and Exchange Commission ("SEC" or "Commission") and other regulators, and for educational institutions.

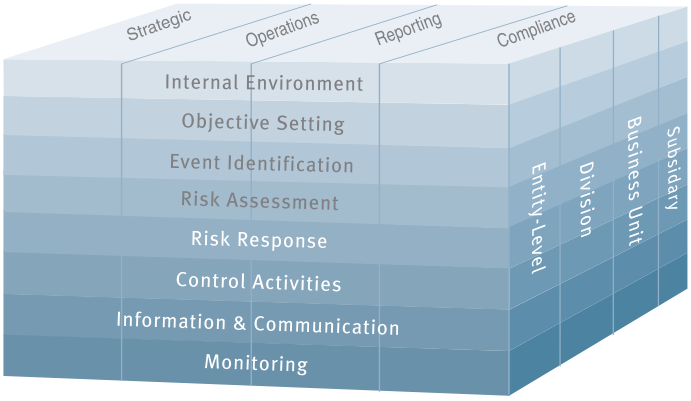
The sponsoring organizations are the American Institute of Certified Public Accountants (AICPA), The Institute of Internal Auditors (IIA), Financial Executives International (FEI), Institute of Management Accountants (IMA) and American Accounting Association (AAA). COSO so far has produced two documents, one in 1992 on the Internal Controls – Integrated Framework (which is the framework of choice in the United States for purposes of complying with Section 404 of Sarbanes-Oxley), and the other in the mid-1990s on derivatives.

26. Why was the COSO Enterprise Risk Management – Integrated Framework created?

The project to develop this framework began in 2001, before the scandals fueling the Sarbanes-Oxley legislation arose. In the foreword to the framework, COSO indicated that "recent years have seen heightened concern and focus on risk management, and it became increasingly clear that a need exists for a robust framework to effectively identify, assess, and manage risk." COSO's purpose was to develop a framework that "would be readily usable by managements to evaluate and improve their organizations' enterprise risk management." COSO goes on to point out that after the high-profile business failures occurred during the period of the framework's development, there were "calls for enhanced corporate governance and risk management, with new law, regulatory and listing standards." All these developments made more compelling the need for a framework to provide a common language and give clear direction and guidance.

27. What is the COSO Enterprise Risk Management – Integrated Framework?

COSO broadly defines ERM as "a process, effected by an 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 risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives." The framework encompasses, but does not replace, the Internal Control – Integrated Framework published by COSO in 1992.



Like its internal control counterpart, the ERM framework is presented in the form of a three-dimensional matrix. The matrix includes four categories of objectives across the top – strategic, operations, reporting and compliance. There are eight components of enterprise risk management, which are further explained below. Finally, the entity, its divisions and business units are depicted as the third dimension of the matrix for applying the framework.

As outlined by COSO, the framework provides eight components for use when evaluating ERM:

1. *Internal environment:* This component reflects an entity's enterprise risk management philosophy, risk appetite, board oversight, commitment to ethical values, competence and development of people, and assignment of authority and responsibility. It encompasses the "tone at the top" of the enterprise and influences the organization's governance process and the risk and control consciousness of its people.

2. *Objective-setting:* Management sets strategic objectives, which provide a context for operational, reporting and compliance objectives. Objectives are aligned with the entity's risk appetite, which drives risk tolerance levels for the entity, and are a precondition to event identification, risk assessment and risk response.

3. *Event identification:* Management identifies potential events that may positively or negatively affect an entity's ability to implement its strategy and achieve its objectives and performance goals. Potentially negative events represent risks that provide a context for assessing risk and alternative risk responses. Potentially positive events represent opportunities, which management channels back into the strategy and objective-setting processes.

4. *Risk assessment:* Management considers qualitative and quantitative methods to evaluate the likelihood and impact of potential events, individually or by category, which might affect the achievement of objectives over a given time horizon.

5. *Risk response:* Management considers alternative risk response options and their effect on risk likelihood and impact as well as the resulting costs versus benefits, with the goal of reducing residual risk to desired risk tolerances. Risk response planning drives policy development.

6. *Control activities:* Management implements policies and procedures throughout the organization, at all levels and in all functions, to help ensure that risk responses are properly executed.

7. *Information and communication:* The organization identifies, captures and communicates pertinent information from internal and external sources in a form and timeframe that enables personnel to carry out their responsibilities. Effective communication also flows down, across and up the organization. Reporting is vital to risk management and this component delivers it.

8. *Monitoring:* Ongoing activities and/or separate evaluations assess both the presence and functioning of enterprise risk management components and the quality of their performance over time.

The thought process underlying the above framework works in the following manner: For any given objective, such as operations, management must evaluate the eight components of ERM at the appropriate level, such as the entity or business unit level.

28. How can we obtain the COSO ERM framework?

Interested parties can obtain the executive summary of the framework at **www.coso.org**. At this site, they can also place an order for either a hard copy or electronic copy of the integrated framework, which includes three segments – the Executive Summary, the Framework and the accompanying Application Techniques.

29. How was the COSO ERM framework developed?

Appendix A to the COSO ERM framework describes the process. COSO engaged PricewaterhouseCoopers (PwC) to conduct the project. PwC obtained input from a broad range of executives – chief executive officers, chief financial officers, chief risk officers, controllers and internal auditors representing public and private companies of varying sizes and from different industries and government agencies. Input was also obtained from legislators, regulators, external auditors, lawyers and academics. PwC received advice and counsel from an advisory board to the COSO board. Periodically, PwC, the advisory board and the COSO board would meet to discuss the project plan, progress, framework drafts and specific topics and issues germane to completing the framework.

As discussed in Appendix A of the framework, the project consisted of five phases – Assessment, Envisioning, Assessing and Designing, Preparation for Public Exposure and Finalization. The document was exposed for a 90-day period and the framework was field tested with selected companies. Input was considered from both the comment period and the field tests. Published sources considered by the project team were listed in Appendix D to the framework, including two books authored by a Protiviti managing director. Appendix E includes a summary of the project team's consideration of specific issues arising during the comment period.

30. How do we use the COSO ERM framework?

On pages 6 and 7, COSO suggests alternative uses of the framework according to the user. For example:

USER	POSSIBLE USES
Directors	• Discuss with management the state of ERM • Provide oversight to risk management activities • Ensure they are apprised of risks and management's actions to address them • Consider input from internal auditors, external auditors and others
Senior management	• Assess the organization's ERM capabilities
Managers and other entity personnel	• Consider how they are conducting their responsibilities in light of the framework components • Discuss with superiors ideas for improving ERM
Internal auditors	• Consider the breadth of their focus on ERM in the audit plan

COSO also provided suggestions for regulators, professional organizations and educators.

In summary, the COSO framework should be used as a benchmarking tool to evaluate the effectiveness of the ERM process in place as well as specific risk management activities at all levels of the organization. The framework can provide the context for defining improvements in risk management capabilities.

31. Are companies required to use the COSO ERM framework?

No. Use of this framework is optional. To put this statement in perspective, however, readers should understand that when it was issued in 1992, the Internal Control – Integrated Framework was also optional. Now almost every public company in the United States is using it.

32. Does the COSO Enterprise Risk Management – Integrated Framework replace or supersede the COSO Internal Control – Integrated Framework?

No. Both frameworks stand alone. Appendix C to the ERM framework addresses this question. COSO states that internal control is encompassed within and is an integral part of ERM. Therefore, the new ERM framework does not replace or supersede the internal control framework. This point is important because many U.S. companies are using the COSO Internal Control – Integrated Framework for purposes of complying with Section 404 of Sarbanes-Oxley.

33. How does the COSO Enterprise Risk Management – Integrated Framework compare to the COSO Internal Control – Integrated Framework?

Appendix C to the ERM framework addresses this question, laying out the differences between the two frameworks. For example, in comparison to the internal control framework:

- The ERM framework is a broader focus on risk management and encompasses the internal control framework.
- The ERM framework added a new category, strategic objectives, and expanded the reporting objective to include internal reporting.

- The ERM framework introduced the concepts of risk appetite and risk tolerance.
- The ERM framework expands the risk assessment component into four components – objective-setting, event identification, risk assessment and risk response.

There are also specific differences in the components themselves, which are discussed in Appendix C to the framework. For example, roles and responsibilities are expanded to focus on risk management versus internal control. The internal environment component of the ERM framework encompasses the seven attributes of the control environment component of the internal control framework, with the emphasis on risk management, and adds three additional attributes – risk management philosophy, risk culture and risk appetite.

34. Does the new COSO framework broaden the focus of ERM beyond the traditional risk management model's focus on insurable risk? If so, how?

Yes. The COSO ERM framework focuses comprehensively on all risks, not just financial or insurable ones. The framework achieves this broader focus in at least two ways:

- It emphasizes strategic, operational, reporting and compliance objectives and, therefore, addresses risks to the achievement of those objectives.
- The eight components of ERM, as outlined by COSO, are sufficiently comprehensive and extend beyond the procurement of insurance.

Thus when COSO uses the term "Enterprise Risk Management," it is referring to a broader risk management concept than the insurable risk management model.

35. Are there other standards and frameworks in existence and, if so, what do they promulgate and how does the COSO Enterprise Risk Management – Integrated Framework relate to them?

There are indeed other standards, which COSO lists in Appendix D. These standards include:

- Internal Control Guidance for Directors on the Combined Code (United Kingdom)
- King Report on Corporate Governance for South Africa
- International Organization for Standardization – ISO/IEC Guide
- Australian/New Zealand Standard 4360: Risk Management
- A Risk Management Standard (Institute of Risk Management, Association of Insurance and Risk Management)

COSO did not publish a reconciliation of these various standards to its ERM framework. However, the project team considered these frameworks in the Assessment phase of the project. In addition, Question 164 relates ERM to the Basel Capital Accord requiring financial institutions to report on operational risk. Questions 165 and 166 briefly comment on the relationship between the COSO ERM framework and other frameworks, such as CobiT, ISO 17799, BITS, NIST Special Publication 800-53 and ITIL.

36. What is the point of view of the Securities and Exchange Commission (SEC) with respect to ERM?

The Commission had not issued an official statement as of the date this publication went to print. However, an SEC Commissioner periodically has addressed the importance of ERM in a number of speeches.

37. What are the deliverables when the COSO ERM framework is implemented?

The "deliverables" vary according to the techniques and tools deployed to implement the eight ERM components, the breadth of the objectives addressed, the nature of the industry, the nature of the risks and the extent of coverage of the organization's units. The ERM infrastructure, which is intended to provide the

discipline, focus and control to advance the enterprise's capabilities around managing its priority risks, may include such elements as the following:

POSSIBLE ERM INFRASTRUCTURE ELEMENT	DISCUSSED IN QUESTIONS
Presence on CEO agenda	3, 4, 21, 30, 40, 41, 56, 88-90, 129, 136, 141, 142, 144
Overall risk management policy	65, 110
Common risk language	74-76, 98
Enterprisewide risk assessment process	65, 69-85, 103, 106, 129, 131
Common process view	99, 103, 104
Clarity of roles and responsibilities related to risk management	30, 56, 57, 90, 91, 110, 144
Focused risk committee(s)	48, 49, 56, 85
CRO (or equivalent executive)	50-52, 56
Integration of risk responses within business plans	50, 54, 108, 109, 127, 129, 133
Integration of risk management with strategy-setting	3, 4, 41, 49, 56, 66, 67, 85, 108, 109, 111, 129, 131, 133, 135
Alignment of organizational behavior with risk appetite	45, 49, 53, 54, 56, 65-67, 95, 102, 106, 127, 129, 131, 133
Risk reporting	45, 50, 109, 111-113, 121
Knowledge sharing process for identifying best practices	51, 91, 101, 103, 111, 121, 123
Common training	111, 123
Proprietary tools to portray a portfolio view of risk	3, 56, 108, 109, 111, 112, 127, 129
Supporting technology	110, 111, 113-121

Additional "deliverables" include the improved capabilities around managing the enterprise's priority risks. The value proposition, as summarized in Question 4, illustrates the benefits achievable through an effective ERM infrastructure.

Note that a relationship exists between (a) the need for ERM infrastructure on the one hand and (b) the nature and extent of gaps in risk management capabilities on the other. The greater the gaps in the current state and the desired future state of the organization's risk management capabilities, the greater the need for ERM infrastructure to drive the advancement of capabilities over time to close these gaps. The good news is that the existing management infrastructure of most companies already includes elements of ERM infrastructure.

38. Can a company "partially" adopt the COSO Enterprise Risk Management – Integrated Framework with success?

In defining ERM, COSO has indicated that the framework is applied across the enterprise. This can be accomplished, however, within a specific unit, subsidiary or division, representing a form of "partial adoption" while still retaining an enterprisewide focus. The application of ERM to strategic operating units works because such units often have distinctively different objectives and strategies, manage distinctive product groups, serve heterogeneous markets and act as standalone profit centers. Therefore, they have distinctly different risk profiles. Executive management at the parent level may even foster, explicitly or

implicitly, a competitive environment among different strategic units. If so, the risk profiles for separate business units may differ to such an extent that it may be appropriate to evaluate and manage them separately. In such circumstances, a decentralized approach may make more sense with ERM applied at one or more selected operating units.

Ultimately, taking an enterprisewide view means achieving the highest level of risk-adjusted return possible from the resources available to managers within the defined enterprise boundaries, whether for a specific operating unit or for the enterprise as a whole. From a risk management standpoint, this view has to be consistent with executive management's view of the organization. If management takes a centralized view of the business, an enterprise view must of necessity extend to the entire organization. On the other hand, if management has a decentralized view of the organization with different units operating autonomously, an enterprise view would apply at the unit level.

THE ROLE OF EXECUTIVE MANAGEMENT

39. Who should participate in the ERM process, and how?

While ultimate responsibility for ERM starts at the top, everyone who matters within an organization should participate to some extent in the ERM process. While several executives have significant responsibilities for ERM, including the chief risk officer, chief financial officer, chief legal officer and chief audit executive, the ERM process works best when all key managers of the organization contribute. The COSO framework states that managers of the organization "support the entity's risk management philosophy, promote compliance with its risk appetite and manage risks within their spheres of responsibility consistent with risk tolerances." Therefore, identifying leaders throughout the organization and gaining their support is critical to successful implementation. A goal of ERM is to incorporate risk management into the organization's agenda and decision-making processes. This means that ultimately, every manager is responsible, which can only happen when performance goals are clearly articulated, and the appropriate individuals are held accountable for results.

40. Must the CEO be fully engaged in the ERM process or system for it to be successful, or can he or she delegate it to someone else?

The COSO framework states that the CEO "is ultimately responsible and should assume ownership" over the implementation of ERM. Because ERM, as COSO defined it, is integral to running and managing a business, the CEO's involvement is vital to the success of ERM. For example, an effective ERM solution affects the organization's culture, because it establishes an environment where people can raise their hands and express issues without fear of retribution. This kind of open and positive environment is not possible without the CEO's active and visible support. The CEO sets the tone by asking the tough questions about risk and risk management and by demonstrating a commitment to raising the focus of risk management to a strategic level.

A point that is often omitted in this discussion is that it is important to the CEO that he or she be involved in the process. The CEO's participation keeps the focus at a strategic level. The CEO wants to know the answers to at least two questions about risk. First, are there any unknown exposures to events that can abruptly shift the organization's agenda to "damage control" in a heartbeat should they occur? Second, if such exposures exist, what can be done cost-effectively to prevent the potential future events from happening and how will the organization respond should the events occur? ERM can help supply CEOs with answers to these two questions, but only if the CEO is sufficiently involved to ensure the process is appropriately focused on strategic and reputation risks.

Support from the top is vital to an effectively functioning ERM infrastructure. To create and sustain momentum, senior management must demonstrate a strong commitment to ERM through consistent communications and actions. This level of commitment arises from a compelling business case. The business case articulates the organization's priority risks, the gaps around managing those risks, the ERM infrastructure needed to close significant gaps and the resulting costs and benefits. The business case clarifies

why ERM infrastructure is needed, focuses on the big picture with a shared vision of the future state of risk management within the organization, sets realistic goals and develops a clear plan of action. A well articulated business case helps get the CEO engaged.

41. How will senior management benefit from supporting ERM implementation?

As they focus on investment and return, on opportunity and reward and on competitive advantage and growth, CEOs and their management teams must pursue promising – though uncertain – opportunities in the face of changing market conditions. They must be in a position to confidently assure investors and other stakeholders that the organization is managing risk effectively. They must also comply with Sarbanes-Oxley and other applicable laws and regulations.

Research we have conducted several times since 1995 (with the most recent study completed during fall of 2005) almost consistently indicates that approximately 6 in 10 senior executives lack high confidence that their organization's capabilities are identifying and managing all potentially significant business risks. Senior executives can gain increased confidence from an effective process that engages everyone who has key responsibilities within the organization for assessing and managing risk. Our research has also indicated that roughly 50 percent of senior executives have made significant changes within the previous two years and that about 50 percent report they plan to make significant changes during the next three years.

These results are not surprising. Opportunity-seeking behavior is invigorated if managers possess the confidence that they understand the related risks and have the capabilities to manage those risks. In a rapidly changing world, traditional risk management approaches will not be effective because they are fragmented, treating risks as disparate events and easily compartmentalized in silos. While the tight focus of traditional risk management activities on loss prevention is not a bad thing, neither is it a good enough thing *because* the activities are not adequately integrated with the identification, evaluation and pursuit of growth opportunities. Moreover, current risk management approaches are too firmly rooted in the command and control era, which means they may not effectively balance the desire for control with the need for agility, responsiveness and cross-functional cooperation.

The inevitable conclusion is that the current state of risk management is not conducive to instilling the necessary confidence in senior management that all potentially significant business risks are identified and managed. An enterprisewide approach to business risk management will help executives meet the challenges they face by improving the linkage of risk and opportunity during the strategy-setting process and positioning risk management as a differentiating skill in managing the business.

42. How should executive management evaluate ERM?

The COSO framework provides insights into the question of how executive management evaluates the application of ERM within the organization. The four categories of objectives, the extent of application (across the entity and its divisions and business units) and the eight components of ERM, as defined by the COSO framework, provide the basis for that evaluation. Management must evaluate the appropriate ERM infrastructure the organization needs in place to realize its chosen risk management vision, goals and objectives. The business case provides the economic justification to proceed with an ERM solution. Once the business case is approved, the design and implementation of the capabilities that deliver management's desired solution are boiled down to a project plan that will make the ERM solution happen over management's selected time frame. The key success factors articulated in the business case are used to evaluate the ERM solution over time. Examples of measures of success are provided in our response to Question 136.

43. What is the role of the CIO in an ERM environment?

Every ERM solution is impacted by technology in various ways. Enterprise software solutions are informational tools that act as an enabler for ERM, particularly for purposes of managing nonfinancial risks. As companies configure enterprisewide systems to work seamlessly with risk measurement systems, they will consolidate much more information. Depending on the complexity and strategic importance of these systems

and the number of internal stakeholders involved, the CIO may play a key role in this transition.

In addition, an ERM solution may provide the means for the CIO to assert considerable influence over the management of critical IT risks on an enterprisewide basis. The CIO's interest in ERM stems from the overall governance issues relating to the IT operations, the processes impacting IT, the various application and data owners throughout the organization and the need to eliminate gaps and overlaps in the ownership of IT-related risks. The CIO is in the position of setting the tone for managing IT risks across the enterprise by instructing business unit managers and process owners on how to understand, evaluate and manage IT risks and controls, and to address in a timely way any unresolved IT control issues.

44. What is the role of the treasury and insurance in an ERM environment?

Treasurers and insurable risk managers are vital stakeholders from a risk management standpoint. They manage exposures and uncertainties related to (a) physical and financial assets on the balance sheet, (b) the prospects for expected future cash flows from core business activities, and (c) various contractual obligations of the enterprise, among other things. Their activities have been integral to the traditional risk management model, as discussed in Question 6, for decades.

ERM does not replace the traditional risk management model, but is rooted in and improves upon that model. From a treasury perspective, the risk management process has often been applied to financial and hazard risks in isolation, either by risk type or by the unit or activity potentially exposed to the risks. A competent and effectively executed hedging program has been an important aspect of competent regional and global treasuries for a long time, as the classic risk management focus on products and transactions has delivered value in many industries and companies. That is why the traditional risk management model will have a lasting legacy.

That said, an enterprisewide view suggests that those closest to the risks must be directly engaged in the management of the risks. Whether that means they assume primary responsibility to decide, design and monitor or secondary responsibility to build and execute (according to the design) depends on the circumstances. That is why cutting-edge treasuries and insurable risk management functions are taking a broader, more strategic view of the business, leading their organizations to a more formal and systematic approach to managing operational and other business risks. Visionary and progressive leaders from treasury, insurance, internal audit and other corporate-level functions – most often with support from top management – have helped their organizations to understand risk more clearly and improve risk management capabilities.

45. Does ERM require reporting to executive management? If so, what types of reports are most suitable for executive management?

The effectiveness of ERM is highly dependent on the effectiveness of the organization's information and communication, which is one of the eight components of the COSO framework. Reporting is integral to this component because it drives transparency about risk and risk management throughout the organization to enable risk assessment, execution of risk responses and control activities as well as monitoring of performance. There are many questions regarding reporting, however. For example, what specifically should be reported, to whom should reports be issued, how often should reports be available, how are reports used and how granular should they be?

Risk management information may be summarized in many ways – for the enterprise as a whole, by business unit, by risk unit, by geography and by product group, for example. The objective is to enable decision-makers to evaluate risk management performance monthly, weekly, daily or even in real-time (which is difficult to achieve and rarely required for executive management), as the nature of the risks and circumstances dictate. Following are a few examples of risk management reports that serve the purpose of providing information for decision-making to executive management:

- A summary of the enterprise's risks, broken down by operating unit, geographic location, product group, etc.
- A summary of the existing gaps in the capabilities for managing the priority risks.

- A summary of the top and worst performing investments and reasons why.
- From an "environment scan" process or early warning system, a report of emerging issues or risks that warrant immediate attention.
- Value-at-risk reports to assess the sensitivity of existing portfolio positions to market rate changes beyond specified limits, and consider the exposure of earnings or cash flow to severe losses.
- Summary of scenario analyses evaluating the impact of changes in other key variables beyond management's control (e.g., inflation, weather, competitor acts and supplier performance levels) on earnings, cash flow, capital and the business plan.
- Operational risk reports summarizing exceptions that have occurred versus policies or established limits (i.e., limit breaches), including any significant breakdowns, errors, accidents, incidents, losses (as well as lost opportunities) or "close calls" and "near misses."
- Special studies or targeted analyses to evaluate questions about specific events or anticipated concerns that could "stop the show." For example, what is our Latin American or Asian exposure?
- Summary of significant findings of business process audits performed by internal audit or reviews conducted by other independent parties such as the organization's regulators.
- Summary of the status of improvement initiatives. Are planned improvement initiatives on track? If not, why?

In addition to the above reports, there is dashboard or scorecard reporting. Models, risk analytics and web-enabled networks make it possible to aggregate information about risks using common data elements to support the creation of a risk management dashboard or scorecard for use by risk owners, unit managers and executive management. Dashboard and scorecard reporting are flexible enough to enable the design of reports to address specific needs. Examples of dashboard reporting, which often features "traffic light" indicators, are provided in the Application Techniques of the COSO ERM framework. It is discussed further in Question 121.

THE ROLE OF THE DIRECTOR

46. How are ERM and governance related?

To answer this question, we need to establish a context. We suggest the following point of view:

> The top performers in the rapidly changing global marketplace will be those that best understand their risks and align their risk taking with what they do best. Management can use guidance and input from savvy, experienced directors as they work to achieve this objective. Governance is the process by which directors oversee the decisions and actions of executive management in a constructive manner, consistent with applicable laws and regulations, as management formulates and executes strategies to accomplish enterprise objectives. Effective governance provides assurance to investors and other key stakeholders that the enterprise conducts its affairs with integrity and reports its performance in a fair and transparent manner.

If we accept the above point of view with respect to governance, then ERM and the governance process are inextricably linked. Good governance facilitates implementation of ERM because ERM is built on transparency. Conversely, an effectively functioning ERM infrastructure would provide greater confidence to the board and to executive management that risks and opportunities are being systematically identified, rigorously analyzed and effectively managed on an enterprisewide basis. Thus the two go hand-in-hand.

47. Why should directors be concerned about whether their companies implement ERM?

A McKinsey quarterly survey of 1,000 directors conducted in March 2005 reported that directors want to spend more time on risk and strategy. According to McKinsey, "this refocusing seems to reflect three forces at work among boards: a shortfall of knowledge about the current and future strategy of their companies, a

certain lack of confidence in management and a desire to assume a more active overall role." Thus directors want answers from management to the following questions:

- What are your critical risks to the execution of the business model and strategy? How do you know?
- How are you managing the critical risks? Are the risks undertaken consistent with the organization's risk appetite? How do you know?
- When there are significant changes in the underlying risks the organization faces, are you informing the board in a timely manner?

If directors desire greater involvement in formulating strategy and assessing risk, they are likely to start by working with executive management to understand the enterprise's current strategic position as clearly as possible. In turn, executive management should accommodate the board by developing and proposing a number of alternative long-term strategic options for the board's review. Working together, management and the board test and challenge these optional strategies before choosing the most appropriate one, taking into account the relative risk and reward. ERM augments this process by ensuring appropriate integration of risk.

48. How should the audit committee view ERM?

ERM is broadly focused on business risks, whereas the audit committee has historically limited its focus to public and financial reporting risks. However, this limited focus could expand somewhat over time. The NYSE listing requirements specify that, when addressing the audit committee's duties and responsibilities, the committee charter should state that the committee must discuss management's policies with respect to risk assessment and risk management. The ERM framework provides a context for this discussion. For example, an enterprisewide risk assessment process provides fresh insight as to new and emerging risks for timely action and possible disclosure. Because risk assessment is a component of internal control and the evaluation of internal control must be risk-based, the audit committee may want to inquire as to the effectiveness of this process. An enterprisewide risk assessment process is also an effective first step to implementing ERM.

When discussing risk assessment and risk management with senior management, the audit committee should:

- Discuss the organization's exposure to potential future events (e.g., catastrophic losses, fraud, illegal acts, litigation, etc.) which could impact its brand image and reputation.
- Understand management's assessment of financial reporting risks and ask the external auditors if they concur with that assessment.
- Understand the soft spots relating to financial reporting that give rise to significant risks, e.g., the reserves, contingencies, valuations, computations and disclosure areas requiring significant judgment.
- Understand the extent of self-assessment and entity-level and process-level monitoring in place to manage financial reporting risk.
- Understand the internal auditor's assessment of risk and the audit plan based on that assessment.
- Inquire as to whether there are managers responsible for identifying, assessing, managing and monitoring critical risks, and whether the committee should meet from time to time with those managers to discuss the implications of their activities for public and financial reporting.
- Understand the results of management's enterprise risk assessments and the implications to public and financial reporting.

Of course, the audit committee can expand the above activities to address other aspects of risk assessment and risk management; however, most committees are focused on and have their hands full with public and financial reporting issues. Therefore, that focus is emphasized in the points above. Other board committees, such as the finance committee or a designated risk committee, may emphasize other business risks through their respective activities.

49. How should the board exercise oversight of ERM implementation?

In the Executive Summary of the ERM framework, COSO states the following:

> The board should discuss with senior management the state of the entity's enterprise risk management and provide oversight as needed. The board should ensure it is apprised of the most significant risks, along with actions management is taking and how it is ensuring effective enterprise risk management.

Just as a company needs a process to procure quality materials at a competitive cost from its suppliers, it needs a process to manage and reduce its risks to an acceptable level. Without a process, risk management is an ad hoc, reactive activity that is fragmented across the enterprise. With the purpose of instilling the discipline to improve continuously the organization's capabilities around managing its priority risks, ERM infrastructure provides an alternative. Because it leads to risk management capabilities that are repetitive, defined and managed, ERM can assist the board in better understanding management's risk appetite and in gaining confidence in management's reporting on risk and risk management performance.

Anticipatory and proactive oversight requires a strong emphasis on up-front board involvement in policy setting, risk assessment and strategy formulation. Through the activities of their various committees, boards enhance the quality of the oversight process by adding value to management's assessment of the organization's risks. Once risks are identified and sourced, boards should ensure that management evaluates the company's options for managing the critical risks, leading to policies clarifying responsibilities, authorities and accountabilities. For example, among other things, the board should satisfy itself that:

- Growth and innovation are encouraged and rewarded without creating unacceptable exposure to risk.
- The risk appetite inherent in the organization's opportunity-seeking behavior in developing new products and new markets is clarified, understood and managed.
- Defined boundaries and limits clearly exclude behaviors and actions that are off-strategy and unacceptable.
- Performance measures and targets do not encourage excessively risky behavior.
- An enterprisewide view, rather than a narrower unit or functional view, is taken when selecting strategies to optimize risk and reward for the enterprise as a whole.
- Effective internal controls and checks and balances are in place in high-risk areas.

Effective oversight is also reactive and interactive. The board should determine that management has in place the appropriate capabilities to execute approved risk responses. Risk ownership and personal accountability must be sufficiently focused so that the appropriate risk management and control processes are designed and implemented by competent personnel. Risk owners – the individual, the group, the function or the unit authorized to make choices and take action within established bounds to manage one or more priority risks – must be designated in a timely manner so that each key risk has a name by it. For critical risks, the capabilities in place must often be at a higher state of maturity than the capabilities for less significant risks. Therefore, the board should ensure that management determines that sufficient resources are allocated to the management of these risks.

Examples of the questions directors might ask management about ERM are provided below.

With respect to strategy:

- Does management involve the board in a timely fashion during the strategy formulation process and discuss management's risk appetite?
- Does management involve the board when making decisions to accept or reject significant risks?

- Is the company taking significant risks that the board does not understand (e.g., if an operating unit or product group is earning superior returns relative to competitors, is it due to taking significantly greater risks than competitors)?
- Are the critical risks inherent in the organization's business model fully understood and managed by personnel with the requisite knowledge, skills, tools and information? How do you know?
- Does the board understand the priority business risks and how those risks are addressed?
- Are the company's key risks on a list? Is the list current?
- Is there sufficient time during board meetings to discuss the key risks and whether there are significant gaps in the capabilities for managing those risks?

With respect to policy:

- How does management encourage and reward growth and innovation without creating unacceptable exposure to risk? For example, are there defined boundaries and limits that clearly specify behaviors that are off-strategy and off-limits?
- Are the entrepreneurial activities and the control activities of the business in balance so that neither is too disproportionately strong relative to the other? Are the risks inherent in opportunity-seeking behavior understood and managed? How do you know?

With respect to execution:

- Does management understand the uncertainties inherent in its strategies for achieving business objectives and performance goals? How do you know?
- Are there adequate assurances that risk responses and the related control activities and information and communication processes are operating effectively? How do you know?
- Are effective contingency plans in place to respond in the event of a crisis? How do you know?
- Is there an early warning system or executive team dashboard for "mission-critical" risks?
- Are there effective processes in place to continuously identify risk, measure its impact and evaluate risk management capabilities (e.g., the related control activities, information and communication processes, and monitoring activities)? How do you know?
- Are there managers responsible for identifying, assessing and managing critical risks whom directors should meet with from time to time?

With respect to transparency:

- Is there an effective process for reliable reporting on risks and risk management performance? How do you know?
- Is there an organizational structure in place that supports the risk management reporting process? How do you know?

The board's purpose when directing questions to management regarding risk management is to understand the risks that the organization faces in the context of established business objectives and determine whether the entity has the appropriate strategies and capabilities in place to manage its key risks. The COSO ERM framework provides an excellent benchmarking tool for directors to use to direct and focus their oversight activities with respect to risk management. This evaluation should take place at least annually.

Over time, the best way to engage the board is through information. This does not necessarily mean providing the board the same reports prepared for executive management. While as a general rule risk

management information given to the board should not be too detailed, the level of granularity will oftentimes be a matter of personal preference. The objective of risk management reports to the board is to position directors to execute their oversight role. Following are a few examples of risk management reports that will help lengthen the board's memory:

- A high-level summary of the top risks for the enterprise as a whole, broken down by operating unit, geographic location, product group, etc., along with significant gaps in risk management capabilities
- A summary of the top and worst performing investments and reasons why
- Report of emerging issues or risks that warrant immediate attention
- Summary of significant risk events, e.g., significant exceptions versus policies or established limits
- Summary of significant changes in key variables beyond management's control (e.g., interest rates, exchange rates, etc.) and the effect on earnings, cash flow, capital and the business plan
- Summary of the status of improvement initiatives

Some of these reports may be similar to reports received by executive management, as outlined in our response to Question 45.

THE ROLE OF THE CHIEF RISK OFFICER

50. Should our organization have a chief risk officer (CRO) and, if so, what is his or her role?

As a champion of ERM, the CRO facilitates the execution of ERM process and infrastructure. His or her role may be either consultative (assess and recommend) or authoritarian (approve) or both, depending on the risk area. With the assistance of a staff function (the business risk management function (BRMF) described in Question 56), the CRO supports the board (or a designated board committee), the CEO, the executive committee (or a designated risk management committee) and business unit and support unit managers. The CRO:

- Establishes and communicates the organization's ERM vision.
  - Works with an empowered group of senior executives to define the appropriate role of risk management in the organization.
  - Assists senior management in communicating that role to the organization.
- Determines and implements an appropriate ERM infrastructure.
  - Assists management with integrating risk management with the strategic management process.
  - Develops and communicates risk management policies and limits, as approved by the CEO and the executive committee (or a designated risk management committee).
  - Identifies risk ownership gaps and overlaps requiring resolution to ensure appropriate ownership of the priority risks. Monitors the planned actions to fill the gaps and clarify the overlaps, working with the executive committee (or designated risk management committee) as circumstances dictate.
  - Works with appropriate executives to establish the control environment that (1) monitors risk across the enterprise, (2) oversees and enforces risk management policies and limits, (3) instills the discipline to close significant gaps in risk management capabilities and (4) ensures that organizational cultural issues are being managed effectively.
  - Assists the CEO and the executive committee (or a designated risk management committee) with monitoring the enterprise's critical risks.
  - Directs the BRMF (see Question 56) with respect to (a) the collection, aggregation, summarization and assessment of data points obtained from business units and support units (see Question 56) regarding

risk management performance and exposures to potential future events, and (b) the assembly and distribution of risk management reports.

- Establishes, communicates and facilitates the use of appropriate ERM methodologies, tools and techniques.
  - Establishes enabling frameworks, such as a common risk language, with which to facilitate the collection, analysis, synthesis and sharing of risk and risk management data, information and knowledge.
  - Validates measurement methodologies in place to ascertain the integrity of the underlying data and the reliability of reports.
  - Facilitates sharing of best risk management practices across the enterprise.
- Facilitates enterprisewide risk assessments and monitors the capabilities around managing the priority risks across the organization.
  - Coordinates the application of risk assessment across the organization to obtain an enterprisewide view of risk.
  - Periodically facilitates enterprisewide assessments of risk management policies, processes, competencies, reporting and systems to identify significant gaps in the capabilities around managing critical risks.
  - Works with business units and support units (see Question 56) to establish, maintain and continuously improve risk management capabilities enterprisewide.
  - As requested, consults with and assists managers of business units and support units (see Question 56) during their assessment of risk and formulation of risk responses.
  - Conducts risk management education and training from time to time.
- Implements appropriate risk reporting to the board, audit committee and senior management.
  - Develops measurement methodologies and monitoring methods, which aggregate risk exposures and risk management performance on an enterprisewide basis.
  - Supports the reporting of risk exposures and monitoring results to the board, CEO and executive committee (or a designated risk management committee).
  - Assists the CEO and the executive committee (or a designated risk management committee) with capital and resource allocation decisions.

To be truly objective and effectively positioned within the organization to enhance the appearance of objectivity, the CRO should be insulated from and independent of business unit operations. However, it is not unusual for one or more risk units (see Question 56) to report to the CRO if he or she is responsible for overall management of certain risks.

In addition to the above activities, the CRO can also provide an independent view regarding proposed business plans and transactions. The CEO and board often desire an objective assessment that the risks resulting from a transaction or deal are broken down into their fundamental components with a balanced view so they can be measured and systematically evaluated and managed. Executive management and directors must be on guard for managers who view the marketplace through "rose-colored" glasses to complete a transaction without considering its merits or consequences to the enterprise as a whole. That is why some companies may establish a strategic risk control or oversight unit led by a CRO who is independent of the business units.

A strategic risk control or oversight unit works with the operating units to disaggregate business plans and transactions into the component risks that the organization is taking on. Based on that understanding, the unit can then recommend how to improve proposed plans and transactions by mitigating some of the downside exposures that present potential obstacles. This is the ideal function of an oversight structure – some individual, group or committee acting as a risk unit to assist operating units with pulling things apart and understanding the important issues and the essence of what could happen, and then quickly and

succinctly communicating that understanding. The objective is to improve proposed business plans and transactions so they are more likely to succeed in creating while protecting enterprise value. The means by which this role is fulfilled – whether by a CRO, by an independent strategic risk unit or by some other group – is for senior management to decide.

51. What are the skill sets of the CRO?

Successful CROs have several common attributes. They have the ability to operate effectively and gain respect at all levels of the business, whether with directors and the CEO or with business unit and functional unit managers and employees. They have a broad understanding of all key areas of the business. Good CROs are not intimidated by hierarchy and position within the organization, and draw their influence through an active four-way communications and knowledge-sharing style.

CROs are senior executives with at least 12 to 15 years of experience. They possess the following skill sets:

- They are able to think strategically, i.e., they possess the authority and resources to monitor the performance of risk units and risk owners on matters of significance to the enterprise as a whole.
- They understand that organizations must take risks to compete and thrive in the global marketplace.
- They have excellent communication and facilitation skills.
- They are able to organize and motivate others, who in many cases may be in a more senior position.
- They have the ability to work with all levels of management.
- They have a strong presence and can interact effectively with senior management.
- They have previous experience reporting to boards and audit committees.
- When articulating their assessments, they are concise and direct under fire in their communications with top management and directors.
- They can effectively analyze significant amounts of data and information, and distill it to the key points that help senior management analyze risk in a given situation.
- They also have the capability to accumulate, summarize and interpret risk reports from business units, risk units, support units and assurance units (see Question 56).

Previous experience in auditing, risk assessment or risk management is a plus.

52. To whom does the CRO report?

If management desires to appoint a CRO, he or she should be positioned within the organization to enhance his or her objectivity, both in fact and in appearance. Often, the CRO is the ultimate ERM champion as it is applied to all units and divisions of the enterprise. As the ERM process champion, the CRO does not directly own responsibility for managing specific risks, but operates in a consultative and collaborative role, with authority vested by the executive committee (or a designated risk management committee), the CEO or the board (or a committee of the board). While this model can be sketched out in many ways, the consultative and collaborative process champion approach is the one that many organizations are generally adopting in practice, primarily because of cultural constraints. The primary variant in practice is whether the CRO reports to the CEO, to another senior executive (i.e., the CFO) or to the executive committee (or a designated risk management committee). We are also seeing some CROs with dotted line reporting to the audit committee (or to a risk management committee, if one exists) of the board.

THE RISK MANAGEMENT OVERSIGHT STRUCTURE

53. What is the primary purpose of the risk management oversight structure?

An effectively functioning oversight structure incorporates several of the elements of ERM infrastructure introduced in our response to Question 37. An oversight structure accomplishes many things. For example, it:

- Provides direction for the allocation of resources (such as capital) to risk management activities.
- Facilitates development of the organization's risk appetite and reaffirms that risk appetite, as approved by the board and executive management, in conjunction with its oversight activities.
- Establishes the appropriate ERM infrastructure for the organization, including risk policies, metrics, reporting and monitoring.
- Ensures that appropriate risk owners are designated on a timely basis.
- Determines that resources and staffing are sufficient, that incentives for desired behaviors are in place and that hiring, retention and training practices work as intended.
- Makes sure that managers at all levels are cooperating with and are active participants in the ERM process.
- Delineates the specific roles and responsibilities pertaining to risk taking versus risk monitoring.
- Provides assurance that communication plans are both coherent and capably executed.

The risk management oversight structure facilitates continuous improvement of the organization's capabilities around managing its priority risks. The oversight structure – guided by risk management goals, objectives and policies – is intended to assist directors and the CEO in balancing the organization's risk taking with its risk appetite. Management's challenge is to keep the entrepreneurial side and the control side of the enterprise in balance and to avoid letting either one of these two activities gain a disproportionate degree of strength relative to the other. Unrestrained and unfocused entrepreneurial activity leads to excessive risk taking and unethical behavior. An overemphasis on control leads to dysfunctional, risk-averse behavior. Neither of these extremes is as desirable as a reasonable balance.

The ultimate goal of continuously improving risk management capabilities and achieving balance is to protect as well as enhance enterprise value. For example, if the business generation side of the organization takes risk without regard to the entity's appetite for risk, it may not pay attention to the warning signs posted by the control side. That can get a business unit as well as the entire organization into a lot of trouble very quickly. Conversely, if the control side of the organization becomes every dealmaker's nightmare, it will squelch the creativity and entrepreneurial risk taking that goes with being a successful player in the marketplace. Because of constant change in the operating environment, extreme and out-of-balance conditions are undesirable regardless as to whether the enterprise has a low or a high risk appetite.

54. How are compensation issues considered when organizing the risk management oversight structure?

While crystal clear answers to this question are elusive because of the importance of the organization's facts and circumstances, we can point out some of the issues. There are often a myriad of compensation issues that have to be addressed to make sure that neither the entrepreneurial side nor the control side of the organization gets too far out front of the other. For example, if the control side is a group of "naysayers" who aren't particularly creative in making good deals better or marginal deals good, they won't be respected and effectively utilized by "deal makers." If they stop new business opportunities constantly without figuring out ways to fix problems, they will not be viewed as value-added. On the other hand, if unit managers are focused on getting deals done at any cost and there are no checks and balances, the organization may be exposed to

unacceptable risk. Because compensation is a critical determinant of behavior, compensation issues should be carefully considered. Ideally, the CRO needs to be independent and objective without a vested interest in whether business plans, deals and transactions are approved. For example, the CRO's incentive compensation might be linked to overall enterprise performance.

Behavior is strongly influenced when accountability for results is linked to the reward system. Accordingly, in risk management, it is important that performance expectations create incentives for balanced "results," i.e., "production without quality" should not be the goal. With a balanced focus on production, quality, cost and time, managers have strong incentives to set realistic targets, understand the risks and adopt objective measures.

Still, questions remain: How are managers rewarded? Should the control organization be rewarded for enabling more business to be completed successfully, or should it be a wall that can't be breached? At the same time, should business unit managers be rewarded for taking a broader enterprisewide view or for taking a business unit perspective? These are important questions because the way business unit managers and the so-called "star performers" are compensated can breed a cavalier and confrontational management style and "warrior culture" in which executives compete with each other to get as much capital allocated as possible to their unit's initiatives, regardless of the consequences to the enterprise as a whole. These managers can become dangerous as they pursue new sources of business without a balanced enterprisewide view as to both the downside as well as the upside and, as they do so, they could significantly exceed the entity's risk appetite as understood and approved by the board. Therefore, having an independent view of risk – whether through the executive committee, a CRO or an independent risk unit – is especially vital to managing risk, enterprisewide, within the established risk appetite. With respect to risk reporting, a CRO or independent risk unit can augment the governance process by making possible a "longer memory" in the CEO and the board and creating strong accountability of operating units to deliver on promised results.

55. Is there a recommended organizational oversight structure?

As noted in Question 53, the risk management oversight structure facilitates continuous improvement of the organization's capabilities for managing its priority risks and assists directors and the CEO in allocating resources and balancing the organization's risk taking with its risk appetite. There is no one-size-fits-all structure for accomplishing these objectives.

There are alternative organizational models. The Application Techniques of the COSO framework illustrate alternative approaches, along with the related benefits and challenges. The primary differentiator among the alternatives lies in the answers to the following questions:

- Who is responsible for identifying, assessing and responding to risk?
- Is it done centrally?
- Do the various units of the organization do it?
- Is it done both centrally and by the organization's units?

According to the Application Techniques:

> Many companies find that as they expand in size and complexity, they can most effectively apply enterprise risk management principles and disciplines by pushing much, if not all, responsibility to the lines of business and functional support units. At the same time, a small central supporting infrastructure addresses the more pervasive, entity-wide risks.

The COSO Enterprise Risk Management – Integrated Framework was designed to apply to all types of entities – public and private, small and large, for-profit and not-for-profit. So the framework was designed to provide a principles-based approach rather than setting down rigid rules.

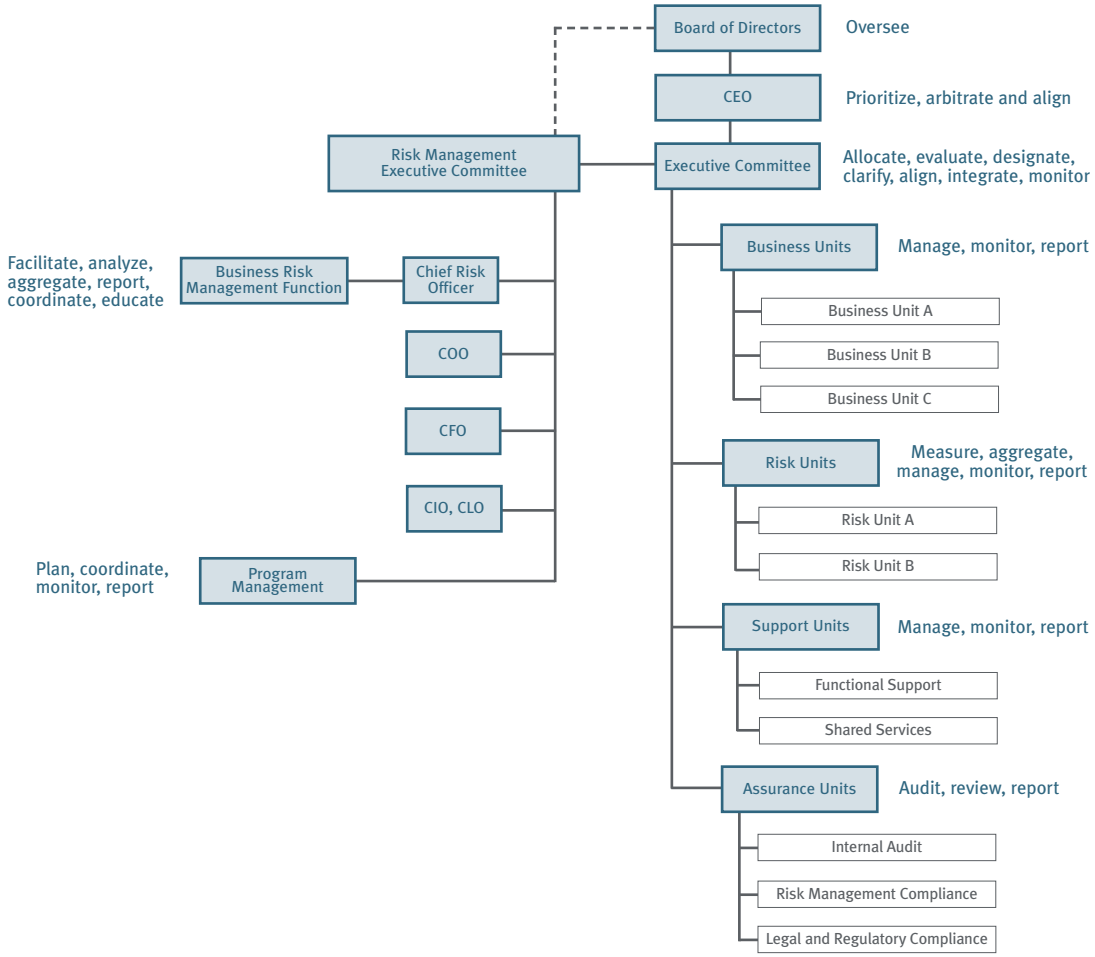
While selecting the appropriate organizational structure is more art than science, there must be a decision-making structure in place to break through the logjam of gaps and overlaps in risk management responsibilities that exist in many organizations. The key is to build on the existing management structure and to take into account the entity's business model, objectives, culture and risk appetite. For smaller organizations, the oversight structure can be as simple as the executive committee exercising its managerial prerogative to identify and prioritize risks, assign risk owners, analyze gaps, approve action plans and monitor results. For larger and more complex organizations, a chief risk officer and/or a risk management executive committee may be needed. Question 56 provides insights as to the potential pieces of the puzzle and provides some diagnostic questions to consider when selecting the appropriate organizational structure.

56. How does the risk management oversight structure relate to the entity's existing organizational structure?

An organizational oversight structure is needed to oversee risk management. Because an effective oversight structure often includes a board committee, a senior management working committee, a senior executive responsible for ERM, formal charters and job descriptions, and clear authorizations and reporting lines, it should be integrated with existing management structures and processes. The oversight structure clarifies the process ownership issues so that everyone who matters, from top to bottom in the organization, also has a role to play in managing risk.

A Baseline Oversight Structure

A baseline oversight structure helps us understand the potential elements of the oversight structure and how it is integrated within the existing organization.



The schematic on the previous page illustrates how ERM can be integrated within the existing organization. It depicts how directors, senior executives, units and functions all play a vital role in making an ERM infrastructure work. In viewing the schematic, recognize that business units, support units and assurance units already exist in most organizations. On the other hand, risk units may or may not exist, and provide an alternative for management to consider.

The essential elements of the organizational structure, as illustrated in the previous schematic, and the ERM-related roles and responsibilities across the organization are discussed below.

- The ***Board of Directors*** provides an oversight role, with emphasis on understanding the priority risks, approving risk management policies for critical risks and determining that risk responses for those risks are effective. This oversight activity may also be carried out by the audit committee, by a risk management committee (if there is one) and by other committees (such as the finance committee).

- The ***CEO*** is the "comprehensive risk executive." He/she is ultimately responsible for ERM priorities, strategies and policies, and acts as the final enforcer on such matters as aligning objectives, strategies and risk appetite, eliminating gaps and overlaps in risk management responsibilities and authorities, and resolving significant internal conflicts. The RMEC and other risk management oversight structure components are designed to support the CEO's delegation of these responsibilities. The CEO also ensures the ERM implementation is applied in strategy-setting.

- The ***Risk Management Executive Committee*** (RMEC) coordinates decision-making. For example, it recommends risk tolerances and profiles to the CEO and board in the context of the enterprise's business strategy. It evaluates risk measurement methodologies. It establishes capital allocation frameworks. It develops enterprisewide and specific risk policies and limit structures. It assigns owners of significant risks. It evaluates the effectiveness of the infrastructure in place for managing specific risks and ensures that necessary improvements are made to close any gaps. While the ***Executive Committee*** could retain these responsibilities for itself, many members of that committee can also serve on the RMEC. A separate RMEC may be appropriate if there is much to do with respect to improving risk management capabilities. In such instances, the RMEC oversees development of the ERM infrastructure needed to enable it to monitor risk policies and limits and to report to the executive committee and the board on the closure of gaps around the management of the priority risks. The RMEC has dotted line reporting to the board, as noted in the schematic, as it ensures that directors receive appropriate information about the enterprise's risks. It is periodically tasked by the board to follow-up on specific inquiries. It may or may not assume the role of a focused risk committee accountable for managing a specific risk (see discussion of ***Risk Units*** on the following page).

- The ***Chief Risk Officer*** (CRO) is a member of the RMEC and reports either to the CEO or to a ranking senior executive. The CRO oversees the business risk management function (see below) and is a key champion of ERM. The CRO may also have authority for managing selected risks on an enterprisewide basis (see Questions 50 through 52). He or she should chair the RMEC and have a reporting relationship to the board. The CRO should also facilitate the integration of risk assessment and management into the normal, ongoing strategic and business planning processes of the organization.

- To bring the top of the organization and its business units and their activities together, a ***Business Risk Management Function*** (BRMF) provides "enabling frameworks." These tools are the common language that facilitates the collection, analysis and synthesis of data and reporting of exposures and results of the process on an aggregate enterprisewide basis. The BRMF usually reports to a senior executive (i.e., a CRO) and/or the RMEC. Its charter is typically defined by the designated senior executive and/or RMEC and is approved by the organization's executive committee.

- Reporting to the RMEC (or to the CRO), the ***Program Management*** function provides the oversight necessary to ensure effective integration and coordination of multiple projects conducted over the ERM journey life cycle. For relatively simple ERM solutions, this function will be unnecessary. For more complex solutions, ERM may be achieved in stages over time in the form of multiple, related projects. In such instances, a program management discipline may be needed. See Question 138 for further discussion.

- ***Business Units*** are the line operations of the enterprise with specific objectives, strategies, markets, customers and products. Successful business units know their competition, their customers, their opportunities and their risks. They manage and monitor operations to generate revenues, satisfy customers, increase quality, compress cycle time and reduce costs. They offer products and services to targeted market segments at a price sufficient to cover the related costs and risks and generate acceptable risk-adjusted returns for shareholders. They report their activities to the CEO and executive committee.

  Risk must be a top-of-mind issue for business unit executives. Business units often take risks when they introduce a new product, enter a new market or invest in a new R&D initiative. They have many exposures relating to the customer relationships, supplier relationships, employee "talent pool" and proprietary assets they manage. These exposures and the uncertainties affecting them need to be understood and the business unit should have the capabilities to manage them. In essence, front-line business unit management is responsible for and is the first line of defense against many of the risks inherent in their chosen business model.

  Business units:

  - Align their risk priorities, tolerances and strategies with enterprisewide policies and guidelines
  - Target business and product development activities to create new sources of value consistent with the enterprise's overall risk appetite
  - Identify, source and measure risk
  - Benchmark processes and share best practices with the objective of continuously improving measures and processes
  - Assign risk management responsibilities and accountabilities to key managers
  - Report on the overall quality of risk responses, control activities and information and communication, as applied to specific risks
- ***Risk Units*** are an optional component of an ERM solution, and may or may not already exist within the organization. Risk units manage specific risks that are inherent in the enterprise's business model but are either not managed by the business units or are more effectively managed across the enterprise, consistent with a portfolio view. The objective of a risk unit is to make risk management related to one or more risks a core competence of the organization. Risk units may be responsible for such risks as interest rate risk, currency risk, commodity price risk, credit risk, weather risk and catastrophic risk. They evaluate, pool, reduce, transfer and exploit the risks for which they are accountable. They work with the business units when those units consider taking on risks they do not have the knowledge and expertise to manage. Risk units are often an important contributor to the execution of the organization's business strategy. They may consist of a function or an autonomous unit within the organization, and may be accountable to a focused risk committee of senior executives.

  For example, when a proposed transaction, deal or investment (the "proposed investment") is considered, the interest rate risk component may be assigned to treasury or to the "IR desk," which evaluates this risk component in the context of the enterprise's existing aggregate interest rate risk portfolio. That evaluation is made an integral part of the overall risk assessment of the proposed investment. If the proposed investment is consummated, the interest rate risk component is managed on an enterprisewide basis as opposed to a standalone transaction or unit basis. The incremental exposure may be offset against other rate risks in the enterprise's consolidated pool of interest rate exposures. Or it may be hedged to transfer the risk through a derivative transaction. Or the risk may be accepted without further action to exploit the market as a "pure play" on rates.

  To be effective, risk units must build the capabilities needed to manage risks that business units do not or cannot manage because they lack the competencies to do so. Risk units support the business model for creating enterprise value by providing directors and the CEO assurance that the risks undertaken do not exceed the enterprise's risk appetite. In doing so, risk units significantly contribute to the protection of enterprise value. But if they profit from taking on risk, they also evolve to "value creation status" as well (e.g., GMAC and GE Capital).

Risk units also assist business managers in identifying and evaluating all of the risks and business assumptions associated with a proposed transaction, deal or investment. They assist the CEO and the board by providing assurance that the most capable individuals and tools have been brought to bear with respect to the risk component the unit manages. Therefore, risk units can be charged with underwriting specific risks undertaken by business units with respect to specific transactions, deals and investments. In doing so, they ensure that a portfolio view of the risk is taken on an enterprisewide basis.

- Success in ERM ultimately is determined by the extent to which line and functional managers cooperate with and actively participate in the process. Functional managers are responsible for ***Support Units***. They manage activities such as human resources, information systems and facilities management. Support units work closely with business units and risk units to manage risks that are germane to their specialized skill sets. The managers responsible for certain support units, such as the chief information officer and the chief legal officer, may participate on the RMEC to coordinate certain activities germane to risk management so that they can be more effectively integrated.

- ***Assurance Units*** play an important validation role. They include risk management compliance, internal audit and value at risk review. In some organizations, these groups may be one and the same. They perform audits and periodic or continuous reviews to provide assurances to the RMEC and the board that the critical processes are performing effectively, key measures and reports are reliable, and established policies are in compliance. Internal audit, for example, is undergoing a transition because the traditional compliance-driven audit approach of the past is not dynamic or forward-looking enough to function effectively in an ERM environment.

Again, we are not suggesting that there is anything new with any of the above components. The above discussion provides a context for the diagnostic questions provided below.

Many Variations Are Possible

While there is nothing new about any of the above components, the participating directors, senior executives, units and functions ALL play a vital role within the organization in identifying and managing risk. Every organization should ordinarily have business, support and assurance units. Risk units, on the other hand, are optional depending on the complexity of the risks inherent in the business model.

When evaluating the organizational oversight structure for risk management, there are many possible variations. Often, companies implement an approach in which the CRO takes a consultative and collaborative approach with the business units. To be effective, an oversight structure must be designed to have "teeth" so it can serve as both the "referee" and the sponsor for moving the organization forward to an ERM environment and instilling the focus, discipline and control to improve risk management capabilities. Access to the CEO and the board when significant risks and process ownership issues arise is vital. Responsibility for risk-taking activities must always be delineated from risk monitoring and oversight activities. Therefore, the CEO, executive committee and the board must vest the authority for oversight in the appropriate individuals.

Some Diagnostic Questions to Consider

Following are some questions to consider when evaluating the organizational oversight structure for risk management. As pointed out in Question 55, there are many alternative models to consider. While it's difficult to generalize, the distinctions between these alternatives can be summarized in terms of several design principles relating to the roles and authorities at various levels of the organization. These principles are expressed by the questions below:

- What is the role of the board and the CEO? Effective risk management starts at the top.

- Is there a need for a RMEC? Does the executive committee have time to focus on the issues, or is it necessary to designate a separate committee?

- If there is a RMEC, who is on it? What are its role and responsibilities? How does the committee interface with the strategy-setting process?

- Does the organization designate a single officer to assume certain overall responsibilities for risk management, e.g., a "CRO" or equivalent executive? If yes:
  - Is this officer independent of the core business activities?
  - If there isn't a single risk officer, is there a committee (or equivalent group) with similar responsibilities?
- If there is a single risk officer OR a risk committee (or equivalent group) with overall responsibilities for risk management:
  - To whom does the officer or committee report, e.g., to the CEO or to the RMEC?
  - What are the overall responsibilities assumed by the officer or committee?
  - What is the nature of the risks integrated under:
    - The officer's job description?
    - The committee's charter?
  - If there is a RMEC, what is its composition?
  - What are the roles and responsibilities, as summarized in the job description and/or charter?
  - Is the role consultative (assess and recommend) or authoritarian (approve) or both?
  - Are governance functions (e.g., internal audit, risk management oversight/compliance and value at risk review) included or separate, i.e., do they report to the officer or committee or to someone else or some other group?
    - Note that the internal audit function should have a reporting line responsibility to the audit committee.
  - If there is a single risk officer:
    - Is there a functioning RMEC with whom that executive works?
    - Is there adequate support staff?
- What are the roles and responsibilities of business unit and divisional management?
- What are the roles and responsibilities of support unit management?
- Are there unique risks inherent in the organization's business model requiring one or more risk units to house, develop and maintain the competencies needed to assess and manage them?
- What independent validation and compliance functions are there? To whom do these functions report? Examples of such functions include internal audit, risk management oversight/compliance and value at risk review.
- Is there clarity as to roles and responsibilities for managing the priority risks?
  - Do you know what your priority risks are?
  - How is accountability for managing risk determined?
  - Who "owns" the responsibility for identifying, assessing and managing specific risks and through what channels do they report results? Is there a risk owner assigned to manage each priority risk? (See Question 57.)
    - Are there gaps (no owner of a risk) to be filled?
    - Are there overlaps (too many owners of a risk) to be eliminated?
  - How are compensation practices aligned with the desired behaviors?

- Are risk management tasks balanced centrally and locally? If so, how? Is it clear as to which tasks are to be accomplished centrally and which tasks are to be executed by the business units?

Depending on the answers to these and other relevant questions, an appropriate oversight structure is designed. Remember: Design the oversight structure on the existing management processes and keep it as simple as possible.

While the above discussion may seem complex, it is provided to introduce the issues involved in designing the appropriate oversight structure. This is necessary because, as noted earlier, there is no one-size-fits-all solution.

57. Does implementation of ERM require the identification of individual risk owners?

Yes. Whether through the executive committee or RMEC (as discussed in Question 56), resolution of the process ownership questions for critical risks is one of the most important tasks in implementing ERM. Who decides the capabilities needed to manage a given risk? Who designs these capabilities? Who executes? Who monitors performance? Management may not make the final decisions on all of these questions with respect to each of the enterprise's key risks, but it ensures that responsibilities, authorities and accountabilities are defined and articulated clearly so that an individual, a group or a designated unit is accountable for managing each risk.

The accountable individual, group or unit to which we are referring is the "risk owner." The so-called risk owner has the responsibility, authority and accountability to manage the risk. Risk owners, at a minimum, must decide, design and monitor. They *decide* on the risk responses and *design* the capabilities for managing the risks in accordance with the selected risk response. These capabilities preferably should address the source or root causes of the risk. The specific design should consider the needed policies, specific process and control activities, necessary skills, management reports, supporting methodologies and systems and data. Risk owners *monitor* these capabilities over time to make sure they perform as intended. If gaps are noted, they fix them on a timely basis.

Risk owners may elect to outsource the responsibility to build and execute capabilities. However, if they do, that does not compromise their ownership of the risk. The executive committee (or RMEC) makes sure that risk owners are designated for each critical risk and monitors risk owner performance over time.

THE ROLE OF INTERNAL AUDIT

58. What roles does internal audit play in ERM implementation?

The chief audit executive (CAE) and internal audit can play one or more of the following roles in conjunction with implementation of ERM in an organization:

- ***Educator***: Many senior executives don't understand ERM. The CAE can help them understand and use the COSO ERM framework through periodic education over time. If the CAE chooses to deploy the COSO ERM framework when developing focused audit plans, communicating audit results and making presentations, he or she will educate executives and directors in the various components of ERM.
- ***Facilitator***: ERM requires quality risk assessments. Internal audit can play a lead role within the organization by facilitating risk assessments and formulation of risk responses. Internal audit also can play a consultative role in assisting the organization in translating risk assessments into risk responses.
- ***Coordinator***: To the extent that the organization's ERM solution utilizes a common language and other "enabling frameworks," internal audit can play a value-added coordination role to ensure consistent deployment across the enterprise. The CAE can be a proponent of a common language.

- ***Integrator***: Internal audit can assist with (a) the collection, analysis and synthesis of risk-related data fed from multiple sources across the enterprise and (b) the reporting of exposures and audit results on an aggregate enterprisewide basis.
- ***Evaluator***: Internal audit can use the eight components of the COSO ERM framework to evaluate risk management, either for the organization as a whole or for a division, subsidiary or unit. In addition, internal audit can evaluate:
  - The effectiveness of the Internal Environment component, as defined by the COSO ERM framework
  - The effectiveness of the risk assessment process, taking into consideration the Objective-Setting, Event Identification, Risk Assessment and Risk Response components of the COSO ERM framework
  - The effectiveness of control policies and procedures related to specific risk responses, as explained by the Control Activities component
  - The quality and reliability of the information and communication supporting the organization's selected risk responses
  - The effectiveness of monitoring, as defined by the Monitoring component

The above roles are consistent with the assurance and consulting activities envisioned by The Institute of Internal Auditors (The IIA) in its definition of internal auditing. The IIA has asserted the following point of view:

> Organizations should fully understand that management remains responsible for risk management. Internal auditors should provide advice and challenge or support management's decision-making, as opposed to making risk management decisions. The nature of internal auditing's responsibilities should be documented in the audit charter and approved by the audit committee.

Consistent with the above point of view, The IIA has identified core roles for internal audit in ERM implementation as well as roles that are not appropriate for internal audit. Examples of core internal audit roles include the following:

- Giving assurance on the risk management processes
- Giving assurance that risks are correctly evaluated
- Evaluating risk management processes
- Evaluating the reporting of key risks
- Reviewing the management of key risks

The roles The IIA has indicated internal audit should not undertake are:

- Setting the risk appetite
- Authorizing and dictating the implementation of risk management processes
- Assuming the role of management in providing assurance on risks and risk management performance
- Making decisions on risk responses
- Implementing risk responses on management's behalf
- Accepting accountability for risk management

In addition, between these two extremes, The IIA has noted there are other "legitimate internal audit roles," provided there are appropriate safeguards in place. These roles include:

- Facilitating identification and evaluation of risks
- Coaching management in responding to risks

- Coordinating ERM activities
- Consolidating reporting on risks
- Maintaining and developing the ERM framework
- Championing establishment of ERM
- Developing a risk management strategy for board approval

59. Should internal audit lead the ERM effort?

We do not recommend it. Management implements ERM as an integral part of the organization's activities. As noted in our response to Question 58, the CAE and internal audit can perform many value-added roles, including promoting and introducing ERM and generating interest in the process. In essence, the CAE can provide the spark that can help start the ERM journey. However, internal audit should not function in the role of management. Ultimately, ERM must be driven from the top of the organization.

60. Should internal audit integrate the COSO ERM framework into its work?

When the COSO Internal Control – Integrated Framework was issued in 1992, visionary CAEs adopted it as a framework for audit planning, audit execution, and reporting on audit results. That framework wasn't required at that time, but the CAEs who used it discovered that it refreshed their function's audit approach and enhanced the value contributed to their organizations through the audit results they communicated to management and the board. While the new ERM framework is neither a requirement nor a mandate, we predict visionary CAEs will deploy it as part of their function's activities just as they did years ago with the Internal Control – Integrated Framework. Like all such changes, the objective will be to increase the value internal audit contributes to the organization.

61. Hasn't internal audit evaluated the application of ERM within the organization?

Not necessarily. ERM has never been defined as a standard, under due process, until COSO issued the ERM framework. In the past, ERM has been defined as people chose to define it. Going forward, companies now can compare their view of risk management against the COSO framework.

In addition, many internal auditors have evaluated various aspects of their organization's risk management. The COSO framework now gives them an opportunity to take a fresh look at their approach.

62. Does the Institute of Internal Auditors (IIA) support the COSO Enterprise Risk Management – Integrated Framework?

Yes. The IIA was an avid supporter throughout the framework's development.

63. Do The IIA standards require the use of the COSO Enterprise Risk Management – Integrated Framework? For example, what is the relationship of ERM to IIA Standard 2010.A1 (which requires internal audit to undertake an annual risk assessment) and 2110.A2 (which requires a broad risk assessment aligned with the COSO framework)?

The IIA standards did not include such a requirement at the time this publication went to print. The COSO Enterprise Risk Management – Integrated Framework provides insights into approaches to improve risk assessment methodologies. Therefore, internal auditors may use the framework to augment their annual risk assessment methodologies. If management is implementing ERM, internal audit should incorporate this activity into the risk assessment and audit planning process. In other words, once an organization begins its ERM journey, it makes sense for internal audit to broaden its audit focus using the ERM framework.

As a member of COSO, The IIA clearly had input into, and supported the design, rationale and spirit of, the ERM framework. Therefore, application of the framework by internal auditors should be considered desirable and appropriate in light of existing IIA Standards. Standard 2110.A2 clearly supports the concepts in the framework.

RISK MANAGEMENT VISION AND OBJECTIVES

64. How does management develop a shared vision for the role of risk management in the organization? What is the practical use of a shared vision?

The first step in implementing an ERM solution involves developing a shared vision of the role of risk management in the organization. A working group of senior executives should be empowered to articulate this role and define relevant goals and objectives for the enterprise as a whole and its business units. Based on an understanding of the key business units and risks, this articulation provides a "big picture view" of how to organize the entity's risk management, and should be aligned with the organization's business objectives and strategy. It is built on an enterprisewide risk assessment and a gap analysis for the organization's priority risks.

Thus the "risk management vision" is a shared view of the role of risk management in the organization and the capabilities desired to manage its key risks. It is periodically evaluated in the spirit of continuous improvement. To be useful, the risk management vision must be grounded in specific capabilities that must be developed to improve risk management performance and execute management's selected risk response. Risk management capabilities consist of the ERM infrastructure as well as the specific capabilities that relate to managing the priority risks. To illustrate:

(1) Defining the specific capabilities around managing the priority risks begins with selecting the priority risks and determining the current state of risk management capability. Once the current state is determined for each of the key risks, the desired future state is assessed with the objective of advancing the maturity of the capabilities around managing those risks. See Question 111 for examples illustrating risk management capabilities at different stages of maturity.

(2) Examples of elements of the ERM infrastructure are listed in our response to Question 37. They include, among other things, an overall risk management policy, an enterprisewide risk assessment process, integration of risk responses with business plans, presence on the board and CEO agenda, a chartered risk committee, clarity of risk management roles and responsibilities, dashboard and other risk reporting, and proprietary tools to portray a portfolio view of risk.

The greater the gaps in the current state and the desired future state of the organization's risk management capabilities (item (1) above), the greater the need for ERM infrastructure (item (2) above) to facilitate the advancement of risk management capabilities over time.

After the ERM solution is clarified by the risk management capabilities required to close significant gaps and deliver management's desired outcomes, a business case is needed to justify the economics of implementing it. A plan is then developed to build and test the required capabilities and integrate them into the enterprise's existing processes. This plan is monitored against appropriate milestones over time. The COSO ERM framework can be used to benchmark the organization's risk management at the beginning of this process, during the process and, once management completes all milestones under its plan, at the end of the process.

In summary, the risk management vision is a "call for action" to drive the organization to identify, design and build the risk management capabilities needed to close significant gaps and make management's selected risk responses happen. It provides a sense of purpose and focuses subsequent development of more specific risk management goals and objectives. The following is an example of an overall risk management vision statement of a global company with more than 60 operating units:

Business Risk Management is a continuous process, and an element of Corporate Governance. It promotes efficient and effective assessment of risk, increases risk awareness and improves the management of risk throughout the Group. This includes anticipating and avoiding threats and losses as well as identifying and realizing opportunities.

The risk management vision should address the need to make the organization better at managing risk through the collective and coordinated capabilities of specific functions, departments and units. For example, the above vision statement asserts that business risk management is a continuous process and an integral element of corporate governance focused on creating and protecting enterprise value. One individual or function cannot possibly realize this vision alone.

65. How does management define the entity's risk management goals and objectives?

Once the shared vision is articulated, overall risk management goals and objectives must be defined. While a vision statement is often aspirational, the goals and objectives should ordinarily describe in simple terms what is to be accomplished. They should be actionable by the organization. They should be defined in the context of the organization's business strategy. For example, some common risk management objectives chosen by companies to frame their ERM approach include the following:

- Develop a common understanding of risk across multiple functions and business units so we can manage risk cost-effectively on an enterprisewide basis.
- Achieve a better understanding of risk for competitive advantage.
- Build safeguards against earnings-related surprises.
- Build and improve capabilities to respond effectively to low probability, critical, catastrophic risks.
- Achieve cost savings through better management of internal resources.
- Allocate capital more efficiently.

Risk management goals and objectives should be consistent with and supportive of the enterprise's business objectives and strategies. Therefore, the organization's business model provides an important context for risk management. For example:

- It targets the markets and geographies in which the firm does business.
- It specifies the products and services it provides to those markets, the channels it uses to access those markets and the characteristics by which it differentiates its products and services in the eyes of the customer.
- It is built on many important elements: on the processes through which the entity converts materials and labor into products and services; on the employees the entity hires, trains and retains; on the suppliers and customers with which the organization does business; and on the shareholders and lenders that supply it capital.

Business risks are inherent in all of these elements. As the enterprise executes its strategy, it creates and increases its exposures to uncertainty. Therefore, business objectives and strategies provide the context for understanding the risks the enterprise desires to take. COSO affirmed this point by establishing "objective-setting" as a component of the ERM framework.

When defining risk management goals and objectives, management should ask "tough questions," such as those listed below:

- What are our business objectives and strategies? What are our financial targets, e.g., profitability, size and revenue growth? What values do we want to build and reinforce?

- What markets do we choose? What relative market position do we seek? What is our business model for winning in our chosen markets?
- What specific possible future events do we face? Are they related?
- How sensitive are our strategies, markets, earnings and cash flow to the occurrence of future events? How risky are our tangible and intangible assets for creating value? What are the loss drivers affecting those assets?
- Which specific future events could, if they occurred, affect our organization's ability to achieve its objectives relating to quality, innovation, timeliness, safety, compliance, etc., and to execute its strategies successfully? Which events would affect our market share?
- How capable are we of responding to events beyond our control that may happen in the future?
- Do we know what our expected returns are, as adjusted for risk? Do risk-adjusted returns vary by business unit? By major product? By geography?
- Finally, if we decide to accept the exposures inherent in our business model that give rise to our existing risks, do we have sufficient capital to absorb significant unforeseen losses should they occur?

The above questions provide a powerful context for defining risk management goals and objectives.

Following is an example of a statement of risk management vision, mission, goals and objectives:

Vision:

Contribute to the creation, optimization and protection of enterprise value by managing our business risks as we create value in the marketplace.

Mission:

Create a comprehensive approach to anticipate, identify, prioritize, manage and monitor the portfolio of business risks impacting our organization. Put in place the policies, common processes, competencies, accountabilities, reporting and enabling technology to execute that approach successfully.

Goals and objectives:

(1) Design and execute a global business risk management process integrated with our strategic management process:

- Integrate business risk management with our strategy formulation and business planning processes;
- Articulate our strategies so that they are understood throughout our organization;
- Establish KPIs designed to drive behaviors consistent with our strategy; and
- Reward effective articulation and management of key risks.

(2) Ensure that process ownership questions are addressed with clarity so that roles, responsibilities and authorities are properly understood.

(3) Design and execute a global process to monitor and reassess the top quartile risk profile and identify gaps in the management of those risks, based upon changes in business objectives and in the external and internal operating environment.

(4) Define risk management strategies and clear accountabilities and action steps for building and executing risk management capabilities and improving them continuously.

(5) Continuously monitor the information provided to decision-makers in order to assist them as they manage key risks and protect the interests of shareholders.

66. What is "risk appetite" and how is it different from "risk thresholds," "tolerances" or "limits"?

The COSO ERM framework defines "risk appetite" as follows:

> Risk appetite is the amount of risk, on a broad level, an entity is willing to accept in pursuit of value. It reflects the entity's risk management philosophy, and in turn influences the entity's culture and operating style. Many entities consider risk appetite qualitatively, with such categories as high, medium or low, while others take a quantitative approach, reflecting and balancing goals for growth, return and risk. A company with a higher risk appetite may be willing to allocate a large portion of its capital to such high-risk areas as newly emerging markets. In contrast, a company with a low risk appetite might limit its short-term risk of large losses of capital by investing only in mature, stable markets.

The COSO ERM framework defines "risk tolerance," which is a term often used interchangeably with such terms as "risk threshold" or "risk limit," as follows:

> Risk tolerance is the acceptable level of variation relative to achievement of a specific objective, and often is best measured in the same units as those used to measure the related objective.

Based on COSO's definitions of these terms, we can make the following observations:

Risk appetite is strategic. According to COSO, it is a "guidepost" in strategy-setting. The organization's business model provides an important context for assessing risk appetite by clarifying the activities the entity undertakes, who its customers are, what its products are, and how and in which markets it conducts business. A thorough understanding of an organization's business objectives, strategy and operations is very useful when articulating the risks it chooses to accept and the risks it chooses to avoid as it creates value. As the enterprise executes its strategy, it creates and increases its exposure to uncertainty. Therefore, business objectives and strategies provide the context for understanding the risks the enterprise chooses to undertake. Risk appetite also can set boundaries around opportunity-seeking behavior, which impacts the entity's objectives and strategies.

Risk appetite relates primarily to the business model whereas risk tolerance relates primarily to the entity's objectives. An organization's risk appetite reflects both its capacity to bear risk as well as a broader understanding of the level of risk that it can safely assume and successfully manage for an extended period of time. Risk appetite is the extent to which an organization exposes its capital and sources of value to the exploitation of strategic opportunities and retention of performance variability and loss exposure.

Every organization has a risk appetite whether it acknowledges it explicitly or not. Risk appetite is expressed through an entity's actions or inactions. It represents executive management's "view of the world," which drives their strategic choices. It is inherent in the organization's strategy and in the execution of that strategy, in the form of both risks taken and risks avoided. In defining ERM, COSO set a standard for management to manage risk within the entity's risk appetite, as understood and agreed by the board of directors. Management considers risk appetite when defining objectives, formulating strategy, allocating resources, setting risk tolerances and developing risk management capabilities. The board considers risk appetite when it approves management actions. If articulated explicitly, risk appetite provides overall direction for risk management and is grounded during the objective-setting process.

While risk appetite is strategic, risk tolerance is tactical. Risk tolerance is defined within the context of the related objective using the metrics in place to measure performance against that objective. Risk tolerances set the boundaries of performance variability. Once tolerances are set, performance measures are monitored to ensure that performance is managed within those boundaries. Thus risk tolerances are used to ensure that performance variability is reduced to an acceptable level.

Risk tolerance may be reflected differently for different types of objectives, including objectives relating to earnings variability, interest rate exposure, compliance with laws and regulations and the acquisition, development and retention of people. Risk tolerance related to all of these objectives is expressed differently. In effect, risk tolerances address the question, "How much variability are we willing to accept as we pursue a

given business objective?" Guidance on this question is important as it helps managers assess their exposure in terms of the downside risks they are empowered to accept as they seek upside performance. As managers pursue opportunities for growth and new sources of profitability, risk tolerances and limits are an effective tool for countering pressures on them to succeed and produce results. In other words, risk tolerances and limits help managers understand that actions undertaken with the goal of being successful and producing results cannot be executed at all costs and without regard to the potential consequences to the organization as a whole if something were to go wrong.

67. Is there a defined methodology for calibrating performance with risk tolerances?

Calibrating performance with risk tolerances requires a measurement methodology, a monitoring process and a commitment to continuous improvement. This is often described as the "Plan–Do–Check–Act" cycle. "Planning" entails establishing objectives and the related risk tolerances as well as deciding on risk responses. "Doing" refers to the design and implementation of risk management capabilities. Monitoring performance falls under the category of "checking." Continuous improvement based on checking of results is "acting." The measurement methodology is the centerpiece of the cycle, because it facilitates all of the other tasks and is equivalent to "managing by fact." The message is that an effective measurement methodology is directly linked to the performance objective. In risk management, this concept applies best to those risks that are susceptible to measurement.

As noted in Question 66, COSO defines "risk tolerance" as "the acceptable variation relative to the achievement of an objective." There are three different types of risk tolerance, each of which is linked in some way to the distribution used to depict all sources of uncertainty associated with the future value of an exposure. These three types of risk tolerance are not meant to be mutually exclusive in a given situation, as all three could be relevant at the same time. They are introduced to capture the three ways risk managers tend to think about risk tolerance.

What's the message? When developing a policy related to the company's tolerance for risk, care must be taken to relate the policy to the relevant type of tolerance. Each type of tolerance will have different implications, and hence, each will require different policies.

Following are the three types of risk tolerance:

- ***Variability in achieving expected returns***: This articulation of tolerance is often referred to as "performance variability," which is the extent of variation around the expected value, or the level of uncertainty in the mean, or as COSO explains, in the achievement of an objective. It represents the uncertainty the organization is willing to bear in the realization of its expectations, or in the achievement of its objectives. Management has expectations about the performance of an asset, a product, a system, a business unit, etc. The more uncertainty there is about the ultimate realized value, the greater management's uncertainty. In the case of exposures distributed according to a bell curve, this type of tolerance is reflected in the company's risk appetite for the variance. The higher the variance accepted by managers, the higher their tolerance for performance variability.

  Relevant questions illustrating management's focus on understanding this type of tolerance include:

  - What volatility are we willing to accept in interest and currency rates?

  - How crucial is it for us to achieve forecasted earnings and cash flow? What is the minimum level of earnings and cash flow we can accept?

- ***Susceptibility to extreme events***: This articulation of tolerance is often referred to as a loss exposure, or loss driver, which is an exposure to catastrophic loss. Exposure to extreme events can occur without necessarily affecting the extent of variance, so this is a different type of uncertainty. In fact, the two types of uncertainty can occur simultaneously. Considering a bell curve, this form of tolerance is reflected in the company's taste for kurtosis. While a rather obscure statistical term, kurtosis refers to how "fat" the tails of the distribution are, meaning how likely extreme events will happen. The "fatter" the tails, the

higher the probability that there are extreme outcomes in the distribution of future possible events. Therefore, managers must at least acknowledge in the planning process that it is a statistical possibility, however remote, that something extreme could happen.

A concrete example might be accidents related to air travel. These accidents are rare, but when they occur, they are often catastrophic and highly visible. An airline could identify the factors impacting the probability an accident might occur, e.g., pilot error, pilot inexperience, poor maintenance practices, ice on the wings, poor plane design, etc. The successful airline manages its exposure to these factors in order to keep the odds of an extreme event, such as a crash, so statistically negligible as to make air travel safe in the eyes of the consumer.

A question relevant to this type of tolerance is:

– How exposed are we to business interruption, substantial losses of physical assets, catastrophic health and safety issues, or irreparable damage to reputation and image due to systemic failure to deliver on our brand promise?

- ***Inconsistency with the desired risk appetite***: This articulation of risk tolerance is the strategic issue of defining the organization's risk appetite in the context of its business model for creating and protecting enterprise value. As further explained in Question 66, risk appetite is management's choice of the distribution of future possible events or management's assessment as to whether the shape of the distribution of future possible events is consistent with the company's business objectives. In this context, management must address questions such as whether they want to take these kinds of risks or whether this is the business they want to be in. For example, the CEO may be overdosing on risk beyond an acceptable level with an acquisition or growth strategy. In such cases, there may be incongruities in the business model because it fails to effectively balance the creation of enterprise value with the risk appetite considered acceptable by the board. Thus, the distribution of an exposure may be highly skewed, exposing enterprise value to unacceptable risk. Alternatively, the distribution has other features, which are difficult for the company to manage or which do not otherwise match its risk appetite. Or the organization may have retained an exposure, which is inconsistent with its business objectives and risk appetite.

  To illustrate, assume a company produces a part that it should outsource to a supplier having the expertise and processes to produce that same part at a lower cost with comparable or superior quality. In this case, the company does not have the desired aggregate distribution of acceptable possible future events because the risks it assumes by manufacturing the part itself are not consistent with its core competencies. So, this type of risk tolerance is expressed in terms of how willing the company is to deviate from its desired risk appetite, whether for the enterprise as a whole (all exposures combined) or at the level of the individual exposure (an individual business unit, for example).

  Relevant questions include:

  - How well aligned is the overall distribution of risks we are undertaking with our risk appetite?

  - Have we aligned our risk taking with our core competencies, i.e., what we do best?

  - Do we tolerate or do we shut down off-strategy behavior?

  In summary, the business model must first be consistent with the organization's desired risk appetite. Then the organization must align its markets, products, processes, people, technology and places of operation with that model. Otherwise, the game is lost before it begins and risk management becomes an afterthought.

All of the illustrative questions included in this response are strategic in nature. Once managers understand these three illustrations of risk tolerance, they can better evaluate how risk tolerance can be articulated through risk management policies, as well as measured and managed by alternative risk responses.

68. How are the risk management vision and objectives translated into the appropriate ERM infrastructure?

Once the risk management vision and the related goals and objectives (including risk appetite and risk tolerances) are articulated, management defines the capabilities needed to implement the ERM infrastructure that will realize the vision and achieve the stated goals and objectives. "Capabilities" arise from an appropriate combination of policies, processes, competencies, reports, methodologies and technologies. Because companies have different objectives, strategies, structure, culture, risk appetite and financial wherewithal, no two approaches to implementing ERM infrastructure are alike. Therefore, the various capabilities supporting the ERM infrastructure for one company may differ from those of another company.

We recommend organizing the process of defining risk management capabilities in three phases. The first phase sets the foundation. The second phase builds capabilities for critical risks. The third phase enhances existing risk management capabilities. These three phases provide a suggested roadmap of eight steps for addressing the eight components of the COSO ERM framework, as illustrated below:

THE ERM ROADMAP

COMPONENT OF COSO FRAMEWORK	SET FOUNDATION		BUILD CAPABILITIES			ENHANCE CAPABILITIES		
	Adopt common language	Establish oversight and governance	Assess risk and develop responses	Design/ implement capabilities	Continuously improve capabilities	Quantify risk enterprise-wide	Improve enterprise performance	Establish sustainable competitive advantage
Internal environment	X	X	X	X	X	X	X	X
Objective-setting		X	X		X	X	X	X
Event identification	X	X	X		X	X	X	X
Risk assessment	X	X	X		X	X		
Risk response		X	X	X	X	X	X	X
Control activities		X		X	X	X	X	X
Information/ Communication	X	X	X	X	X	X	X	X
Monitoring		X		X	X	X	X	X

For example, as discussed further in Question 96, the SET FOUNDATION phase includes the step, "adopt common language." There are several possible elements to consider when formulating a common language for use in risk management, including a risk model, a risk management glossary, a process classification scheme and other relevant frameworks. These suggested elements of a common language are not intended to be all-inclusive, as there are others that might facilitate the adoption of a common language.

The same thought process also applies to the other seven steps. Every potential element germane to a particular step need not be implemented. The suggested elements provided within this publication are illustrative and intended to provide a starting point for management to consider. Management needs only select those elements considered essential in building and enhancing risk management capabilities. While the COSO components provide the evaluation framework necessary to assess the effectiveness of ERM infrastructure and underlying risk management capabilities, the three phases and eight steps outlined above provide the roadmap for how management can get from Point A to Point B.

The three phases to improving ERM infrastructure and risk management capabilities are briefly introduced below:

- **SET FOUNDATION**: Every organization needs to set a foundation by adopting a common language and establishing effective oversight and governance. As management coordinates its efforts, a common language is needed to communicate. Organizations that combine a common language with an enterprisewide risk assessment process attest to more effective discussions at the highest levels of the organization, particularly during the strategy-setting process. These discussions result in a better understanding of risk and lead to more timely and focused risk responses. With respect to oversight and governance, the board working with and through the CEO should understand what the key risks are, who is managing them and the effectiveness of performance. They should inquire as to whether there are any significant gaps in risk management capabilities and whether steps are being taken to close those gaps. The ultimate objective of the oversight process is to provide assurance to the board and CEO that the entrepreneurial activities and the control activities of the organization are reasonably in balance so that neither one is disproportionately stronger than the other.

- **BUILD CAPABILITIES**: Setting the foundation puts in place some of the elements of the ERM infrastructure needed to build and continuously improve capabilities around managing the priority risks. The goal is to design and implement repeating, well-defined capabilities for assessing, managing and monitoring risk and deploying those capabilities enterprisewide. The three steps of the "build capabilities" phase relate to the process by which management executes specific tasks with respect to managing risk. The three steps of this phase are, first, assess risk and develop responses, followed by design and implement capabilities and culminating with continuously improve capabilities, all contributing to a never-ending cycle for improving risk management performance over time. The development of uniform processes and tools for identifying, sourcing and measuring risk build confidence that all potentially significant future possible events are identified and the related risks are assessed, providing a basis for taking on risk with knowledge and evaluating and formulating risk responses. Once the appropriate risk responses are selected, capabilities are designed and implemented to execute them. These capabilities include the control activities, information and communication, and monitoring components, as explained in the COSO framework. Once implemented, risk management capabilities are continuously improved over time. Critical to all of these tasks is the collection and analysis of information for decision-making. Common processes pave the way for defining, organizing and reporting information, enterprisewide. They provide a systematic process for implementing enhancements to the organization's ERM infrastructure.

- **ENHANCE CAPABILITIES**: This phase enhances the organization's existing risk management capabilities and further integrates risk management with the strategy-setting process. It consists of three steps: quantify risk enterprisewide, improve enterprise performance and establish sustainable competitive advantage. These steps lead to more advanced capabilities, as the state-of-the-art evolves. For example, risk-adjusted performance measurement has evolved at world-class financial institutions and is considered a "best practice" for managing market and credit risks. VaR (Value at Risk) and EaR (Earnings at Risk) measurement methodologies are becoming more accepted by corporate enterprises and regulators alike. Increasingly, these and other capabilities are seen as invaluable for allocating capital and measuring performance based on the risks inherent in the business portfolio. They enhance established risk management capabilities by strengthening the link to defined risk tolerances and improving the evaluation of business performance.

As a general rule, the more mature an organization's capabilities in terms of the skills, processes and supporting methodologies and technology committed to risk management, the more effective the organization will be in implementing ERM. The three phases described above for building risk management capabilities are structured to provide overall guidance on proper sequencing of steps during the ERM implementation process.

> For example, when designing an ERM solution, start with setting the foundation FIRST. After setting the foundation, THEN proceed to building capabilities around the priority risks, with emphasis on closing significant gaps. THEN, focus on selected enhancements.

The concept of sequencing recognizes that effectively functioning risk management capabilities provide a basis for implementing subsequent enhancements. "Too far, too fast" is an all-too-familiar story in risk management.

The organization's business model and culture, the relative maturity of its risk management capabilities, the degree of centralization or decentralization, its risk appetite, the comparability of the risk profiles relating to different business units within the enterprise and other factors must be weighed when deciding which capabilities to build and enhance as the organization implements its ERM solution. The more management has enhanced capabilities in place, the greater the alignment of risk management policies, processes, people, technology and knowledge, and the greater the degree of integration with strategic and operating processes.

CONDUCTING RISK ASSESSMENTS

69. What is the relationship between risk assessment and risk management?

Risk assessment is the process of identifying, sourcing and evaluating individual risks and the interrelationships between risks. It provides a systematic approach to analyzing the impact of potential future events on the achievement of an organization's objectives. The risk assessment process itself typically encompasses an evaluation of available data and the application of judgment to determine the significance of potential future events and the likelihood of their occurrence. Effective risk assessment leads to formulation of risk responses. Therefore, the risk assessment activity is undertaken with a strong bias toward determining the need for further action.

Risk management, on the other hand, encompasses risk assessment as well as the activities associated with managing risk. These activities include policies, processes, competencies, reporting, methodologies and systems. The eight components of the COSO Enterprise Risk Management – Integrated Framework provide a point of view for understanding what risk management entails when applied during strategy-setting and across the enterprise. This framework includes three components – objective-setting, event identification and risk assessment – which are essential to assess risks effectively.

70. What is the relationship between risk assessment and performance assessment?

Risk assessment is a forward-looking activity applied to future possible events to identify the potential impact on the achievement of objectives and the likelihood of occurrence over a defined time horizon. ***Performance assessment*** is a retrospective activity applied to evaluate the performance of a unit, a process or a function against a pre-determined target or standard over a stated period of time.

Risk assessment is related to performance assessment because both activities apply to objectives. For example, as explained by the COSO framework, risk assessment begins with objective-setting to establish an effective context for identifying potential future events that create risks and opportunities. The assessment of a risk should desirably consider management's risk tolerance, which COSO defines as "the acceptable level of variation relative to the achievement of a specific objective." Risk tolerance is often best measured using the same units as those used to measure the related objective.

Performance assessment deals directly with the measure of an objective, which is often applied during the performance assessment activity. Performance assessment requires a pre-defined target or standard, defined in the context of an objective. Risk tolerance is often set using established performance measures as a framework for defining the limits of acceptable performance variability. Once tolerances are set, performance measures are monitored to ensure that performance is managed within those boundaries. Thus risk tolerance is used to ensure that performance variability is reduced to an acceptable level. Operators instinctively understand performance assessment because that is what they do on a day-to-day basis. For example, once performance gaps are identified, operators often focus on understanding the root cause of the gaps, designing and implementing process improvements to close the gaps, and monitoring performance to ensure the gaps

do not re-emerge. If the gaps re-emerge, the improvement cycle begins anew to eliminate them. Risk assessment, on the other hand, is a more difficult activity for operators to apply, because it deals with potential future events rather than historical past events. When risk assessment and performance assessment are effectively combined, management's focus becomes more anticipatory and less reactive.

71. What are the components of an effective objective statement and why are objectives important to an effective risk assessment?

Objectives are important to a risk assessment because they articulate what an entity is striving to achieve. An effectively articulated objective statement is realistic, understandable, measurable, believable and actionable. It is used to set the target or goal of an organization, business unit, process or function. In the context of ERM, it is important because the effect of risk is observed and measured as it impacts the achievement of business objectives. Objectives provide the context for identifying future possible events, which in turn provide the basis for conducting a risk assessment.

72. What is the difference between an event and a risk?

They are related concepts. According to the COSO Enterprise Risk Management – Integrated Framework, an event is "an incident or occurrence, from sources internal or external to an entity, that affects achievement of objectives." A risk is defined by COSO as "the possibility that an event will occur and adversely affect the achievement of objectives." Events can have either a negative impact or a positive impact. An event with a negative impact on achieving an objective represents a risk, which can prevent value creation or erode existing enterprise value. An event with a positive impact represents an opportunity. Thus an event is the circumstance that impacts an objective and creates the condition for a risk, IF it has a negative effect. For example, the failure of a supplier to provide a key production component is an event. As a result, the risk of not meeting production deadlines occurs, along with the related consequence of late deliveries to customers.

Under the COSO framework, event identification precedes risk assessment. There are events (e.g., changes in the market, in systems, in competitor products, in personnel, etc.) that may drive changes in the organization's view of risk. Understanding these internal and external factors helps make the risk identification and assessment more relevant, as conditions inside and outside the company constantly change.

73. Why doesn't COSO's definition of risk incorporate the notion that risk includes upside as well as downside?

COSO defines a "risk" as "the possibility that an event will occur and adversely affect the achievement of objectives." Some respondents to the ERM exposure draft argued that the definition of risk should not focus solely on the likelihood of bad things happening. These respondents argued that many risks also have an upside and should therefore include the likelihood of good things happening. In effect, they argued that risk is the distribution of all possible future events or outcomes, both positive and negative, in a firm's performance over a given time horizon due to changes in key underlying variables. The respondents also pointed out that the ERM framework would be more relevant if it incorporated the likelihood and significance of opportunities into the definition of risk.

COSO carefully considered this issue both before and after the issuance of the ERM exposure draft. As discussed in Question 72, COSO uses the term "event" to capture the positive and negative aspects of "what can happen" in the future. Events can have either a negative or a positive impact on an enterprise. A potential future event that could have a negative impact is a risk, whereas a potential future event that could have a positive impact is an opportunity. Based on input obtained from key user and stakeholder groups and the results of field tests, COSO concluded that most of the likely users of the ERM framework tend to think of risk in terms of the "downside" only. In other words, most users view risk as relating to the failure to achieve important objectives. Thus COSO concluded that broadening the definition of risk to include the potential for "upside" would cloud the concepts and frustrate a primary objective of the framework to provide a common language for ERM.

74. How do we articulate the concept of inherent risk so that it can be effectively used as risk assessment criteria?

Inherent risk is an essential aspect of assessing the significance of a risk and is defined in the COSO ERM framework as "the risk to an entity in the absence of any actions management might take to alter either the risk's likelihood or impact." In a risk assessment setting, inherent risk is more typically considered in the context of a risk's impact on the achievement of a business objective with no specified management processes or internal controls in place. While this concept is on one level easy to describe, it is at the same time difficult to apply in practice during a risk assessment. For many people, it is difficult to think about risks without considering the existing processes or controls in place.

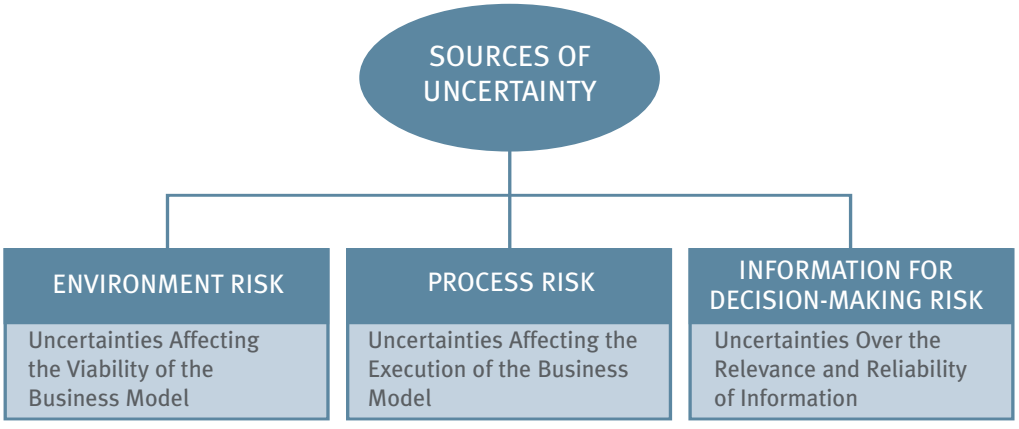
One way to describe inherent risk is the risk present in a business activity. Thus participants in a risk assessment envision a scenario where the business unit under assessment is newly formed in the same operating environment and under the same circumstances as the current unit operates. The participants can then ask the question, "What is the impact of the identified risk before any policies or control procedures are put into place?"

Some argue that an inherent risk approach is not as intuitive as a "residual risk" approach in which current policies and procedures are considered during the assessment. While a residual risk approach may be easier for some to understand, it can overlook a critical risk because the participants agree that the potential impact of the risk on the achievement of business objectives is negligible due to their collective perceptions around the effectiveness of existing risk management capabilities. If critical risks are ignored, management may not even be aware they exist, and the opportunity for sharing risk responses, control activities and best practices is lost. The COSO framework points out that risk should be assessed on a residual risk basis after considering risk responses selected to mitigate the significant risks.

75. Is there an officially endorsed risk language we can use for our organization?

As of the date of this publication, we are not aware of an authoritative risk language or model either adopted by COSO or any other organization. COSO's intent was to allow for flexibility in organizations in grouping potential events into categories. COSO points out "event categorization … allows management to consider the completeness of its event identification efforts." This is the central purpose of a common language. Either management begins a risk assessment with (a) a blank sheet of paper with all of the start-up that choice entails or (b) a common language that enables busy people with diverse backgrounds and experience to communicate more effectively with each other and identify relevant issues more quickly. COSO provides an example of event categories consisting of external factors and internal factors in the framework (see Exhibit 4.2 on page 34 of the framework).

The sources of uncertainty an enterprise must understand and manage may be external or internal. In addition, risk is about knowledge. When management lacks knowledge, there is greater uncertainty. Thus sources of uncertainty also relate to the relevance and reliability of information about the external and internal environment. These three broad groups – environment, process and information for decision-making – provide the basis for an enabling framework summarizing sources of uncertainty in a business.



- ***Environment risk*** arises when external forces can affect the entity's performance, or make its choices regarding its strategies, operations, customer and supplier relationships, organizational structure or financing obsolete or ineffective. These external forces include the actions of competitors and regulators, shifts in market prices, technological innovation, changes in industry fundamentals, the availability of capital or other factors outside the company's direct ability to control.

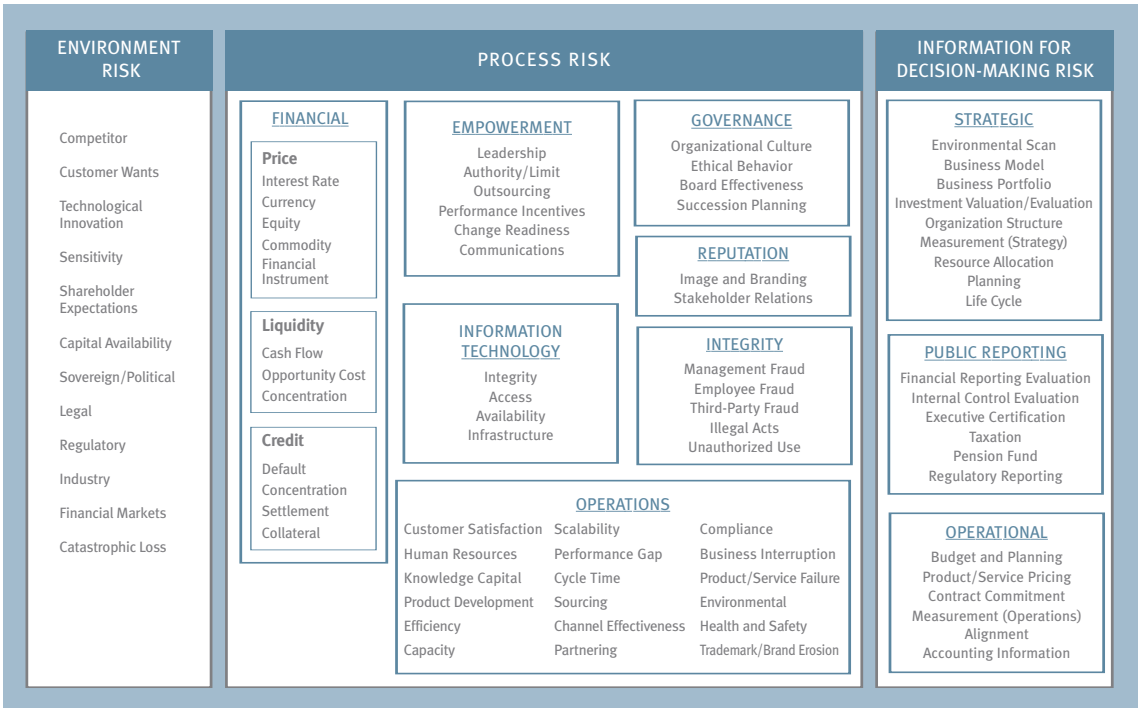
- ***Process risk*** arises when internal processes do not achieve the objectives they were designed to achieve in supporting the entity's business model. For example, characteristics of poorly performing processes, or process risks, include poor alignment with business objectives and strategies, dissatisfied customers and inefficient operations. They also include diluting (instead of creating or preserving) enterprise value; and failing to protect significant financial, physical, customer, employee/supplier, knowledge and information assets from unacceptable losses, risk taking, misappropriation or misuse.

- ***Information for decision-making risk*** arises when information used to support business decisions is incomplete, out of date, inaccurate, late or simply irrelevant to the decision-making process. These risks are uncertainties affecting reliability of information used to support decisions to create and protect enterprise value.

These three groupings of risk are interrelated. The environment risks and process risks that the enterprise faces are driven by the external and internal realities of the business. Information for decision-making risk is directly affected by the effectiveness and reliability of information processing systems and informal "intelligence gathering" processes for capturing relevant data, converting that data to information and providing that information to the appropriate managers in the form of timely written reports and oral communications. Process risk is sometimes indistinguishable from information for decision-making risk because information is needed to make informed decisions about a process. A steady flow of information should provide decision-makers the insights they need about the external environment and the performance of the firm's processes so that they can manage the organization's risks effectively. In summary, these three groupings of risk provide a broad foundation on which more specific categories of risk can be identified and detailed.

The three groupings of risk are depicted using the Protiviti Risk Model℠ shown below.

PROTIVITI RISK MODEL℠



Using this model, examples of events may be identified within each relevant risk category listed in the model. For example, catastrophic loss risk is the inability to sustain operations, provide essential products and services, or recover operating costs as a result of a major disaster. The inability to recover from such events in a competent manner could damage the company's reputation, ability to obtain capital, and investor relationships. There are two sources of events which can lead to catastrophic loss:

- Uncontrollable events: Disasters from war, terrorism, fire, earthquake, severe weather and flooding, and other similar events that are completely beyond the control of the company. While these events cannot be prevented or even predicted, their effects on the organization's assets and operations can be managed.
- Controllable events: Some events can be as catastrophic in their effects on a business as an uncontrollable disaster. For example, environmental disasters, pervasive health and safety violations, spectacularly large underwater real estate deals, headline-grabbing high litigation costs, huge losses from derivatives, massive business fraud, and significant losses in market share due to failure to abandon strategies that no longer work. The business activities that contribute to these events are within the control of the company, i.e., they may be impacted by management's choices or by the effectiveness of the internal control environment.

COSO recommends a "top down" approach, i.e., management defines the objectives of the organization and the related risk categories impacting those objectives. Specific events are then identified within each category. Thus the use of a common business risk language begins at a strategic level, starting with a model like the one on the previous page, and is then customized to the unique circumstances of each business unit. A well-conceptualized model is a springboard to deeper discussions and understanding of risk, an essential step or "building block" towards ERM.

76. To what extent does the organization strictly define risk for the enterprise as a whole, when the organization has a variety of different businesses?

A common risk language begins at a strategic level for the enterprise as a whole and is customized to specific units, geographies and products. This "cascading" approach has the advantage of identifying risks that are common across the enterprise. For operating units with distinctive risk profiles, however, the overall risk language must be customized to address the unique risks faced by those units. The distinction is an important one. Risks common to all business units drive enterprisewide risk responses. Risks unique to individual units drive unit-specific risk responses.

77. What are risk maps and how are they used appropriately during the risk assessment process?

Risk mapping is probably the most common tool used by companies to identify and prioritize the risks associated with their business activities. The most effective use of risk mapping occurs when it is integrated with business planning and used to identify areas requiring further analysis and specific risk responses. For example, as a ranking and prioritization technique, risk mapping is especially useful in facilitating dialogue. From a decision-making perspective, it is more of a directional than an actionable tool.

The basic technique is intuitive and simple to understand. Business unit managers assess their risks using pre-determined criteria. Their assessments often address a set of possible future events identified by senior management or, alternatively, possible future events identified by unit management. Once well-defined potential future events are identified, they are plotted on a grid or map according to their impact on the achievement of business objectives and the likelihood of their occurrence.

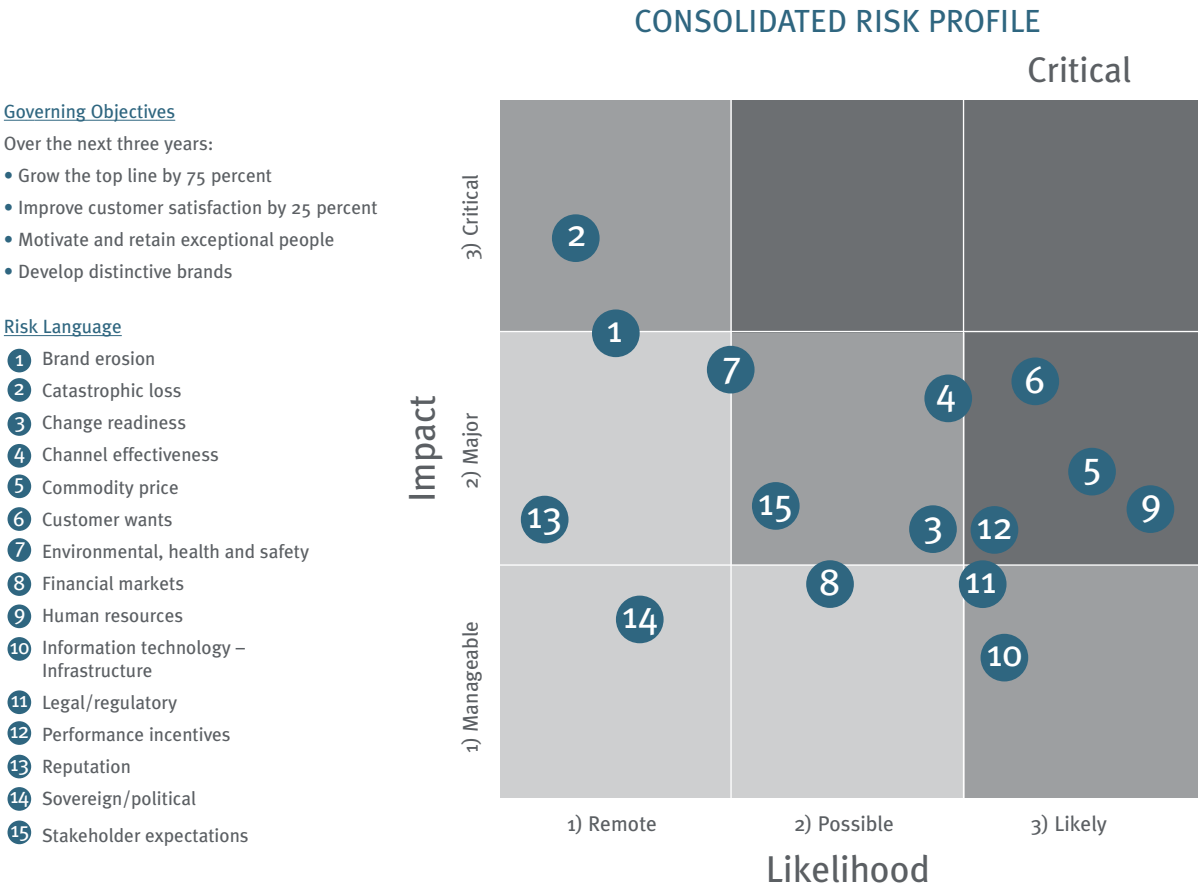
Following is commentary on these assessments:

- ***Impact***: Management rates the significance of risk to the business in terms of the effect on achieving business objectives. The risk mapping tool is flexible enough to consider other criteria, including the potential financial impact, the impact on the execution of key strategies and the potential cost to the business in terms of losses of capital, earnings, cash flow and brand equity. The greater the significance of the impact, the more severe the risk. When rating impact, time horizon is a factor that must be clearly

defined. For example, one company might assess the significance of risk to the execution of its strategy over the next three years. Another might assess the risk considering a one-year business-planning horizon (the time frame within which many unit managers operate). If time horizon is not clearly and consistently articulated, the participants in the process will get confused. For example, some issues, such as a capacity shortage, can be quite severe over the short term to a manufacturing company. However, most risks, including capacity, are less of an issue over the longer term because management has more flexibility to make adjustments. Therefore, management should define time horizon explicitly. Separate risk maps are appropriate for events likely to occur over the short, intermediate or long term.

- ***Likelihood***: Using the same time horizon as that used for determining impact, management assesses the likelihood that an identified potential event, or two or more potential events, will occur. The higher the probability of occurrence, the greater the likelihood. When estimating likelihood, the evaluator should consider the quality of the assessment itself. Just how likely is the risky event? If statistical methods are not used, then how do you know that the selected probabilities are reasonable? While statistics are not necessary at this stage of the assessment process, the most knowledgeable personnel should prioritize the risks. At this stage, management is often looking for an order of magnitude estimate (as opposed to a precise number). There are techniques available to apply the judgment of an "expert jury" to accomplish this assessment for critical risks not subject to rigorous measurement.

An example of a risk map is provided below:



78. What's an effective way for an organization to conduct a risk assessment?

There are many ways to conduct a risk assessment. For example, companies may conduct interviews or surveys of key personnel, review key documents, conduct facilitated workshops, perform targeted reviews, or utilize any combination of these options. The following table discusses each of these options:

	INTERVIEWS	ONLINE SURVEYS	PAPER SURVEYS	DOCUMENT REVIEW	FACILITATED WORKSHOPS	TARGETED REVIEWS
DESCRIPTION	Individual stakeholder interviews to identify potential events and prioritize associated risk	Online survey consisting of either a checklist of events or risks OR an open-ended request	Hard copy survey consisting of either a checklist of events or risks OR an open-ended request	Review of existing public documents, regulatory reviews, audit reports, special purpose studies and other materials	An in-person or online workshop attended by key stakeholders	Special studies or targeted analyses to evaluate questions about specific events or anticipated concerns
ADVANTAGES	• Interaction provides opportunity to: - "Set the stage" - Ask the appropriate follow-up questions - Probe/ understand underlying root causes - Clarify questions, if necessary - Cover sensitive topics more thoroughly • More insight and depth regarding potential future events	• Can be accessed by participants without limitations of time or geography • Can support the process with links to risk definitions and additional resources • Can be delivered efficiently at low cost (relative to interviews) • Can be administered to large numbers of people • Self-documenting and reporting • Efficient, easy to administer to large numbers and geographies • Standardized scales can lead to common aggregation • Can track status	• Can be completed by participants without limitations of time or geography • Can be delivered efficiently at low cost although not as cost-effective as online • Can be administered to large numbers of people • Standardized scales can lead to common aggregation	• Comprehensive in scope • Fact-based • May provide basis for quantifying risk • Less time required of stakeholders during fact gathering process • Not limited to internal documents	• Interaction among knowledgeable participants creates broad picture of potential events and related business impact • Interaction stimulates discovery of previously unidentified risk areas, which can remain undetected in other formats • Structure provides for efficient use of time • Collaboration builds consensus around priority risks and their impact • Similar to interviews, interaction provides opportunity to: - "Set the stage" - Ask appropriate follow-up questions - Probe/understand underlying root causes - Clarify questions, if necessary - Cover sensitive topics more thoroughly • Discussion and collaboration regarding priority risks can provide quality inputs to risk response planning	• Same advantages noted for document reviews • Conducted by subject matter experts • Accommodates in-depth understanding of specific potential events and related business impact • May be applied on a macro or micro basis • Can integrate external/internal perspectives • Can provide recommended risk responses
ISSUES	• Time intensive • Scheduling challenges • Logistics must be managed • Interviewer must subjectively aggregate the data points • Individual interviews do not directly support consensus-building	• Limited follow-up • Post-survey time is required to review and understand responses • Risk of misinterpreting responses • Depth of responses may be limited • Individual responses do not gain from the perspective of others	• Same issues noted for online surveys • Not considered "best practice" • Greater elapsed time to send and receive • Compared to online surveys, more time and effort to: - Distribute - Support - Process - Monitor progress - Compile results	• Higher cost to review and analyze existing material • Often not forward-looking • May not reflect current business realities • If unfocused, can waste time and money	• Effectiveness is dependent on facilitator and sufficient structure • Requires advance planning • Logistically challenging to arrange participant's time and location • Can be time-consuming due to numbers of people and need to clarify event definitions	• Expectations must be clearly set • Must be carefully scoped • Often requires more time than other options

As previously noted, any combination of these options is appropriate.

For companies that have not completed an enterprisewide risk assessment, we recommend the use of a facilitated workshop that convenes a meeting of key stakeholders to assess and prioritize risks. Enterprise risk assessment workshops are often attended by members of the senior management team and also may include participants possessing companywide knowledge of compliance, information technology, marketing or other activities integral to the organization's core mission.

The use of a facilitated risk workshop for assessing risks provides certain advantages over an assessment by a single individual. Identifying a knowledgeable group of stakeholders and bringing them into a collaborative environment for the purpose of assessing risk can efficiently identify risks arising across the enterprise, and achieve consensus and alignment regarding priority risks and possible actions to take to mitigate those risks. In addition, group sessions can facilitate learning by clarifying differences in perspectives, raising awareness of the organization's most significant exposures, surfacing sensitive or previously unrecognized issues and promoting communication across individual areas of responsibility. These sessions may be preceded by interviews, a risk survey and/or a document review to facilitate paring down the list of risks to a more manageable one for the purpose of conducting the workshop within the allotted time.

79. What are the common mistakes and pitfalls during the risk assessment process?

In our response, we will focus primarily on risk workshops. Inefficient risk workshops occur for many reasons – lack of planning, not adhering to the agenda, lack of clear ground rules and not seeking the input of all participants, to name a few. For the risk assessment process to be effective, management must take care to avoid common mistakes and potential pitfalls. These are noted below:

- ***Lack of clarification and common understanding of the meaning or definition of risk***: Applying too narrow a focus to the meaning of risk can lead management to overlook potential events and issues. It is important to consider all relevant business objectives as a context for a risk assessment.
- ***Not including all stakeholders***: Failing to include all of the stakeholders in the workshop, survey or interview process can be fatal. "Stakeholders" include any person directly impacted by the issues under discussion or whose lack of inclusion could undermine the achievement of the desired outcome.
- ***Not considering or giving appropriate weight to knowledgeable positions***: In a group risk assessment setting, there will ALWAYS be one or two individuals who know a great deal more about a risk than the others. The purpose of the assessment is to hear, consider and learn from everyone who has knowledge of a particular risk. Therefore, it is important to create an open environment to share all information about a risk and arrive at the best possible understanding. Effective assessment of the likelihood and impact of a potential future event is not necessarily the result of the total number of votes or responses. Dialogue is often more important than the voting process during a risk assessment.
- With respect to a facilitated risk workshop:
  - ***Setting unclear or unrealistic objectives***: It is important to work with the meeting sponsor to set meeting objectives that everyone will understand and accept.
  - ***Failing to structure the meeting agenda for success***: Once the meeting objectives are set, it is important to organize the meeting to ensure the objectives are achieved. For example, keep in mind the following:
    - Walk the meeting sponsor through the proposed agenda to make sure he or she agrees with it.
    - While time is always limited, make sure you have allotted enough to accomplish your objectives. If you don't, revisit the objectives to align them with the available time.
    - Carefully consider whether there is any aspect of the agenda that might be different from what the participants might expect. If this is the case, consider how to communicate the design decision (e.g., change in approach, reordering of information, etc.) to the meeting participants. For example, prior

to a risk assessment, participants may be provided a risk model (as illustrated in Question 75) and asked to consider the probability of occurrence and potential impact of different possible future events. Because of a need to save time during the session, an agenda design decision is made to combine these two criteria into a single assessment of "level of risk" for use during the workshop. If this change is not properly presented to the participants, the difference between their expectation, which was created through their preparation for the session, and the actual activity applied during the workshop, can create confusion and cause the facilitator and the process to lose credibility.

Review supporting materials (such as strategic planning documents, internal management reports, stated business objectives, etc.) carefully if they will be incorporated into a workshop. Do not assume that every participant is familiar with the material, understands it and supports it. Check the facts in advance.

- ***Placing too little emphasis on discussion***: Remember that while voting is interesting during a risk workshop, it is only a means to an end. The discussion is just as important.
- ***Letting technology glitches distract the process***: If the technology is not operating as it should during a risk workshop (e.g., you are using voting keypads and are only getting nine votes when you are supposed to be getting 10), don't let the technical difficulty disrupt the meeting. Try to conduct the workshop without highlighting that things are not working.
- ***Not getting everyone involved***: It is common for facilitators to become mesmerized by the discussion and to miss key discussion points. They should pay attention to the participants, note the pace and tone of the conversation and get people involved, making everyone's time as productive as possible. If participants become bored or distracted, the facilitator must get to work. Participation correlates to the perceived value received from the assessment.
- ***Not creating a "safe" and open environment***: Encourage open communication, with explicit agreement regarding the use of information. Identify and, if necessary, meet and understand the person who could potentially undermine the results of the workshop. For example, this could be the CEO, board chair or most senior person in the room. It also could be individuals who tend to dominate discussion. Not only do you want to know if they understand the material being presented, you also need to be sure that they understand and support the workshop objectives. A facilitated risk assessment cannot succeed without an open environment in which candid discussion can occur.
- ***Failing to clarify roles and responsibilities***: Facilitators should communicate the approach and plan an agenda in advance. There must always be only ONE facilitator. Work out expectations so there aren't any contradictions between the facilitator, the subject matter expert and other team members, which can interrupt the flow of the meeting.
- ***Poor facilities***: Room shape and size is important during a risk workshop. Try to avoid conference tables, if possible. The ability of the facilitator to move within a "u-shaped" setting supports group interaction. This dynamic can and should be applied to create a robust environment for communication. It encourages the participants to be more involved.

• With respect to setting the ground rules for a risk assessment:

- ***Lack of participant understanding of how to apply assessment criteria consistently***: The participants need to understand the criteria for assessing impact and likelihood of occurrence. If there is confusion in applying the scale used during the assessment, the process will not be successful.
- ***Confusion over inherent risk***: This is an area that confuses many participants in a risk assessment. See our response to Question 74.
- ***Confusion over time horizon***: This is another area that confuses participants. See our response to Question 77.
- ***Not acknowledging that the future is inherently unknowable***: On the surface, this point is obvious. Yet, many managers often assess the future with a "single-point-estimate" perspective. That is why it is important to be open to a broad range of possibilities during a risk assessment. The art and science of risk assessment should be applied to create the greatest chance of success in identifying potential future events, assessing their likelihood and impact, and formulating cost-effective risk responses.

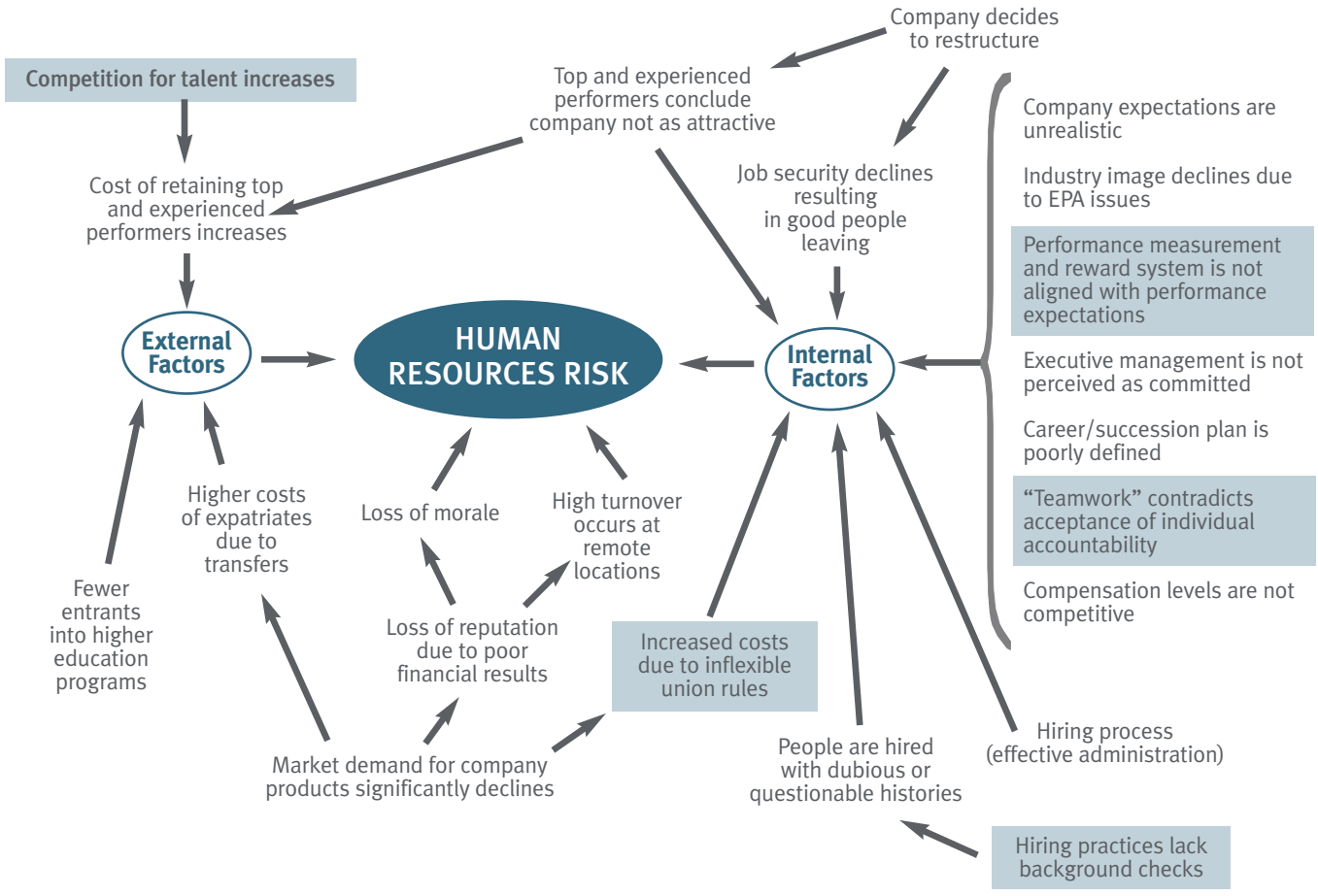
– ***Overlooking external environment events because of a perception that they are outside of management's control***: A risk assessment should focus on all potential future events of consequence, whether they are controllable or not. For example, while management may not have direct control over political and legislative outcomes, there are nonetheless potential mitigation activities which can only be developed by assessing this category of risk. To illustrate, these activities might include lobbying, awareness campaigns, plans for responding to changes in the political environment, etc.

– ***Ignoring the interrelationships among risks***: The participants to a risk assessment must acknowledge that there are cause-effect interrelationships between multiple events, with the occurrence of some events causing or triggering the occurrence of other events. This is a point that requires thought and consideration during the risk assessment process.

80. How do we identify, understand and apply interrelationships among risks?

The COSO framework states: "Where potential events are not related, management assesses them individually … But where correlation exists between events, or events combine and interact to create significantly different probabilities or impacts, management assess them together. While the impact of a single event might be slight, the impact of a sequence or combination of events might be more significant."

Most individuals can visualize how to assess an individual event. The question many ask is, "How do you assess multiple, interrelated events?" There are various approaches to identifying and understanding interrelationships among risks. One, a risk drivers map, is illustrated below:



The common thread in all approaches, including the one in the previous illustration, boils down to assessing the following question: Will the occurrence of one event, either individually or in combination with other events, cause another event to happen or, alternatively, affect, impact or contribute to the severity of another event? For example, by following a pattern of analysis as just illustrated, a model of interrelationships among events for a risk category ("hiring and retention risk") can be described. Through refinement of this cause-effect analysis, management can select the most critical events (the ones shaded in the previous illustration) and focus additional attention on understanding them.

By examining the critical events related to multiple risk categories, management can evaluate the interrelationships between those events. This understanding of potential future events to source why, how and where the entity's risks originate lays a foundation for developing measurement and monitoring tools addressing risk through a portfolio view.

81. What is the appropriate level of depth when assessing risk?

Judgment regarding the level of depth at which risks are assessed is made within the context of the objectives and events being evaluated. In order to craft an appropriate risk response, there must be sufficient clarity as to the nature of the risk, including how, why and where it is sourced. An understanding of the nature of the risk facilitates development of a mitigation strategy. If risks are assessed at too high a level, it is difficult to identify the precise issue and management will be unable to decide what to do after the assessment is completed. At the same time, if the assessment is conducted at too granular a level, the "big picture" issues get lost in a sea of details and it will be difficult to complete the risk assessment in a reasonable amount of time.

Thus the evaluator may find a common language useful for aggregating multiple risk events for purposes of conducting the risk assessment. Priority risks can then be disaggregated into relevant future possible events when formulating an appropriate risk response. Experience is the best teacher as to the appropriate level of depth for purposes of conducting a risk assessment. Ultimately, the goal is not the risk assessment itself, but to move beyond the printed page of the risk assessment into actionable steps in the business plan.

82. Who should participate during the risk assessment process?

The appropriate participation in the risk assessment process is influenced by the objective of the risk assessment and the scope of the risks being assessed. At the entity level, executive management should be included. In some cases, individuals with specific knowledge of unique business risks, issues and operations may be included to provide input on their specific areas. In other cases, the board of directors may be engaged. At the unit level, unit management and key process owners should be included in the assessment process.

83. How is risk assessment related to risk quantification and should risk quantification be used during risk assessment?

Risk assessment is improved and is more robust when risks are quantified. When risk is quantified, it can be monitored against management's established risk tolerance (see Question 67). Risk measures are discussed further in our response to Question 112.

84. Is there value in using qualitative information when assessing risk?

Yes. Because the future is inherently an "unknown," it is often necessary to make qualitative assessments of the impact and likelihood of risk using the best information available. Some risks do not lend themselves to quantitative measurement because the related events occur so infrequently and, if and when they do occur, they are subject to such a wide range of possible outcomes in terms of severity that it is difficult, if not impossible, to quantify them. When that is the case, the managers closest to the source of the risk are the individuals best positioned to understand its nature and root causes. Consider the risk to an automobile manufacturing organization when a defective electrical connection leads to brake failure for a particular car model. The direct impact of administering the recall program and incurring warranty costs for that particular model may be projected based on quantitative information. The impact on sales of other models and the time and cost to overcome the effects of reputation damage to the company overall is a qualitative judgment that is best evaluated

through the collective input of marketing, sales, production and economists. When applying qualitative data, it is helpful to obtain perspectives from multiple individuals, as any one individual's view of risk will be limited to their own experience and may be affected by their own personal stake in the outcome of the assessment.

Qualitative information is most effective when used in conjunction with reliable metrics and other quantitative data. When reliable metrics are not available, qualitative information is often directional at best (i.e., it serves as a pointer to specific areas for further investigation and analysis) and is not effective in driving management decisions.

GETTING STARTED – SET THE FOUNDATION

85. What are the best steps to take when getting started?

For organizations choosing to broaden their risk management focus to ERM, there are five practical implementation steps to get started. While these steps provide a simplified view of the task of implementing ERM, the implementation process does not occur overnight and, for certain, is not easy to accomplish. ERM is a journey. These steps provide a starting point for that journey. It is important that all of these steps have the support of senior management, and that the appropriate foundation has been set to gain buy-in from all participants.

STEP 1: Conduct an enterprise risk assessment (ERA) to assess and prioritize the critical risks.

An ERA identifies and prioritizes a company's risks and provides quality inputs for purposes of formulating effective risk responses, including information about the current state of capabilities around managing the priority risks. It is a risk assessment spanning the entire organization, including critical business units, functional areas and business processes. It encompasses the objective-setting, event identification and risk assessment components of the COSO ERM framework and provides a holistic, portfolio view of risk. It is applied using the business strategy as a context. Questions 69 through 84 provide guidance on conducting risk assessments.

If a company has not identified and prioritized its risks, ERM becomes a tough sell for senior management because the value proposition can only be generic. Using the entity's priority risks to identify gaps provides the basis for improving the specificity of the ERM value proposition. Risks are prioritized using the business strategy as a frame of reference.

STEP 2: Articulate the risk management vision and support it with a compelling value proposition using gaps around the priority risks.

This step provides the economic justification for going forward. The "risk management vision" is a shared view of the role of risk management in the organization and the capabilities desired to manage its key risks. It is further discussed in Questions 64 and 65. To be useful, this vision must be grounded in specific capabilities that must be developed to improve risk management performance and achieve management's selected goals and objectives.

"Risk management capabilities" include the policies, processes, competencies, reporting, methodologies and technology required to execute the organization's response to managing its priority risks. They also consist of what we call "ERM infrastructure." In terms of making decisions as to whether to improve ERM infrastructure, there are two points to keep in mind:

Point (1): Defining the specific capabilities around managing the priority risks begins with prioritizing the critical risks (see Step 1 with respect to conducting an ERA) and determining the current state of capabilities around managing those risks. Once the current state of capabilities is determined for each of the key risks, the desired state is assessed with the objective of identifying gaps and advancing the maturity of risk management capabilities to close those gaps.

Point (2): ERM infrastructure consists of the policies, processes, organization oversight and reporting in place to instill the appropriate focus, discipline and control around continuously improving risk management capabilities. Examples of elements of ERM infrastructure include, among other

things, an overall risk management policy, an enterprisewide risk assessment process, presence of risk management on the board and CEO agenda, one or more chartered risk committees, clarity of risk management roles and responsibilities, dashboard and other risk reporting, and proprietary tools that portray a portfolio view of risk.

What's the message? The greater the gap between the current state and the desired state of the organization's risk management capabilities [Point (1)], the greater the need for ERM infrastructure [Point (2)] to facilitate the advancement of those risk management capabilities over time. A working group of senior executives should be empowered to articulate the role of risk management in the organization and determine the structure and timetable for making it happen. This group should articulate a compelling business case that defines the expected capabilities from the ERM solution and the economic justification for moving forward. The above inputs facilitate this process.

STEP 3: Advance the risk management capability of the organization for one or two priority risks.

This step focuses the organization on improving its risk management capability in an area where management knows improvements are needed. Like any other initiative, ERM must begin somewhere. Possible starting points include:

- Compliance with corporate or governance initiatives such as the Sarbanes-Oxley Act or Basel II
- Evaluating enterprisewide risk assessment results to identify priority areas other than financial reporting (e.g., other compliance risks, information technology risks, selected operational risks, etc.)
- Integration of ERM with existing management structures and processes (e.g., strategic management, annual business planning, new product launch or channel expansion, quality initiatives, performance measurement and assessment, offshore production and outsourcing planning, etc.)

STEP 4: Evaluate the existing ERM infrastructure capability and develop a strategy for advancing it.

It takes discipline to advance the capabilities around managing critical risks. The policies, processes, organization and reporting that instills that discipline is called "ERM infrastructure." The purpose of ERM infrastructure is to eliminate significant gaps between the current state and the desired state of the organization's capabilities around managing its key risks. Some examples of ERM infrastructure were provided above when discussing Step 2. Other examples include a common risk language and other frameworks, knowledge sharing to identify best practices, common training, a chief risk officer (or equivalent executive), definition of risk appetite and risk tolerances, integration of risk responses with business plans, and supporting technology. ERM infrastructure is discussed further in Question 37.

ERM infrastructure facilitates three very important things with respect to ERM implementation. First, it establishes fact-based understanding about the enterprise's risks and risk management capabilities. Second, it ensures there is ownership over the critical risks. Finally, it drives closure of significant gaps. If the existing organizational oversight structure provides the discipline, focus and control to make these things happen, then very little change is necessary organizationally to move the ERM implementation forward.

ERM infrastructure is not one-size-fits-all. What works for one organization might not work for others. The elements of ERM infrastructure vary according to the techniques and tools deployed to implement the COSO framework, the breadth of the objectives addressed, the organization's culture and risk appetite, the nature of its risks and the extent of coverage desired across the organization's operating units. Management decides the elements of ERM infrastructure needed according to these and other factors. When making this decision, management considers the elements of ERM infrastructure already in place.

STEP 5: Update the ERA for change and advance the risk management capabilities for key risks.

At this stage, the organization has advanced its capabilities for one or two priority risks (see Step 3) and has implemented ERM infrastructure (see Step 4) to make these improvements happen. Now management is in a position to broaden the focus to other priority risks by updating the ERA for change and determining the

current and desired states for each priority risk using the business strategy as a context. The objective is to advance the maturity of the capabilities around managing the priority risks.

Risk management capabilities must be designed and advanced, consistent with an organization's finite resources. For each priority risk, management evaluates the relative maturity of the enterprise's risk management capabilities. From there, management needs to make a conscious decision: How much added capability do we need to provide reasonable assurance we will achieve our business objectives? Further, what are the expected costs and benefits of increasing risk management capabilities? The goal is to identify the organization's most pressing exposures and uncertainties, and to focus the improvement of capabilities for managing those exposures and uncertainties. The ERM infrastructure which management has chosen to put in place drives progress toward this goal.

The capability maturity model discussed in our response to Question 111 provides a framework for evaluating the maturity of an organization's risk management capabilities. Using this model, management rates the enterprise's capabilities in key risk areas, identifies gaps based on the level of capability desired in specific areas, and shifts the dialogue on operating metrics to incorporate appropriate emphasis on process maturity. The ERM infrastructure ensures that the evaluation process is fact-based and conducted with integrity by the participating risk owners. Where there are unacceptable gaps, the enterprise should organize appropriate activities to build, test and integrate over time the expected capabilities, as described by the business case.

86. Is ERM another "project"?

No. ERM is a journey because it represents a commitment to continuous improvement. Because an organization's risks are constantly changing, so must its risk management capabilities constantly improve. ERM provides the focus, discipline and control for making that happen over time within the context of the strategy-setting process.

87. Are there specific things an organization should accomplish the first year?

The organization should understand the overall risk management objectives and obtain buy-in from senior management. Ideally, the organization should set the foundation by adopting a common language and establishing effective oversight and governance. On the foundation of these elements of ERM infrastructure, the organization builds the appropriate process with emphasis initially on an ongoing enterprisewide risk assessment process. During the first year, companies also should consider the following:

- Inventory the activities that may be occurring across the enterprise to improve risk management capabilities and build on those activities.
- Leverage past risk assessment results as much as possible to gain insight into the priority areas.
- Take into account the current state of the existing capabilities using the capability maturity model (see Question 111) and avoid over-engineering the process.
- Focus on achieving visible successes.

88. Who is responsible for "leading the charge" to implement ERM?

Executive management is responsible for leading ERM implementation. They must demonstrate a commitment to ERM through consistent actions to create and sustain momentum for the initiative. See our responses to Questions 7, 39, 40 and 89.

89. Who should sponsor ERM implementation?

While they may delegate specific responsibilities to others, the CEO and executive management team should be the ultimate sponsors of the ERM implementation. See Questions 39 and 40.

90. How is buy-in obtained from key senior executives?

Increasing ERM capabilities requires a focused and disciplined approach that is consistent with the organization's structure and culture and with management's operating philosophy. Following are suggestions for obtaining buy-in from senior executives:

- ***Top management commitment and support***: Discipline starts at the top with a committed CEO and executive management who demonstrate support for ERM through consistent actions that create and sustain momentum for the initiative. They must decide whether to go forward and, once that decision is made, they must provide unwavering support. To obtain their buy-in, the ERM initiative should be integrated with existing management processes and linked to significant issues that are clearly on the senior management agenda. Executive management will have little appetite for an appendage or overlay.
- ***With executive management's assistance, develop a strong business case that clarifies why improving risk management is the only option***: A business case addresses the internal and external pressure points that create the need for change as well as the state of readiness and existing structures which can drive or constrain change. Executive management should answer the following question, "What is the role of risk management in our organization?" As discussed in Question 85, the business case should be grounded in the organization's priority risks and in the gaps in capabilities around managing those risks. It should assert and explain why risk management is integral to strategy-setting. See Questions 134 through 136 for further discussion of the business case.
- ***Focus on the big picture with a compelling shared vision***: Once the need has been established, top management must provide a compelling, shared vision of the future goal state that provides direction for positive change. This vision should clearly describe the scope, goals and objectives for the ERM initiative and articulate the "what's in it for me" for everyone expected to contribute to the design and implementation process. This vision should articulate a value proposition that highlights unacceptable gaps in risk management capabilities (see Question 85) and provides economic justification for closing those gaps.
- ***Set realistic goals***: Risk management objectives should not exceed the firm's capacity for executing risk management capabilities. For example, an organization at the initial or repeatable stage in specific risk areas, as further explained in Question 111, cannot be expected to function at the managed state overnight. Goals should be understandable, measurable and actionable.
- ***Develop a clear plan of action***: A well-defined plan for change provides a roadmap for the organization to proceed as well as milestones to monitor progress. This plan supports the business case.
- ***Make periodic use of management checkpoints***: Management checkpoints serve many purposes. Most importantly, they keep the program on-plan and on-strategy, serving as both a reality check and reaffirmation of management support. They also provide needed motivation to move the design and implementation activities along.

91. How do we obtain buy-in among our operating managers?

Operating personnel have many exposures. They manage inventories, plants, equipment and other physical assets; products and processes; brands; external relationships with customers and suppliers; and talented and skilled people. These sources of value are affected by many uncertainties. For example, changes in demographics can impact customer demand for the company's products. They also can affect the talent pool

of people who perform skilled tasks within the business, thus raising the stakes in the search for talent. In today's risky times, operators can benefit from thinking about the risks they face in the future and the alternatives available to managing those risks.

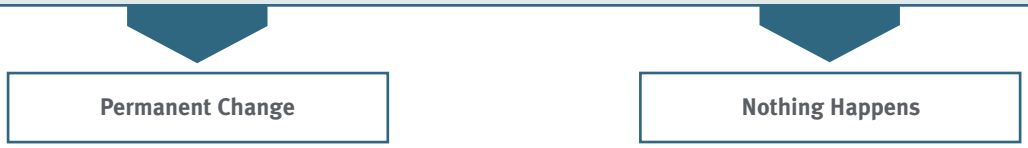
One challenge operators have with risk management is the immediacy of the operating environment. Operators deal with day-to-day quality, time and cost-performance issues. Risk assessment presents a challenge because it is a forward-looking activity focused on a time horizon that often extends well beyond the day-to-day routine of the operating environment.

Buy-in is obtained from operating managers first through senior management support. In addition, operating managers need convincing evidence the ERM solution will assist them in managing their operating units and divisions more effectively. Following are suggestions for achieving ownership and commitment from operators:

- ***Obtain stakeholder involvement and commitment***: Identify key leaders throughout the organization and gain their support for ERM implementation. An effective change process transitions key stakeholders along a continuum from awareness to buy-in and ultimately to ownership.
- ***Establish accountability for results***: An understanding of the people and accountability issues is one of the most vital steps of the change process. A goal of ERM is to incorporate risk management into the daily agenda and decision-making processes of the organization. This means that ultimately, every manager is responsible. This can only happen if goals are clearly articulated, and the appropriate individuals are held accountable for results.
- ***Enable change by focusing on the "human side"***: Too often, the change focus is limited to technical matters such as policies and limits, processes, measures, reports, systems and data, all of which define the infrastructure for a risk response. While important, these are not the only objects of change. A common language, effective communications, risk awareness and effective knowledge sharing are also important.
- ***Support the implementation process***: The journey towards ERM requires a systematic approach using sound project management techniques and discipline. The implementation process must be supported with dedicated resources, appropriate standards, best practices, measures and feedback mechanisms. The use of piloting as well as clear communications regarding the purpose and authority of implementation teams are vital to empowering key personnel to do what they need to do to be successful.
- ***Align organizational, process and individual performance measures***: The firm's reward systems and incentive plans should be aligned with the change process through appropriate performance metrics.
- ***Align the change process with the firm's culture***: ERM cannot be seen as an independent initiative but must become an integral part of existing business processes – "the way we do things around here." Management must build on current practices that support the risk management vision and develop new or improved procedures, tools and techniques that will be accepted within the organization. By integrating these procedures, tools and techniques into already established processes, management achieves a "quiet splash" rather than implementing "another program."

The above change enablement practices, as well as the practices outlined in Question 90, are summarized in the following chart, along with the consequences if they aren't executed competently. If executed, they lead to sustainable change. If not, nothing happens.

CHANGE ENABLEMENT PRIORITY →	CONSEQUENCE IF UNADDRESSED
Top management commitment and support	No leadership or role models
Compelling business case for change	No action
Clear shared vision	No direction or focus
Realistic goals	No credibility or impact
Well-defined action plan for change	No roadmap
Stakeholder involvement and support	No commitment or momentum
Accountability for results	No ownership
Manage the "human side" and effective communications	No endorsement of change or consistency in execution
Process view of implementing change	No systematic approach
Align performance measures	No achievement of objectives or realization of benefits
Align process with the culture	No success



92. Can we leverage existing infrastructure so that we don't create more overhead?

If the ERM infrastructure is not based on existing management structures and processes, it will likely be viewed as an appendage. By integrating ERM into processes that are already in place, the cost of additional overhead is reduced. For example, management can build ERM infrastructure into the strategic management process, the business-planning process, the Six Sigma process (or other quality initiatives), the organization's performance measurement (e.g., the "balanced scorecard") and/or the compliance process. Furthermore, management should take into consideration existing initiatives to improve risk management. ERM should not be implemented in a vacuum.

93. What types of skills are needed to implement ERM?

It depends on the nature of the capabilities needed to close significant gaps and define the desired ERM infrastructure. There is no one-size-fits-all. The necessary skills are dependent on the policies, processes, measures, methodologies and systems capabilities management decides the organization requires. That is why an enterprise risk assessment identifying the priority risks and a gap analysis around the capabilities for managing the priority risks are so important.

94. Do we need to put a name on an ERM initiative, i.e., isn't ERM just good business practice with another name?

ERM is definitely good business practice and organizations can call it whatever they want. In fact, there is no requirement or need to call the organization's improvements and initiatives to implement ERM by that name. Some organizations integrate procedures, tools and techniques into already established processes, and don't label the effort with a name. Their focus is on improving "what we already do."

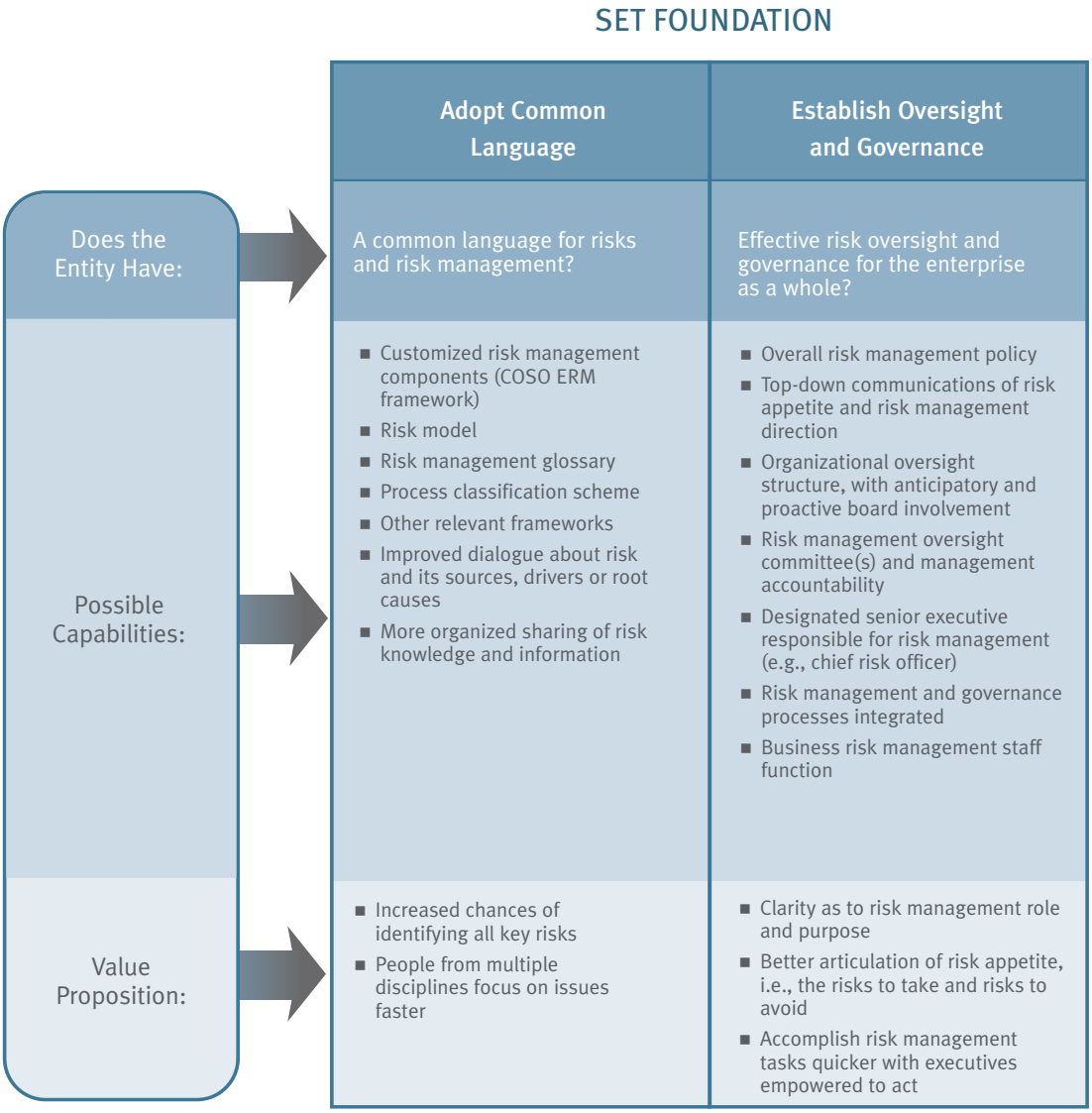
95. Do companies typically add full-time personnel to successfully develop and roll out an ERM process and system, or do they ordinarily use existing personnel who devote their efforts to this initiative on a part- or full-time basis?

They do both, with emphasis on the latter. Again, it depends on what the company decides to implement. An enterprise risk assessment identifying the priority risks and a gap analysis around the capabilities for managing the priority risks provide insights to the answers to this question.

96. What steps does management take to set the foundation?

For companies getting started, setting the foundation is key. There are two groups of capabilities to consider when setting the foundation – ***adopt a common language*** and ***establish oversight and governance.*** These capabilities are not a linear progression. They may be addressed concurrently, with choices with respect to one exerting influence on choices affecting the other. Further, not all possible foundation capabilities need be selected when designing an ERM solution. Management need only select sufficient capabilities to provide a common language and establish oversight and governance related to risk management. Once the foundation is set, management builds the components of the ERM process.

Following is a summary of examples of possible elements to consider when setting the foundation:



The previous examples are intended to be illustrative and are not all-inclusive.

97. How does management decide on the appropriate foundation capabilities?

With respect to adopting a common language, it is a matter of judgment, culture and operating style. The structure and complexity of the organization are additional factors. What works for one organization will not necessarily work for others. A good technique is to pilot a suggested framework or alternative frameworks to test application in practice and gauge acceptance before committing to using them across the organization.

With respect to establishing oversight and governance, we recommend that management carefully consider all of the "possible capabilities" summarized in the response to Question 96. The organization's structure and extent of centralization versus decentralization impact the oversight structure management puts in place.

98. Why have a common language and are there examples?

Communication is essential. The lack of a common perspective or language inhibits communication and the sharing of best practices, and therefore impairs effective risk management. Moreover, without a common language supporting a uniform process, everyone starts with a "blank sheet of paper" every time they confront the subject of risk and risk management. Therefore, a common language is a tool for facilitating an ongoing dialogue among the firm's managers and employees about risk and the capabilities in place to manage risk. Essential elements of a common language include:

- Clarifying terminology that assists the organization with the identification of risks and provides a basis for ongoing discussion and analysis
- A process classification scheme that decomposes the business into its operating, management and support components to facilitate the sourcing of risk and sharing of best practices
- Effective frameworks that simplify communications about risk management capabilities, enable fact-based evaluations of process capability and focus improvement efforts to address significant gaps

See our response to Question 75 for an example of a risk language. See our responses to Questions 110 and 111 for examples of proven frameworks for evaluating process capability.

99. Are there examples of a process classification scheme?

A process classification scheme is a summary of an organization's processes and is a useful tool when assessing the source of risks. These process categories are further broken down into sub-processes that can be applied or customized to any business or industry. The point is that the organization must devise its own framework for organizing its process classification scheme to supplement its risk language and populate that framework over time.

There are many examples of a process classification scheme. The Porter model is one approach companies have used. Protiviti has its own process classification scheme customized to different industries. There are other similar frameworks available to decompose a business into its operating, management and support processes.

100. How is dialogue about risk and its root causes, drivers and sources improved?

When sourcing risk, the company focuses on understanding the underlying causes, or "drivers," of the risk. Risk sourcing requires an effective analysis of the external environment and the firm's internal processes and conditions. While event identification focuses on what events can possibly happen in the future, risk assessment is the evaluation of the likelihood of the event occurring and the severity of impact if the event occurs. Events giving rise to potential risks can happen either outside the organization or within its business processes. Therefore, management needs to understand the *why*, *how* and *where* regarding the related events to formulate an effective risk response. That is the objective of risk sourcing.

Risk sourcing is the process of understanding a risk and its interrelationships with other risks as well its drivers or root causes, which are the ultimate sources of uncertainty. Determining the type and nature of the significant drivers is often a critical step towards the development of a risk measurement methodology. For example, if a manufacturer is concerned about the amount of time required to bring a completed product to market, then the company's management would need to understand a number of business processes. In particular, they need to look for unnecessary or redundant activities that clearly do not add value to the process in achieving the "speed to market" objective. This exercise could even entail looking upstream to the firm's suppliers' processes as well as downstream to its distribution channels. Organizational boundaries can blur when sourcing risk.

A common language and approach can assist management in determining the root causes or drivers of multiple risks and provide a foundation for measuring, controlling and monitoring risk. The frameworks supporting risk sourcing (such as the one illustrated in our response to Question 80) help risk managers understand the type and availability of relevant risk data that will influence (a) how risk can be measured, and (b) the selection of an appropriate risk response. Approached on a systematic basis through analyzing risk drivers and business processes, risk sourcing also can identify risky situations that managers may decide to fix immediately with appropriate internal controls.

Root causes or sources of risk stem from a variety of factors, including:

- Changes in one or more external environment factors
- Anomalies or deficiencies in one or more business processes or systems
- Poor management of interfaces between processes and activities
- Inadvertent or deliberate errors
- Breakdowns in the flow of information supporting a process (the "flow of information" is the sequence of activities that capture and record business data, process that data into information and ultimately report information and knowledge to management and outsiders)
- Facilities or equipment that malfunction or are not suited for the job they are put in place to accomplish
- Internally driven events that result from management actions or inactions, e.g., poor communications, lack of leadership, inappropriate performance expectations and incentives, etc.

External environment risks are sourced using such analytical techniques as industry analysis, competitor analysis, market analysis, country analysis, benchmarking and the analysis of other relevant external data. For process risks, process and risk owners should understand the processes first (through process mapping, for example), then source the root causes of risk. For all risks – environment, process and information for decision-making – risk driver analyses are useful for sourcing purposes. When analyzing root causes or drivers, it may be necessary to understand the portfolio effects of multiple risks that are beyond intuitive guesswork because of the complex interrelationships between risks and the factors affecting them, e.g. instrument terms, environment risk drivers and other variables.

101. How is knowledge sharing about risk management improved?

To communicate effectively up and down the enterprise and across its units, functions and departments, managers and employees need a common language. As with anything else heavily dependent on effective communication, the absence of a language leads to miscommunication and oversights. If the appropriate people are effectively communicating information about risks (and opportunities) and coordinating risk management activities, the organization will be better positioned to learn and adapt to a changing environment.

A common language adds value in that it can help business unit or process managers to more effectively identify and assess their exposures to potentially adverse events and design improved risk management capabilities. However, its real value becomes evident when it is deployed within a uniform risk management

process that is applied to different risks across the enterprise. Only then will the breakthrough benefits be realized: prioritization, sourcing, quantification, aggregation, learning, knowledge-sharing and timely risk response development. A common language is not only essential to the implementation of ERM; it is also a vital first step in the journey to that capability.

Common frameworks translate into powerful knowledge-sharing tools that can drive continuous improvement. For example:

- The Internet, proprietary intranet applications and electronic mail systems create opportunities to poll risk owners and their teams regarding the likelihood and impact of key events and to share knowledge and experience. For example, intranets can serve as the means of providing uniform risk assessment tools for business unit managers. The combination of a common language and common process enable the development of technology-based risk aggregation techniques.

- If each business unit maintains its own database of risk and risk management information, a common language enables aggregation of common data points to develop an enterprisewide perspective for managing priority risks. This approach enables a corporate business risk management function to access the data of all group companies and accelerate the knowledge sharing process. Direct knowledge sharing and/or Q&A among group companies is also possible and is supported by the "open" discussion platform features of the database.

- Top-down communication is an integral part of four-way communication. All stakeholders in the organization's risk management process, e.g., the board, senior management, risk management owners and business process owners, must be able to freely communicate about business risk issues. Executive management's top-down communications emphasize strategic direction ("Where are we going?"), overall organization performance ("How are we doing?"), employees' risk management responsibilities ("What's expected of you?") and the purpose of risk management. Top-down communications include formal and informal processes. They work best in an environment supported by a framework that includes a common risk language.

- Upward communication is also important and is much more than "whistleblowing." Management should provide employees with a process for communicating information upward regarding what is happening in the external environment and internally within the business. The common language provides a context for this communication, which is vital because without it, senior management of large organizations can lose touch with reality.

- Horizontal communication across operating units and divisions, functions and departments is also critical to more organized sharing of "best practices" information and continuous improvement.

102. What does it mean to increase an organization's awareness of or sensitivity to risk?

An effective risk management oversight function, as articulated in Question 56, coupled with a well-defined uniform enterprisewide risk assessment process will help create a risk-sensitive and risk-aware culture, one where risk is embraced in an open, positive and proactive manner at all levels of the organization. ERM is as much about the right culture as it is about policies, processes, people and systems. It is a framework that managers can use to embrace risk, not run from it. But some ask, "What does it mean to have in place a 'risk-sensitive and risk-aware culture'?"

A risk-sensitive and risk-aware culture is one in which risk management is effectively integrated with strategy-setting. In this environment, roles and responsibilities relating to risk management are clearly articulated at all levels of the organization so that managers are encouraged to portray realistically the potential outcomes of prospective transactions, deals, investments and projects. They are expected to understand and portray the full picture. For example, they must look at the downside and the upside relative to taking advantage of an opportunity. How bad would it hurt if things don't go as planned and does the potential upside opportunity adequately compensate the organization for taking on the downside risk?

Most business managers understand the fundamental principle here. However, as the "risk as threat" view is so predominant in many organizations in many industries, putting the principle into practice in a careful and balanced way is difficult. For example, say you have a business unit that's trying to consummate a major transaction or is under significant earnings or budgetary pressure, or is trying to make a lot of money in a very short period of time. Capital is available, competition is stiff and entrepreneurial "can do" optimism abounds in the hallways and meeting rooms of the organization. This profile of managers can very quickly become enamored with an opportunity. They can start ignoring the downside risk and just focus on the upside opportunity. Then, all of a sudden, without the appropriate oversight controls (including appropriate risk limits, reporting and monitoring) and without a robust enterprise risk assessment process, the organization ends up "owning" the risk resulting from pursuing that opportunity. If the risk/reward profile is not properly weighted, the enterprise may not be appropriately compensating itself for the risk it is undertaking. That can get managers, not to mention their organizations, into trouble.

So when new market, business and product opportunities arise, the organization needs the capability to articulate and assess the key events associated with opportunity-seeking behavior. How bad can it get? How good can it get? Where can we end up between these two extremes, including the most likely outcome? THIS is the kind of robust analytical process that management needs BEFORE committing capital to the pursuit of new opportunities. In essence, management must evaluate the potential downside and upside against the entity's risk appetite.

A risk-sensitive and risk-aware culture is one in which ALL key personnel in the organization – or at a minimum some independent individual or group or unit – have the opportunity to speak their mind about something that the enterprise is attempting to do. If people don't feel able to freely articulate what they really think about a particular transaction, an acquisition, a new product, a proposed project or other opportunities, they're not going to say it. Then the organization has lost the benefit of getting those points of view out on the table and openly discussing them with the senior executives and directors of the organization. The dialogue focuses unduly on upside opportunity without appropriate consideration of the related downside risk.

The irony about creating an open environment is that a robust dialogue can lead the organization to taking more risk, not less. The real question is, "Does the organization really know what it is getting into?" And just as importantly, what might it be missing if it doesn't act? If an enterprise has a product group that's trying to push forward an idea, management needs the fully balanced view that is so vital to making an informed decision. No one is going to stand up and say, "I don't think this acquisition, deal or transaction makes any sense because we're paying about twice as much as we should," unless they are structurally insulated from any repercussions that that statement could have on their compensation and career.

In summary, a risk-sensitive and risk-aware culture is one that enables people to speak up and then be listened to by decision-makers. It follows word with deed – by insulating people from retribution, direct or indirect. It is not to be confused with whistleblowing, which deals with a different issue. Most executives would agree that there are many good ideas with respect to undertaking risk and opportunity. While some filters are needed, getting those ideas out on the table and discussed in a positive and proactive environment is what a risk-sensitive and risk-aware culture is all about.

TAKING A PROCESS VIEW – BUILDING CAPABILITIES

103. What steps does management take to build risk management capabilities?

Once the organization has set the foundation with elements of a suitable ERM infrastructure (see Question 96), it is ready to advance its capabilities around managing its priority risks. There are three steps management should take when building risk management capabilities:

- The first step, ***assess risk and develop responses***, is addressed after the appropriate foundation is in place. It includes an enterprisewide risk assessment process, a process around planning responses to priority risks and the development of focused risk policies.

- The second step – ***design and implement capabilities*** – makes it all happen. Risk management capabilities include the processes, competencies, reports, methodologies and technologies (systems and data) needed to implement a selected risk response and carry out risk policies consistently across the enterprise.
- The third step – ***continuously improve capabilities*** – relates to continuous improvement, a discipline which applies to risk management as it does to any other business process. The need for improvements to processes, competencies, reports, methodologies and systems that are identified through monitoring should be evaluated and implemented, consistent with a continuous improvement mindset.

As with setting the foundation, not all elements suggested in this publication for building risk management capabilities need be selected when designing a solution for each of the organization's priority risks. Management need only select sufficient capabilities for each risk or group of related risks to meet the entity's stated objectives. Once the desired capabilities are in place, management can then implement appropriate enhancements.

Following is a summary of examples of elements to consider for each of the three steps for building risk management capabilities:

BUILD CAPABILITIES

	Assess Risk and Develop Risk Response	Design and Implement Capabilities	Continuously Improve Capabilities
Does the Entity Have:	A uniform process for assessing business risks and developing risk responses?	A framework for evaluating the appropriate components of infrastructure when designing and implementing risk management capabilities?	A framework for continuously assessing risk management capabilities and improving risk policies, processes and measures?
Possible Capabilities:	■ Robust enterprisewide risk assessments that increase understanding of priority risks ■ Initial risk identification and prioritization (risk maps) ■ Sourcing of drivers for selected risks (process maps and key drivers maps) ■ Initial quantification of selected risks ■ Examples of COSO ERM framework components applied to priority risks ■ Clearly articulated risk responses for priority risks, including policies for individual risks and groups of related risks ■ Risk responses for managing specific risks that consider appropriate options ■ Pilot test results of risk assessment and risk response planning processes at specific units ■ Increased risk sensitivity and awareness	■ Better understanding and documentation of current state of capabilities for managing priority risks ■ Selection of desired risk management capabilities to execute selected risk response and policies for priority risks ■ Gap analysis comparing current and desired risk management capabilities` ■ Business processes that execute defined policies, including documented risk responses, control activities, specific monitoring and oversight activities ■ Designated risk owners responsible and accountable for deciding, designing and monitoring risk responses ■ Management reports providing information for decision-making ■ Methodologies for making management reports more robust ■ Reliable systems and data	■ Updated assessments of desired capabilities as conditions change ■ Closure of gaps between current and desired capabilities through staged improvements over time ■ Periodic benchmarking of risk management capabilities ■ Risk management integrated with core operating processes ■ Focused risk sharing and control activities ■ Low value, redundant internal controls eliminated ■ Four-way interactive knowledge sharing and communications of risk management information ■ Continuous employee learning
Value Proposition:	■ Unacceptable surprises prevented through better risk identification and sourcing ■ Risks to achievement of KPI's are understood, including the benefits of addressing them and the consequences of not	■ Improved oversight, monitoring, compliance and reporting ■ Reduced uncertainty through improved information for decision-making ■ More efficient and effective approach to improving risk management capabilities over time	■ Risk management performance matches desired capability for specific risks ■ Improved organizational learning capabilities through knowledge sharing activities ■ Successful implementations with less disruption to organization

The above examples are intended to be illustrative and are not all-inclusive.

104. How does management decide on the appropriate risk management capabilities?

With respect to designing and implementing risk management capabilities, it is a matter of judgment, culture and operating style. What works for one organization will not necessarily work for another organization. Management can pilot components of a suggested process for a given risk or at a given unit to test application and acceptance before deciding to deploy them across the organization.

105. How does management improve the organization's risk assessments?

Risk assessments can be improved in many ways. The most effective risk assessments are designed to provide quality inputs to risk response planning. Management's leadership and commitment to an assessment process are essential for directing the necessary resources to support the process. Improving monitoring and measurement efforts increases the probability that the assessment will be based on relevant quantitative information as well as qualitative information. Other possible improvements include: providing resources for identifying, assessing and managing risks; assigning appropriate risk owners to assume responsibility for priority risks; integrating risk management objectives into individual performance expectations and business plans; and creating an open environment which encourages discussion of common risks across the enterprise.

106. How are objective-setting, event identification and risk assessment related?

"Objective-setting" occurs when management sets strategic objectives, which provide a context for establishing operational, reporting and compliance objectives. Objectives are aligned with the entity's risk appetite, which drives risk tolerance levels for the entity, and are a precondition to event identification, risk assessment and risk response. Future potential events are identified with specific objectives in mind.

Event identification occurs when management identifies potential events that may positively or negatively affect an entity's ability to implement its strategy and achieve its objectives. Potentially negative events represent scenarios that provide a context for assessing risk and the effectiveness of risk responses. Potentially positive events represent opportunities. According to COSO, management channels opportunities back into the strategy and objective-setting processes.

Risk assessment occurs when management considers qualitative and quantitative methods to evaluate the likelihood and impact of potential events, individually or by theme or category, which might affect the achievement of objectives. Therefore, to be effective, risk assessment requires predetermined objectives and a thoughtful inventory of possible future events.

107. How important is risk assessment to the ERM effort?

An effective enterprisewide risk assessment process is needed to identify priority risks and to initiate a gap analysis around the capabilities in place for managing those risks. Unacceptable gaps relating to priority risks provide a basis for articulating the value proposition of advancing an organization's ERM infrastructure. An effective risk assessment also provides quality inputs into risk response planning. Thus risk assessment is vitally important to building risk management capabilities and to the implementation of ERM. If the priority risks are not identified, it is almost impossible to define a specific value proposition that will resonate with senior management. In addition, risks change as market and operating conditions change. Each organization, therefore, needs a process to stay abreast of the effects of change on its customers, suppliers, competitors and operations. That is what the risk assessment process is about. Reference is made to Questions 69 through 84, which address the risk assessment process.

108. What alternative risk responses are available to manage risk?

Following risk assessment, specific risk responses are developed. As indicated by COSO, there are four fundamental choices. They are *avoid* (eliminate the risk by preventing exposure to future possible events from

occurring), *accept* (maintain the risk at its current level), *reduce* (implement policies and procedures to lower the risk to an acceptable level) and *share* (shift the risk to a financially capable, independent counterparty):

AVOID

- **DIVEST** by exiting a market or geographic area, or by selling, liquidating or spinning off a product group or business
- **PROHIBIT** unacceptably high risk activities, transactions, financial losses and asset exposures through appropriate corporate policies, limit structures and standards
- **STOP** specific activities by redefining objectives, refocusing strategies and policies, or redirecting resources
- **TARGET** business development and market expansion to avoid pursuit of "off-strategy" opportunities
- **SCREEN** alternative capital projects and investments to avoid low-return, off-strategy and unacceptably high-risk initiatives
- **ELIMINATE** at the source by designing and implementing internal preventive processes

ACCEPT

- **RETAIN** risk at its present level, taking no further action
- **REPRICE** products and services by including an explicit premium in the pricing, market conditions permitting, to compensate for risk undertaken
- **SELF INSURE** risk through:
  - Internal charges to P&L (pay as you go)
  - Borrowed funds from external sources, should a specific event occur
  - Reserving losses (under accepted accounting principles)
  - Using a pure captive insurance company
  - Participation in a group or an industry captive
- **OFFSET** risk against others within a well-defined pool

REDUCE

- **DISPERSE** financial, physical or information assets geographically to reduce risk of unacceptable catastrophic losses
- **CONTROL** risk through internal processes or actions that reduce the likelihood of undesirable events occurring to an acceptable level (as defined by management's risk tolerance)
- **RESPOND** to well-defined contingencies by documenting an effective plan and empowering appropriate personnel to make decisions; periodically test and, if necessary, execute the plan
- **DIMINISH** the magnitude of the activity that drives the risk
- **ISOLATE** differentiating characteristics of proprietary assets to reduce risk of loss through imitation, obsolescence or other competitive pressures
- **TEST** strategies, products or services on a limited basis to evaluate results under conditions that will not influence perceptions of the broader market
- **IMPROVE** capabilities to manage a desired exposure
- **RELOCATE** operations in order to transfer risk from one location, in which it cannot be well-managed, to another location in which it can
- **REDESIGN** the company's business model, i.e., its unique combination of assets and technologies for creating enterprise value
- **DIVERSIFY** financial, physical, customer, employee/supplier and organizational asset holdings used by the firm's business model

SHARE

- **INSURE** through a cost-effective contract with an independent, financially capable party under a well-defined risk strategy
- **REINSURE** to reduce portfolio exposure through contracts with other insurers, when such arrangements are available
- **HEDGE** risk by entering into the capital markets, making feasible changes in operations or executing new borrowings
- **SECURITIZE** risk by accessing the capital markets and structuring deals with potential investors through efficient pricing mechanisms
- **TRANSFER** risk and rewards of investing in new markets and products by entering into alliances or joint ventures
- **OUTSOURCE** non-core processes (a viable risk transfer option only when risk is contractually transferred)
- **INDEMNIFY** risk by entering into contractual risk-sharing arrangements with independent financially capable parties

While the risk responses summarized on the previous page are, for the most part, straightforward, some clarifying comments are appropriate:

- The organization first decides whether to assume or reject a risk based on an assessment of whether the risk is desirable or undesirable. A desirable risk has at least two characteristics. First, it is one that is inherent in the entity's business model or normal future operations. Second, the company can effectively measure and manage it. For example, if reliable measures are not available within a reasonable time frame with respect to a significant risk, then management needs to seriously consider whether the activity driving the risk should be undertaken. Inability to measure a risk doesn't make it go away. If a risk is undesirable, e.g., it is off-strategy, offers unattractive rewards or the enterprise doesn't have the capability to measure or manage it, then the risk is rejected and the ***avoid*** and ***share*** responses are appropriate. Note that management's risk appetite has a bearing on differentiating desirable and undesirable risks.

- If an entity assumes a risk (i.e., it chooses not to ***avoid*** it), several responses are available. First, it can ***accept*** the risk at its present level. Second, it can ***reduce*** the severity of the risk and/or its likelihood of occurrence. Control activities reduce the likelihood of occurrence. Geographic dispersion of assets reduces the impact of the occurrence of a single event on the company. Third, it can ***share*** the risk with a financially capable, independent party.

- The four responses – ***avoid, accept, reduce*** and ***share*** – address actions that are often applied to individual risks. These options are also applied to groups of related risks consisting of natural families or pools of risks sharing fundamental characteristics (e.g., common drivers, positive or negative correlations, etc.) consistent with a portfolio view.

- As illustrated in the summary of alternative risk responses, ***accept*** can mean much more than merely retaining a risk. Following are illustrations:

  - ***Incurring internal charges to P&L***. This approach provides for losses on a "pay as you go" basis. It is often used to address losses that arise in the normal course of business.
  - ***Creating contingent sources of borrowed funds (from external sources should a risk event occur)***. Losses can be funded through proceeds from external sources when working capital is not sufficient. For example, available revolving credit sources can be used for this purpose. Insurance companies offer such instruments as contingent-surplus notes and catastrophe bonds to fund liabilities arising from a catastrophic event. The issue, of course, with this alternative is whether the funding will be available when and if it is needed. Furthermore, the company remains obligated to repay.
  - ***Reserving losses under generally accepted accounting principles.*** A company can accrue a reserve for a reasonably estimable loss when it is probable that a liability or an asset impairment has been incurred, even though the claims giving rise to the losses may either be unreported or still subject to final determination.
  - ***Setting up a pure captive insurance company.*** This self-insurance vehicle is a wholly owned subsidiary established to underwrite the risks of its parent through prefunded reserves. In essence, it provides a more formalized approach to self-insuring risk, one that offers the attractive advantage of tax deductibility in certain countries. Used effectively, captives provide a disciplined approach to capital allocation.

    When is this option chosen over other self-insure approaches? Based on expected loss levels, management should use a discounted after-tax cost analysis to compare the organization's cash flow and earnings when self insuring the risk versus prefunding reserves through a captive. This analysis should consider such factors as the time value of money, opportunity costs and the value of deductions for premiums paid and the view of tax authorities on the deductibility of premiums paid in each country. Other important factors to consider include regulatory funding requirements, the attainability of tax benefits, the effect of the captive in consolidated financial statements and the extent of captive administration, internal operating and other costs incurred.
  - ***Participating in an associate captive.*** This structure includes group and industry "special purpose" captives that underwrite the risks of several independent firms and their affiliates. A captive of this

nature is structured so that it is not controlled by any of its clients. Therefore, as an unrelated party, its long-term viability is dependent on the loss experience of the group.

When analyzing this option, the factors listed above for wholly owned captives should be considered. When considering an unrelated captive, however, there is increased pressure for capital adequacy stemming not only from regulators but also from captive boards seeking the best possible returns on capital. Regulation continues to move towards risk-based capital in which the captive's net exposure per policy and/or per class of business is analyzed and an assessment of the likelihood of loss per policy and/or per class is made. The result is a potentially costly long-term requirement for capital that can be well in excess of current statutory solvency margins.

This upward pressure on capital requirements could threaten the viability of captives unless they diversify their portfolio of coverages and/or transfer risk through reinsurance. Capital requirements may also be managed by closely coordinating the "tiers" of risk financing, starting with the first loss coverage by the captive, then adding the aggregate deductible borne by the insured, then exposing the captives' equity capital in full and, finally, transferring the remaining risk through reinsurance. In this way, captives provide a gateway for companies to contract with the major reinsurance markets and, for many organizations interested in gaining access to coverages that are difficult to place in the insurance markets, are an essential piece of the total risk management fabric.

- Another ***accept*** tactic is to offset a risk against other risks within a well-defined pool. For instance, a refining company is in the position of both purchasing energy products as raw material inputs and selling refined products as outputs. The costs of these inputs and outputs provide a natural offset because increases in the cost of a company's raw material purchases may be passed through to customers by means of higher product prices. Another example is that of an investment bank writing a financial contract for one client hedging against the risk of higher interest rates, and purchasing a similar contract from another client who is hedging against the risk of lower interest rates. In this case, the exposures generated by each risk offset each other in the investment bank's book.

- Formulating a risk response is not necessarily a matter of selecting one option over another. The best response may be a combination of options. For example, when managing workplace safety, an organization may wish to implement appropriate control activities to ***reduce*** health and safety risk within its business processes as much as possible, obtain adequate workers compensation insurance to ***share*** a portion of the residual risk and ***accept*** the remaining residual risk through deductibles.

- Some believe that risk may be exploited through a proactive and conscious decision to take on new risks or increase existing risks as the enterprise makes bets in the pursuit of value-added opportunities. For example, management decides to take the risks inherent in its choices to enter new markets, introduce new products, merge with or acquire another firm or exploit other market opportunities, all of which result in shaping the organization's risk profile differently, even to the point of increasing the firm's exposure to risks it desires to take in accordance with its business model. While in concept it did not disagree with this thinking, COSO concluded that such actions constitute the pursuit of opportunities (see Question 73). Thus the decision by management to take on or increase the organization's risks is a management decision, not necessarily the application of ERM. For example, some argue that management can ***exploit*** risk by exercising its prerogative to:

  - Diversify financial, physical, customer, employee/supplier and organizational asset holdings used by the enterprise's business model.
  - Expand the business portfolio by investing in new industries, geographic areas and/or customer groups.
  - Create new value-adding products, services and channels.
  - Redesign the firm's business model, i.e., its unique combination of assets and technologies for creating value.
  - Reorganize processes through restructuring, vertical integration, outsourcing, re-engineering and relocation.
  - Allocate capital internally within the entity using disciplined methods to finance risks undertaken and direct entity resources to those opportunities with the highest prospect for generating desired returns.

- Price products and services to influence customer choice toward those products and services that suit the enterprise's risk profile.
- Renegotiate existing contractual agreements to reshape the risk profile, i.e., transfer, reduce or take risk differently.
- Arbitrage price discrepancies by purchasing securities or other assets in one market for immediate resale in another.
- Influence regulators, public opinion, law makers and standards setters through focused lobbying, political activism, public relations, etc.

Under the COSO ERM framework, many of the above tactics are examples of exploiting opportunities.

- Applied in strategy-setting, ERM provides the focus that instills the discipline to drive companies to understand their core competencies well so they can align their risk taking with their processes, skills, technology and knowledge. The four responses – ***avoid***, ***accept***, ***reduce*** and ***share*** – reflect choices by management to act. What if management chooses not to respond? ***Defer*** is another management choice in circumstances when an exposure may have more value in the future than it does today, depending on how the future unfolds. For instance, many research and development projects do not become profitable products. Those that do may become profitable enough to more than offset the cost of the entire R&D program. Since management may not always be able to distinguish successful projects from unsuccessful projects, it may prefer to maintain all the potentially good exposures because of their option value – that value being the chance they may become profitable in the future. Such evaluations are possible in many business situations. The value of deferring a decision to respond – or preserving the option to make a decision to respond in the future – arises from recognizing the facts as they are, but not over-committing when it is not necessary to do so.

- An exposure to an event may be desirable, but uncertainty over its timing may be unacceptable to management. Thus while management may choose to accept a risk, actions may be taken to alter the timing characteristics of the risk. For instance, an entity may anticipate that interest rates will rise (or fall) in the near future, and so may decide to accelerate (or delay) its borrowing activities. Or an asset management company may seek to structure the timing of withdrawals from various funds so that it can best manage its assets without maintaining an unnecessarily large (and costly) cash position. Many such changes in the timing of a business decision or other business activities are possible.

109. What factors must management consider when evaluating alternative risk responses?

Management must make *informed* choices on where to make bets, where to hedge bets and where to avoid betting altogether. There are many factors to consider when evaluating alternative risk responses. For example, management's business decisions and assumptions provide a context for evaluating alternative risk responses. Following are examples:

- ***Management's objectives and strategies***: These objectives and strategies clarify the what, where, when, who and how regarding the enterprise's business model. They are expressed in terms of short-term tactics, medium-term strategies and long-term business objectives, and incorporate short-, medium- and long-term constraints. Risk responses must be tailored to the specific business objectives and strategies they support.

- ***Risk and reward trade-offs***: These trade-offs are inherent in any choice with respect to managing risk, not only operationally for any company, but also from a market perspective for a public company. In other words, why are investors buying stock in the company? Are they in effect taking on the business risk to which the company is exposed? Thus investors' expectations of returns potentially affect management's objectives and strategies driving risk responses.

- ***Risk management capabilities***: Risk responses are only as effective as the entity's capabilities to execute them. If the capabilities to execute are not in place, can management assemble them on a timely basis for deployment within management's chosen planning horizon (see the following)?

- ***Time horizon***: The time horizon is the period of time which management has decided to consider when assessing risk and risk management capabilities. An event that could possibly occur over the short term confronts the entity immediately. For example, an increase in the cost of raw material or energy purchases, a competitor price reduction or an increase in interest rates can occur over the short term. Exposure to events that can occur over the long term, by contrast, represent issues over which an organization has relatively little ability to address over the short term, but can realistically expect to manage over the longer term. For example, loss of reputation due to a systemic breakdown in product quality or a competitor's introduction of a superior manufacturing process resulting in significantly lower production costs can occur over the longer term. If these so-called longer-term issues occur unexpectedly over the near term, the entity could face a crisis situation. Johnson & Johnson's world-class reaction to the Tylenol crisis distinguished the company in the marketplace. By contrast, Perrier's handling of its water contamination crisis cost the company market share and it ultimately was acquired. The key point is that any mismatch between the duration of the exposure and the length of time that management needs to implement a risk response presents a potentially critical risk to the enterprise. Risk responses should take these mismatches into account.

- ***Financing***: Risk responses should also consider the need for risk financing, which is the means by which an organization pays for the outcomes of an unfavorable event through management's choices to share or accept risk. Following are several observations about risk financing:

  - External financing results from the decision to share risk with an independent, financially capable counterparty through insurance, hedging or other forms of contracting.
  - Internal financing of risk is accomplished through the entity's own financial resources, e.g., various forms of self-insurance, insurance deductibles and accounting reserves.
  - Many risks are internally financed, but not all are explicitly recognized. An entity retains all of its risks unless it does something about them. Unless risks are considered too insignificant to warrant further analysis, unplanned retention of risk is not "risk management."
  - If insurance that protects the enterprise from catastrophic events is inexpensive relative to the potential loss, planned retention needs to be based on rational common sense. Who wants to explain to the board that a $50 million loss could have been insured for $10,000?

- ***Residual risk***: Risk responses that eliminate risk are rare. There will always be some residual risk in any risk response. Any differential between the coverage provided by the risk response and the exposure itself provides basis risk; that is, some residual risk remains with the company. COSO recognizes this point by suggesting the extent of this risk should be evaluated. Residual risk arises because management seeks practical solutions that hold risk to tolerable levels and achieve reasonable, not absolute assurance. Often, the tools used to manage a risk, such as when placing a hedge with a futures, swap or options contract, will not fully cover the underlying exposure presented by the risk. Residual risk can occur either because the risk response does not cover all aspects of the exposure to one or more events, or it covers too much. An example of the former is a grain elevator holding grain of different product specifications than that specified in a standard futures contract. An example of the latter is an entity hedging a two-month energy exposure with a three-month options contract. In general, any mismatch between the coverage provided by the risk response and the exposure itself will present new or continued risk.

- ***Inadvertent risk taking***: Related to residual risk is the situation in which management chooses a risk response to manage one risk, but unknowingly creates another risk. A major automobile manufacturer found this out when it purchased a large stake in the metal commodity, palladium, that was a key input to one of its vehicles. The objective was to manage supply risk and make sure it would not run out of this raw material and bring production to standstill. This strategy worked fine until its engineers redesigned the car and eliminated the need for palladium, making the stocks of the commodity on hand virtually useless. This triggered a significant loss. Management should ensure that an enterprisewide view is taken when risk responses are formulated.

- ***Risk manageability***: As executive and unit management direct their efforts toward managing the priority risks, they should differentiate those risks where immediate improvements are more easily obtainable. While not intended as a suggestion to ignore the tough issues, a focus on manageability can lead to early successes in formulating risk responses by reaching for the "low hanging fruit."

Other factors to consider when evaluating alternative risk responses include costs and benefits, the option value of waiting versus acting immediately, the effectiveness in achieving stated goals and the interaction with other contemplated responses, in accordance with the organization's business strategy, that could produce different results than otherwise expected.

When assessing external environment factors and internal risk factors, it is also useful to consider the nature of potential events and the related effect on the organization's risks before formulating a risk response. Following are examples:

- ***Business plan uncertainties***: Uncertainty arises when management does not know in advance the magnitude and direction of change in the value of a key variable, e.g., competitor behavior, interest rates, commodity prices, technological innovation, currency price movements, human performance, regulatory actions, etc. However, potential future changes in key variables create uncertainty for the enterprise only when its sources of value are exposed. Truly understanding the sources of uncertainty relating to each of the firm's exposures (see the next point below) is a vital process that lays the foundation for deciding how to measure and manage risk. It drives such questions as: What are the key variables and assumptions underlying the business plan? Which variables have the greatest impact on the business plan, assuming the extent of change is significantly beyond realistic expectations? Which assumptions underlying the business plan are the most critical to achieving management's objectives? Where are the soft spots in the business plan, e.g., the stretch performance goals where the entity is the most vulnerable to falling short of expectations? Answers to these and other related questions provide quality inputs to risk response planning.

- ***Business plan exposures***: Exposure arises when any asset or source of value (see Question 3) of the enterprise is significantly affected by unexpected changes in key underlying variables resulting from the occurrence of an event. For example, an organization is exposed to risk when a realized change in a key variable within a given time horizon will result in a significant change in one or more of its key performance indicators (KPIs). The greater the potential realized change in performance, either positive or negative, the greater the exposure. A firm may be exposed to performance variation on account of its business model, strategies, processes, brands, customers, employee work force, market positions or other sources of earnings and cash flow. This point is important because strategy-setting often entails taking on risk, and the risk-taking process often creates new or increased exposures. Management should consider whether risk responses are needed for significant exposures identified during the risk assessment and strategy-setting processes.

- ***Performance variability versus loss exposures***: A firm's exposure to future possible events can result in either upside or downside consequences. This is seen in the way both exposures and uncertainties are assessed. For example, assume we list all foreseeable future events or outcomes, including estimates of the net cash flows relating to each possible outcome and their respective probabilities. The results of this exercise depict both upside exposure (opportunities) and downside exposure (risks) when the expected future net cash flows of all foreseeable outcomes include both positive and negative results, giving rise to *performance variability*. In the situation where only negative things can happen (such as when enumerating the potential consequences of a hazard), management would list only downside exposures, i.e., every foreseeable outcome results in a negative net cash flow, creating a loss exposure. The point is this: The nature of the risk can influence the nature of the risk response.

- ***Scenarios***: What event or combination of events can happen in the future and why, how and where can they happen? What is the impact on the business? Effective event identification and risk assessment addresses these questions, providing significant input to the formulation of risk responses. If management thinks through the interrelationships between future possible events during this exercise, the analysis is more robust.

- ***Controllable versus non-controllable exposures***: Most environment risks are beyond the control of management. The impact of these risks on the business must be managed through the organization's strategic response. Business, risk and support units must develop long-term strategies as well as learn to anticipate and adjust opportunistically to changes in the external environment. Internal process risks, by contrast, represent controllable risks. These risks are often addressed through internal policies, processes and controls.

- ***Operational versus contractual exposures***: Every risk response has to be matched with the nature and duration of the risk it addresses. For example, while a fragmented approach of separate functions striving towards functional excellence, and separate business units operating autonomously to achieve focused business plans, may offer short-run contractual protection from certain risks, it is not as cost-effective as long-term strategies that are more operationally focused. For example, some treasurers have hedged foreign exchange exposures associated with overseas sales, enabling operating unit personnel to focus on the core manufacturing business. But hedging may not always be the best answer. The risks arising from day-to-day operations can only be dealt with – over the long term – by solutions of an operational nature. Such solutions include shifting R&D, inventory and labor sourcing to weak currency environments, establishing regional netting centers to "net down" currency risk before hedging and addressing product pricing based upon elasticity studies. That is why the best risk response often arises when a global or regional treasury works closely with operating units to mesh operational and hedging tactics.

  To illustrate further, if a company's foreign exchange arises from a contract with a foreign customer, currency derivatives that align the term of the hedge with that of the contract are effective in safeguarding against adverse movement in exchange rates. By contrast, if the company has ongoing operations in the foreign country, there is no currency hedge whose size, duration and terms exactly match the company's business activities. Therefore, managers must examine the nature and duration of the risk to devise an operational response. Of course, some companies may dispute this example in situations where management is able to conclude that net income from a foreign source is reasonably predictable. When such assertions are credible, those organizations may argue that hedging is effective in such circumstances.

There are other important factors to consider when formulating risk responses. For example:

- ***Compliance issues***: Situations involving compliance matters, such as laws and regulations, authorizations and approvals, hazardous materials handling, shop floor safety and nuclear power plant operations, have one thing in common – rigorous conformance with pre-determined standards is the established norm. These environments and circumstances require appropriate policies and procedures that reduce the likelihood of non-conformance to an acceptable level (as defined by management's risk tolerance).

- ***Pervasive issues***: Is the exposure or uncertainty isolated or does it have multiple effects? Often, companies find certain risks affecting them similarly throughout the organization: regulatory risk, political risk and litigation, for example. The more pervasive the risk, the greater the need for a risk response.

- ***Expected frequency***: Does the exposure to uncertainty arise from infrequent events or from regularly recurring events? One-time events that cannot be anticipated are difficult to measure and virtually impossible to control, but the organization can prepare contingency plans. By contrast, recurring events (e.g., product defects) must be carefully examined and appropriate responses developed, often through process improvements or re-engineering. Events which occur frequently are in substance operational issues management must address rather than risks, because their occurrence is more certain.

- ***Infrastructure issues***: A major source of process risk lies in the interfaces between processes, e.g., the so-called "hand-offs" between functional areas. Interfaces that are not under the control of a process-owner present a significant risk of errors and omissions. Control activities must be designed at or as close as possible to these interface points to reduce process risk to an acceptable level.

- ***Data availability***: Availability of data points is also an issue for many companies for certain types of risk. Some risks have more data points available than others to assist managers in measuring and analyzing

them. Where data is available, the organization can use it in designing a risk response. Examples of these types of risks include on-time product delivery, commodity prices, warranty claims and information technology security access. Where data is not readily available, management must rely on judgment or participate in a broader pool of similar exposures that is susceptible to the underwriting process, e.g., purchase insurance to cover risks related to catastrophic loss exposures. The apparent lack of data does not make the risk go away, and does not mean a risk shouldn't be managed.

While the above summary is not exhaustive, it provides an insight into some of the issues to consider when formulating risk responses.

110. What are the elements of risk management infrastructure, why are they important and how are they considered?

An effective risk management infrastructure provides the capabilities for executing risk responses. There are six elements of risk management infrastructure. These elements are policies, processes, competencies, reports, methodologies and technology (systems and data). Formulating a risk response is an academic exercise if it does not consider these elements of infrastructure. While intended to be more of an iterative than a strictly linear approach, the six elements of infrastructure are often developed one link at a time – each element driven by the previous one. Once in place for a given risk or for a portfolio of related risks, these six elements pave the way for implementing enhanced capabilities.

To explain further:

- ***Business policies***: The formal policy framework includes specific guidelines as well as the more general principles that apply to all aspects of the business and the management of its risks. Policies enable risk owners to understand what the organization intends to accomplish. Policies are the link to strategy; they put a strategy in play.
- ***Processes***: The organization's processes are its primary means of executing its business policies. Risk responses and control activities are desirably integrated within business processes because risks are best managed and controlled as close as possible to the source. Process definitions should precisely describe the sequence of activities and tasks that must be performed to execute the desired risk response.
- ***Competencies***: People with the requisite knowledge, expertise and experience execute the entity's processes. The roles and responsibilities of these process owners must define and delineate risk taking versus risk monitoring functions as well as the interaction and the information and decision flows between related functions. Overall responsibility for implementing improved risk management capabilities should rest with one or more process owners.
- ***Management reports***: The organization's reporting is designed according to the information needs of process owners. Management reports should be actionable, easy to use, linked to well-defined accountabilities and prepared with appropriate frequencies.
- ***Methodologies***: The robustness of management reports is enhanced or constrained by the methodologies supporting them. Effective methodologies help identify and prioritize risk, source risk to their key drivers and quantify risk. They also support analysis of risk/reward trade-offs, portfolio diversification, allocation of capital to absorb potential losses, pricing of products and services to compensate adequately for risks undertaken, and contingency planning given uncertain outcomes.
- ***Systems and data***: Information systems support the modeling and reporting that provide the foundation needed for cutting-edge risk management capabilities. They provide relevant, accurate and on-time information. New technologies are leading to more refined measures and are making it easier to identify and understand risks, risk drivers and the impact they have on the company. Information systems should not only meet the company's current business requirements, they should be flexible for future enhancement, scalability and integration with other systems.

If any one of the aforementioned elements of infrastructure is deficient, the effectiveness of other elements can be significantly diminished. For example, if relevant and reliable data are not available, the value of reports to management is reduced (and may even be misleading). If reports do not provide appropriate information, risk owners cannot execute the processes for which they are accountable. Consequently, the related processes fail to achieve the established policies. The effect, therefore, is cumulative.

The six elements of infrastructure are depicted below:

As noted earlier, the above elements are generally designed from left to right. For example, policies drive the design of processes, the processes dictate the organization of people and skills needed, etc. The use of this structure helps to organize the design of a risk response using a comprehensive and consistent framework. In particular, it ensures that all key elements are appropriately considered. For example, by adequately developing processes and people capabilities first, the common problem of placing undue emphasis on models and systems is avoided. Models and systems, therefore, support processes and people. The positive impact of this thinking is less waste investing in models and systems.

When managers begin to organize and align the organization's infrastructure for managing risk, they send a clear signal that they are serious about risk management. While each individual element of infrastructure is important, equally critical are the interrelationships between the elements. If any one element of infrastructure is deficient, the effectiveness of other elements can be significantly affected.

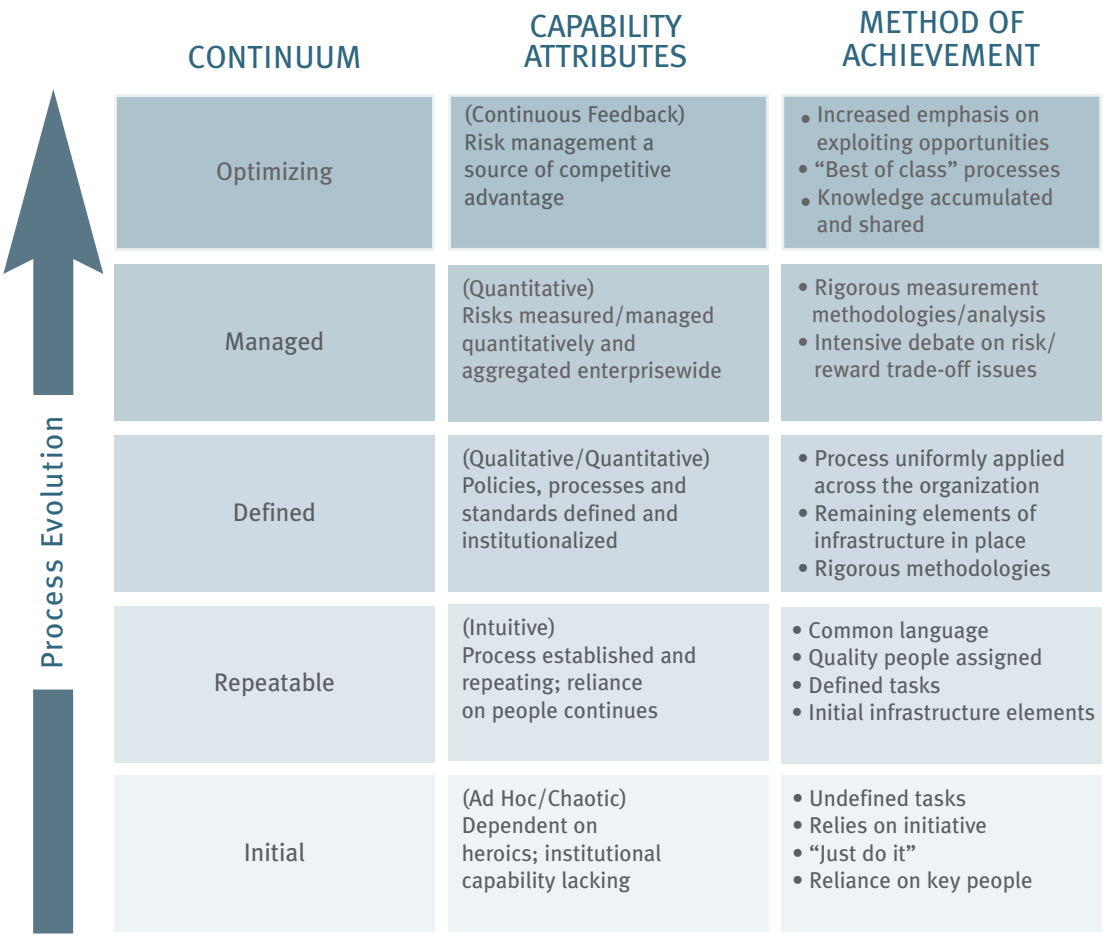
111. Is there a model to help us set our priorities when implementing ERM and monitor our progress as we improve our risk management capabilities?

The capability maturity model is a tool for assisting management in thinking more clearly about such questions as:

- How capable do we want our risk management to be as we improve our policies, processes and measures for each of our priority risks?
- Do we vary the rigor and robustness of our risk responses and related control activities by risk?
- Do we rely on a few well-qualified individuals to manage a particular risk in an ad hoc manner and regularly put out fires? Or do we improve our capabilities?

There are conscious choices to be made when matching the organization's capabilities with its desired risk responses and vice versa. Risk management capabilities must be explicitly—and given finite resources, selectively—pursued. For each type of individual risk or group of related risks, management must evaluate the relative maturity of the enterprise's risk management capabilities. From there, management must make a conscious decision: how much added capability do we need to provide reasonable assurance we will continually achieve our business objectives? Further, what are the expected costs and benefits of increasing risk management capabilities? The goal is to identify the organization's most pressing exposures and uncertainties and to focus the improvement of capabilities for managing those exposures and uncertainties.

That is why a tool is needed to help management think clearly about the problem of matching the organization's existing capabilities with its desired capabilities. The following capability maturity model illustrates:



Source: Adapted from the Capability Maturity Model: Guidelines for Improving the Software Process, Carnegie Mellon University Software Engineering Institute, 1994

Just how capable does the enterprise want its risk management to be for each of its priority risks? That is the question.

To illustrate how the capability maturity model is used to determine the needed improvements in risk management capability, the five states of maturity may be examined using the six elements of infrastructure introduced in our response to Question 110. We will explain the interrelationships between these two frameworks and then discuss their application in practice. The explanation of each state is intended to assist organizations that desire more specificity in terms of criteria to apply the model.

As discussed in our response to Question 85, management should determine the current state of risk management capabilities for the organization's priority risks. By comparing the current state to the desired future state, using the organization's business strategy as a context, management is able to ascertain whether significant gaps exist. The capability maturity model tool facilitates the identification, analysis and presentation of gaps.

The Initial State

At the *initial state* of development, risk management is fragmented and ad hoc. The organization manages individual risks in silos and is often reactive to events. There is a general lack of policies and formal processes in place, so the organization is totally dependent on people acting on their own initiative to "put out fires." There is very little accountability, either due to the absence of a clearly designated risk owner (a gap) or because there are so many "owners" of the risk that no one can be held accountable (an overlap). Too many owners of a risk can be just as dysfunctional as having no owner of a risk, because no one can decide. The existing gaps and overlaps contribute to the lack of accountability.

In effect, the risk management capabilities that exist at the initial state are generally vested in specific individuals, and are not of an organizational capacity. This means that success is ultimately dependent upon exceptional and seasoned managers who operate on their own initiative. Success cannot be repeated without these same competent individuals. When these people leave the organization, the enterprise cannot replicate what they do. Ultimately, the organization's effectiveness depends on the efforts and heroics of these individuals. In addition, significant data quality and data architecture issues hamper the ability to obtain information for decision-making. The costs of data gathering, reconciliations and other sporadic activities are high.

For most risks, the initial state is inadequate and not sustainable. While the initial state can be rationalized for less significant risks that are not critical to the business plan, management should recognize that the lack of direction inherent in this state is a breeding ground for a crisis that can alter executive management's agenda to "damage control" on a moment's notice.

ATTRIBUTES OF RISK MANAGEMENT CAPABILITIES AT THE INITIAL STATE

The Repeatable State

Moving to the *repeatable state*, we see evidence of a basic policy structure that articulates process objectives and requirements. We also see some basic risk management processes and control activities in place to achieve the stated objectives and requirements. Human resources are allocated to risk management efforts with specific individuals designated with defined roles, responsibilities and authorities. Accountability may still be an issue at this stage because reporting is not rigorous enough to hold specific individuals accountable for results. However, progress is being made with respect to improving data quality as management begins to focus on data

architecture issues to develop better information for a few selected risks. The processes in place show some evidence of uniformity or consistency across segments of the enterprise. The "repetition" that is taking place is a result of increased process discipline and established guidelines for managing risks; however, there is minimal controls documentation. Communications across units and functions are improving. Risk management education and training reinforce the stated process objectives and requirements. However, costs are still high.

There is still reliance on people at the repeatable stage. Competent people are and always will be a vital element of infrastructure, just like policies, processes and reports. Now that other infrastructure elements are functioning, when a skilled person leaves the company, the void is not as great as it would have been had these elements not been in place. For example:

- There is basic tracking of quality, time and cost output metrics.
- Basic management reports are issued consistently and timely, with specific supporting detail available on a limited basis.
- Systematic data collection is facilitating improved reporting, increasing overall confidence in management reports.
- A process to monitor, capture and report exceptions is in place.
- A mechanism is in place to capture process and methodology improvements.
- Consistent system security and data integrity standards are in place, although systems and management reports are generally not scalable.

These increased capabilities facilitate further clarification of roles and responsibilities and encourage more effective teamwork. There is still a ways to go, however, to reach the defined state.

ENHANCED ATTRIBUTES OF RISK MANAGEMENT CAPABILITIES AT THE REPEATABLE STATE

The Defined State

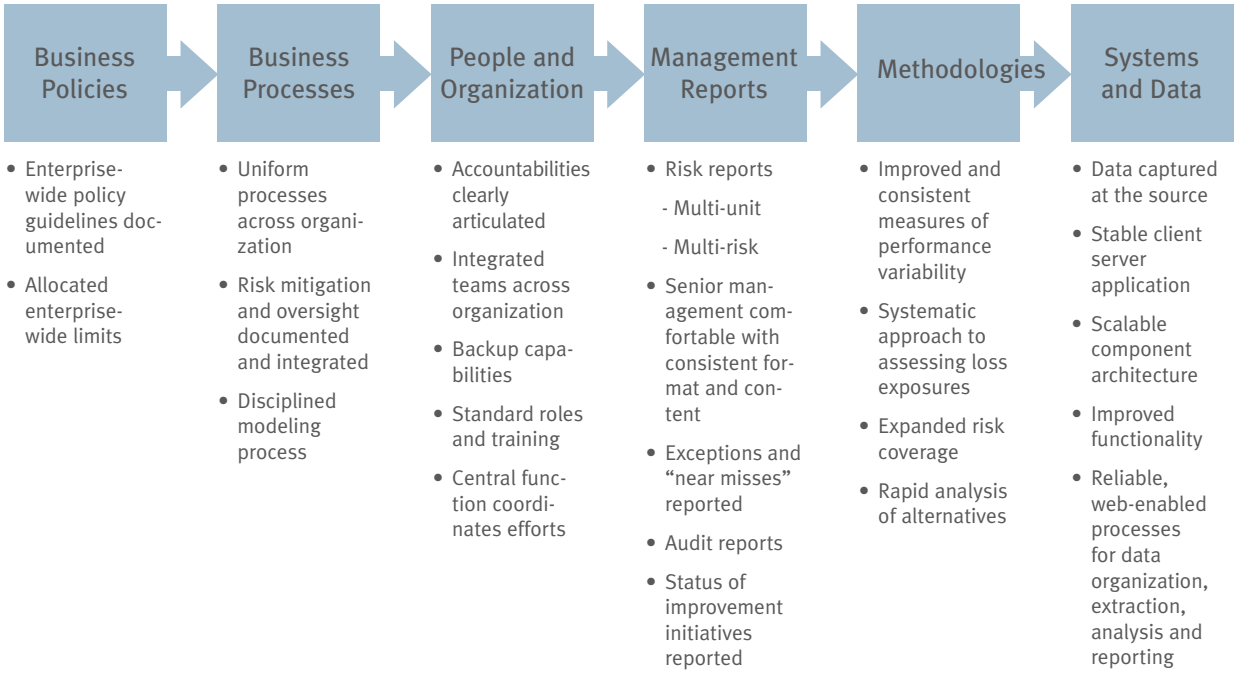
As we progress to the *defined state*, policies are further developed and processes are further refined. The discipline of the risk management process is uniform across the company's units, functions and training. Processes for risk mitigation activities and risk management oversight are clearly documented. All units and risk owners use an approved, tailored version of the organization's defined risk management process, which includes event identification, risk assessment, control activities, information/communication and monitoring.

The other elements of infrastructure are also beginning to take shape. Management is committed to managing the process through cross-functional coordination and more robust controls documentation, so that it is standardized entity-wide. Robust controls documentation includes the identification of the critical controls and the responsible owners of those controls. Verification mechanisms are in place to ensure policies are followed and processes are performing as intended. Roles and responsibilities are clearly defined and consistent across the organization, with a central function coordinating efforts, minimizing duplication and ensuring implementation of appropriate backup capabilities. Management reporting is integrated into decision-making processes across the organization and contains appropriate output qualitative and quantitative performance metrics.

The more rigorous reports, and the methodologies supporting them, add further clarity to risk management accountabilities. Systems are more stable and scalable with improved functionality providing support for reliable, web-enabled processes. Data elements are more consistent, enterprisewide, and data capture is integrated with ongoing business activities so that data is captured at the source. Finally, technology lays a foundation for all of the other infrastructure elements.

It is at the defined state where we see evidence of "risk-sensitive and risk-aware decision-making." Exceptions and "near misses" are reported timely. "Lessons learned" and control deficiencies drive improvement initiatives, which are implemented and reported across the organization.

ENHANCED ATTRIBUTES OF RISK MANAGEMENT CAPABILITIES AT THE DEFINED STATE



The Managed State

The defined state lays the foundation for further process enhancements occurring at the *managed state*. The additional improvements and increased sophistication at this higher state are primarily around improved quantification, and are driven by the more rigorous analysis and experience made possible through capabilities developed at the defined state. Because the managed state is more quantitative than the defined state, there is a stronger emphasis on measuring, aggregating and managing risks enterprisewide. For example, time-tested, integrated models and risk analytics assist decision-makers with anticipating the issues they face and with supporting the choices they make. Risk measures are linked to performance goals, early warning systems are in place and capital allocation techniques are developed and effectively deployed. Aggregate risk limits are established and allocated to operating units. When pre-defined limits are exceeded, corrective actions are taken.

In summary, at the managed state:

- There is consistent understanding of and adherence to enterprisewide policies, procedures and methodologies; employee incentives are aligned with enterprisewide strategies and objectives.
- Processes and outputs are quantitatively defined, understood and controlled; formal quality management techniques are applied to (a) eliminate nonessentials and (b) simplify and focus process activities.
- A balanced family of quality, time, cost and risk metrics reduces waste and rework; management makes decisions and applies judgment based on quantitative data, as appropriate process measures augment the output measures already in place.
- Requisite skills and experience are in place, with role models and teachers evolving and enterprisewide communication, collaboration and knowledge sharing more evident.
- The organization has the ability to conduct forecasting, scenario planning and trend analysis and is prepared for significant disruptions, if they occur.
- There is consistent use and reporting of objectives, targets, performance metrics and risks across the organization using enterprisewide systems providing dashboard reporting and drill-down capabilities.

ENHANCED ATTRIBUTES OF RISK MANAGEMENT CAPABILITIES AT THE MANAGED STATE

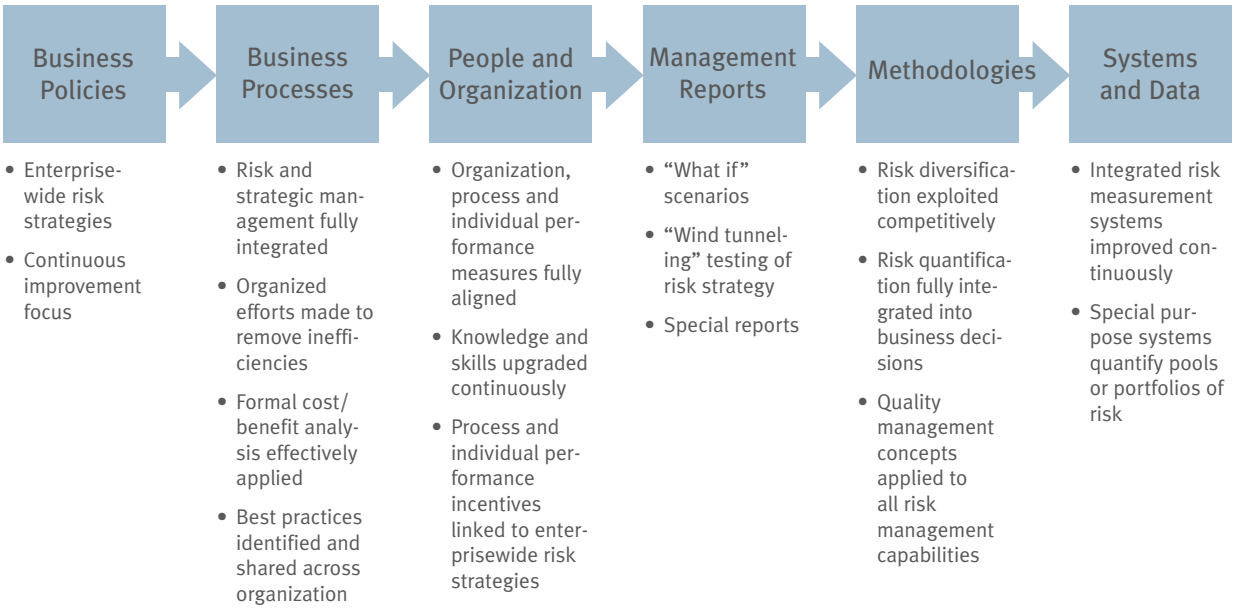
Business Policies	Business Processes	People and Organization	Management Reports	Methodologies	Systems and Data
• Revised limits based upon improved analysis and experience • Business and risk strategies aligned • Aggregate risk limits allocated to operating units	• Process benchmarks achieved • Cost and cycle time reduced • Risk management fully integrated with line management • Corrective action taken when limits exceeded • Action plans managed to completion	• Strong teamwork • Prepared for contingencies • Role models and teachers evolving • Requisite knowledge, expertise and experience fully in place • Experienced personnel apply judgment to quantified results	• Integrated risk reporting • Risk-adjusted profitability measures • Risk measures linked to KPIs • Risks quantified versus tolerances • Limits violations reported	• Integrated physical and financial models • Application of risk measures to performance goals • Early warning systems • Risks measured quantitatively and aggregated enterprisewide • Exposures anticipated through time-tested models and analytics • Capital allocation techniques applied	• Enhanced functionality • Expanded risk coverage • Risk analytics built into decision support systems • Risk analysis systems collect data as part of normal business routines • Database systems support management of risk and risk portfolios

The Optimizing State

The *optimizing state* is the highest level of capability. This stage continuously improves on the capabilities developed during the prior stages, suggesting that the journey of building risk management capabilities is one that is ongoing over time as external and internal conditions change. The entire organization is focused on continuous improvement as organized efforts are made to remove inefficiencies and formal cost/benefit analysis is applied to all risk management practices. Best practices are routinely identified and shared across the organization.

It is at this stage that the organization fully aligns its risk management policies, processes, people, technology and knowledge. It is also at this stage where the enterprise fully aligns its measures at the organization, process and individual levels. Finally, risk policies are evaluated on an enterprisewide basis to balance risk and reward as well as understand and exploit the effects of diversification across multiple risk types.

ENHANCED ATTRIBUTES OF RISK MANAGEMENT CAPABILITIES AT THE OPTIMIZING STATE



In summary, at the optimizing state, we find an innovative and continuous improvement culture, with a strong focus on improving policies, procedures, methodologies, competencies and systems. Defect prevention is the norm as process owners "build in" quality through elimination, simplification and focus techniques and application of root cause analysis consistently across the organization. Ongoing process improvement is driven by quantitative feedback and piloting of innovative approaches and continuous upgrading of knowledge and skills. Corporate improvement initiatives established and applied enterprisewide (e.g., Six Sigma) are applied to and integrated with risk management.

These are the five states of the capability maturity model. Our intent in describing each state is to provide illustrative criteria for each state and apply the six elements of infrastructure to each state. Now we will discuss application in practice.

Application in Practice

Each successive state on the capability maturity model reflects further enhancements in attributes for managing a given risk. The higher "up the curve" a company's capabilities, the greater its prospects for success in managing a given risk or group of related risks, and the lower its potential for failure.

While the various capability descriptions previously provided are generic to risk management, they can be customized to a risk or a group of related risks to provide a blueprint for analyzing the capabilities needed to manage the enterprise's business risks. Consistent and fact-based use of this framework by the enterprise's risk owners allows for a more focused definition of the current and desired states and promotes comparability and understanding across the organization. Coupled with the six elements of infrastructure, the model provides an overall framework for defining the appropriate level of risk management capabilities and the relative sophistication of these capabilities for each priority risk.

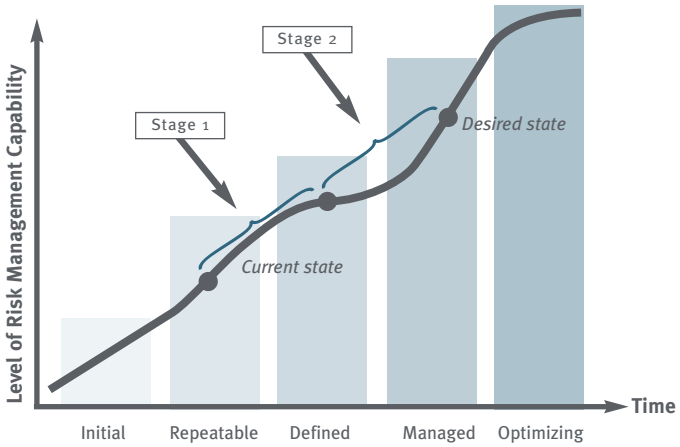
The model works as follows. For each type of individual risk or group of related risks, management evaluates the current state of the organization's risk management capabilities. The *current state* generally refers to those capabilities that are currently functioning and have been in place and relatively stable over a reasonable period of time. The current state may also take into account *planned* initiatives currently funded and underway to improve capabilities. (Note: Some may choose to refer to the effect of planned initiatives as the "improved state.")

Management then decides how much added capability is needed to achieve the selected risk response. This determination is the *desired state*. When assessing the desired state, management should be as realistic as possible. The objective is to select and design capabilities that provide the "best fit" with the core competencies that would be reasonably expected of an organization executing the enterprise's business model and strategy.

The desired state of capability may vary by risk. For example, significant exposure to changes in currency rates may require capabilities at least at the *managed state*. Some operational risks, like operating a nuclear power plant, may drive management to choose the *optimizing state* because there is little margin for error in operation. Windstorm, fire, flooding and other hazard risks, on the other hand, may only warrant periodic analysis and the purchase of insurance with little need for intricate risk reporting of any kind, a *repeatable state* capability. For certain information technology risks, such as integrity, reliability and availability risks, a *defined state* may be adequate. For security risks, a *managed state* may be desired.

Once the gap between the current state and desired state is identified and documented, then management evaluates the expected costs and benefits of increasing risk management capabilities. This is the process of drawing up a plan to transition from where the company currently is to where it intends to be. A gap analysis is the means by which companies design and implement a risk response, because it is rare for a company to implement a risk response with absolutely no capabilities of any kind in place. The actionable steps to close the gaps become an integral part of management's business plan.

To illustrate, assume the current state of a company's credit risk management capabilities lies at the repeatable state. Assume further that management decides that these capabilities should operate at the managed state. How does management close this gap? Should the improvements be implemented all at once or should they be implemented in stages, by first advancing capabilities to the *defined state* and then onward to the *managed state*?



There are three reasons why "a staged approach" to the design and implementation of improved capabilities is preferable to closing the gap at once. First, it is the more systematic of the two approaches from a change enablement perspective, i.e., it is the approach that is least disruptive to the organization and is more in line with the change readiness of its personnel. Second, the deployment of capability maturity with managing software solutions has proven that a staged approach increases the chances of a successful implementation. Third, while best practices are often useful and insightful, they are not a substitute for the exercise of careful thought and judgment by knowledgeable personnel about the enterprise's desired risk management capabilities for a given risk. Therefore, the entity's change management plan should address how the enterprise transitions from the current state to the future state and how quickly. Use of the six elements of infrastructure and capability maturity model facilitates this planning.

To further illustrate the use of the two frameworks, following is a summary of capabilities around managing procurement risk:

	Business Policies	Business Processes	People and Organization	Management Reports	Methodologies	Systems and Data
Optimizing	Aligned strategic plans, total strategic sourcing, defined and integrated policies and responsibilities	Integrated and effective procurement processes and continuous benchmarking	Ability to adapt to changing environments and customer demands, outsourcing of non-core competencies	Fully developed automated, consistent follow-up and planning	Aligned strategic methodologies that emphasize continuous improvement	Complete suite of systems across the supply chain for analysis
Managed	Increased execution of strategic sourcing; personnel aligned with strategy	Effective use of formal risk management techniques	Consolidated and leveraged supply base in place; trained commodity teams	High-quality procurement information, self-assessment commonplace	Sophisticated, robust models and tools	Procurement data warehouse in place and utilized; P-cards and automation
Defined	Annual procurement plans, strategic sourcing for key commodities	Defined processes, strategic partnerships in place	Accounts payable centralized, training offered, and special purpose teams	Key suppliers tracked, standard benchmarks and internal audits	Well-developed models available for decision-making	Organization operates with contracts
Repeatable	Only occasional strategic focus on sourcing and informal polices	Occasional supply leverage; a few strategic partnerships	Some procurement professionals on staff; limited training	Key internal procurement information available with audits occurring	Simple models that are used inconsistently	Suite of fairly effective systems; procedures manual
Initial	Procurement not addressed as a strategic opportunity, no direction or policies	Purchases not leveraged, no strategic partnerships	No leadership and lack of qualified staff	Critical information not available and no internal auditing	No models; reliance on people	Disparate, inefficient, purchasing, accounts payable systems

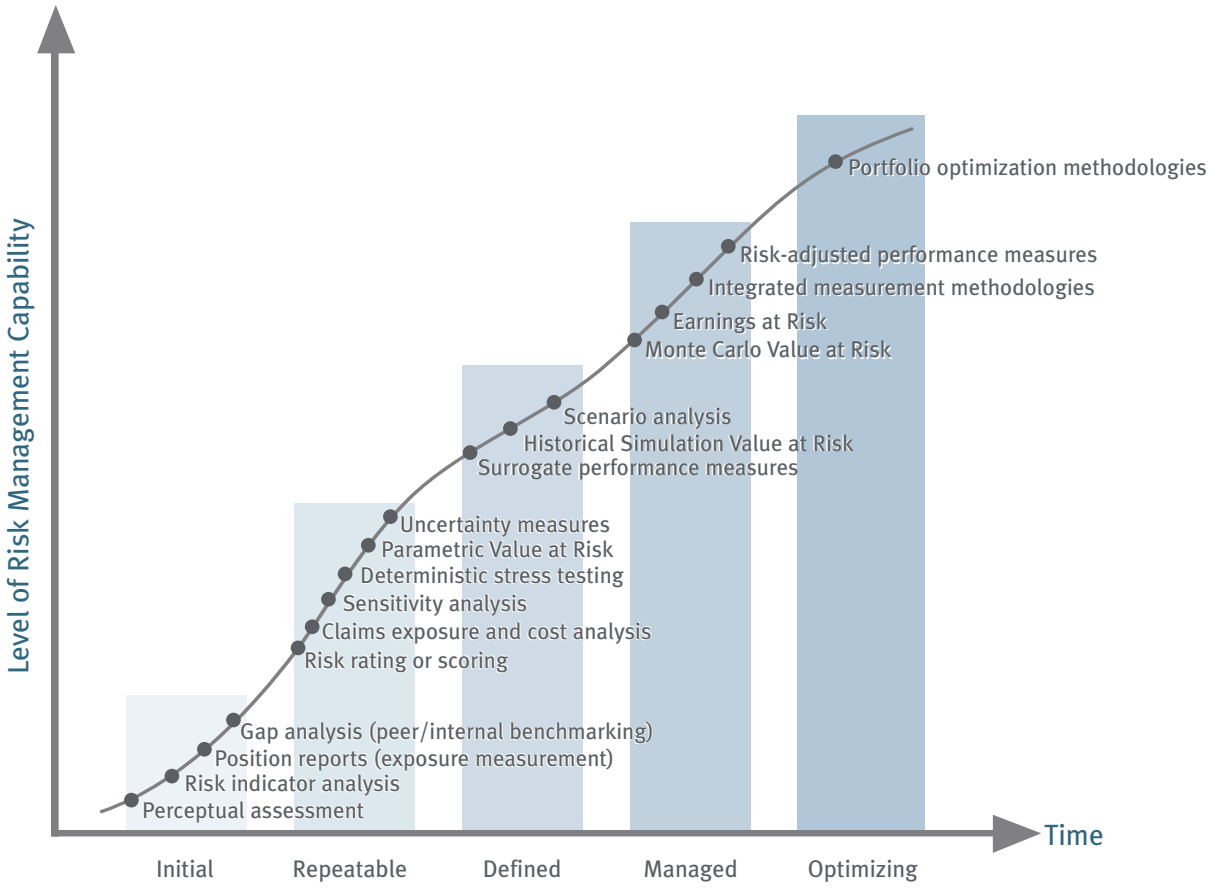
Throughout the risk-response planning process, it is important to recognize that what represents "best practice" in the context of a particular risk at one company may be insufficient or overdone in the context of the same risk at another company. For instance, the more sophisticated applications of value at risk may represent best practice for managing market risk in a trading business. However, in another business where just a handful of transactions exposed to price risk are involved, such sophistication may be unnecessary because of the negligible exposure. It is unnecessary to deploy the most sophisticated and advanced techniques for all risks. No organization has the resources to do that. Nor is there a viable business reason to do so.

112. What are alternative techniques for measuring risk and when are they deployed?

As the organization's capabilities improve, its risk measurement methodologies also improve. There are many methods for measuring risk. In the capability maturity model, there are five states of capability – initial, repeatable, defined, managed and optimizing. With each successively higher state, there is a higher level of knowledge, expertise and understanding. The higher the level of capability, the more sophisticated the measurement methodologies that can be effectively deployed. At the lowest level of capability, the techniques used are typically directional, i.e., they surface areas for further analysis. As capabilities increase, the measurement techniques available are more reliable and actionable for decision-making.

In general, the rigor and sophistication of the measurement methodology needed for a particular risk or group of related risks are driven by the complexity of the environment (for instance, the number of risks and interrelationships between risks), the extent of expected volatility and the criticality of the risk to the execution of the business model. The level of capability desired by management (such as the extent of aggregation and linkage to enterprisewide performance) is also a key factor. Implementation costs and the availability of relevant data (with some level of implementation possible even with sparse or "noisy" data) are also considerations. For example, large, complex portfolios of highly volatile commodities that can have a significant effect on earnings may require more sophisticated techniques, including both statistical models and scenario analysis. Simulation-based models, for instance, can be useful for capturing the interaction of rate, price or other factors when dealing with complex portfolio or risk positions. Sensitivity analysis or stress tests are then used to measure the potential impact of extreme market movements on the value of the portfolio.

The following schematic illustrates examples of risk measurement techniques that are appropriate at each state of maturity along the capability maturity model:



Risk measurement at the initial state – At the initial level of capability, risk management activities are ad hoc. The measurement methods deployed at this stage must be relatively straightforward and easy to apply and understand because the organization lacks the knowledge and basic risk management capabilities to apply more robust and complex methodologies. At the initial stage, it is not enough for the few competent risk management personnel working for the organization to understand the application of these measurement methodologies. Because the organization lacks, among other things, risk management policies, processes and knowledge, these measurement methodologies would more than likely be applied as an appendage rather than as an integrated tool. Thus executive and business unit management will have difficulty translating the insights these methodologies provide into actionable plans. The organization would also not be generating in the normal course the data inputs these methods require. When the individuals using the tools leave, what does the organization do with tools no one else understands? Thus the measurement methodologies need to be as simple and as straightforward as possible for the organization to assimilate them into normal business activities. Self-assessment techniques, facilitated assessments, risk indicator analysis, position reports and gap analyses (using common frameworks) are examples of such techniques. These techniques are more directional than actionable, because they often point out areas requiring further investigation and analysis.

Risk measurement at the repeatable state – At this stage, basic risk management policies are in place, basic risk management processes are established and basic control activities are installed. Measurement methodologies also tend to be somewhat basic. Following are some examples:

- ***Risk rating or scoring***: Systematically rates or scores the level of risk. Often used to rate customer credit risk consistently and to support, manage and monitor credit authorization decisions, both by multiple executives making similar decisions across the enterprise and by individual executives evaluating multiple customers. Risk rating or scoring:
  - Uses analytical templates and systems based upon the application of predefined, preauthorized criteria.
  - Increases the effectiveness, efficiency and consistency of the fact gathering process through a common structure supported by common criteria.
  - Increases the quality of decision-making by requiring managers to apply the same criteria and guidelines when evaluating the facts gathered.
  - Prompts consultation with a higher authority whenever unusual, outlier situations arise.

  Note that some credit risk rating systems are very sophisticated. As organizations take their credit risk management capabilities to the defined and managed states, they enhance their scoring or rating methodologies.
- ***Claims exposure and cost analysis***: Evaluates the variables that ultimately determine the cost of various types of claims – warranty, litigation, environmental, health and safety, etc. Decision-makers use this data to decide on the appropriate actions to take.
- ***Sensitivity analysis***: Determines the aggregate variation in financial performance by assessing the impact attributable to a small differential change in one or more underlying key risk factors on individual exposures at a given point in time.
- ***Deterministic stress testing***: Takes a given "base case" portfolio or forecast and modifies its value to reflect the effects of a hypothetical, extraordinary but highly unlikely situation or event that will result in severe financial stress if it were to occur.
- ***Parametric value at risk***: Calculates value at risk to evaluate the potential impact of an underlying variable, such as a foreign exchange rate, on the value of a portfolio in the future. It is based upon the assumption that the distribution from which the future values of the underlying variable will be drawn over the selected time horizon is identical to an assumed normal distribution.
- ***Uncertainty measures***: Tracks key variables relating to an identified exposure or source of value to obtain a measure of the expected performance variability. Whereas the exposures reported in a position report are the nominal gross measures (total accounts receivable, production throughput or revenue streams),

uncertainty is a measure of the performance variability associated with returns from that gross measure. For example, a foreign exchange exposure might be £10 million, while the risk metric would be defined as the expected volatility in the exchange rates applied to the gross value of the exposure. Examples of key variables for evaluating uncertainty are provided in Question 3.

Risk measurement at the defined state – At the defined stage, measurement methodologies reflect the additional elements of infrastructure that have been implemented, including improved reports, more robust methodologies and more stable technology. Measurement methodologies are more refined at this stage. Following are examples:

- ***Surrogate performance measures***: Uses measures of quality, time and cost performance as surrogates for measuring risk. For example, it may be impossible to measure customer satisfaction risk directly. How do you measure the consequences of customers who are dissatisfied with the company's product or service, considering the customer's likely behavior, the likelihood of new replacement business in future periods, the potential for permanent loss of repeat business and the loss of market share? As an alternative surrogate, the company can integrate internal operating statistics, customer feedback and other external information. By doing so, it can evaluate customer satisfaction measures and gain insights as to how well it is managing its customers. If these measures reflect consistently positive performance over time, the company can infer that it is effectively managing customer satisfaction risk.

- ***Historical simulation value at risk***: Computes value at risk based upon the assumption that the distribution from which future values of an underlying variable will be drawn over the selected future time horizon is identical to the distribution of historical values observed over a specified period of time in the past.

- ***Scenario analysis***: Determines the aggregate variation in financial performance by assessing the impact of large risk factor changes, as defined by a specific scenario, on individual exposures. Like sensitivity analysis, scenarios and their earnings impact are evaluated in a deterministic manner, i.e., no assessment is made of the probability that the events will actually occur. However, scenario analysis is a more robust measurement methodology than sensitivity analysis because it involves (1) multiple variables that are often changed dramatically during the procedure and (2) economic forecasts and models to reprice exposures and portfolios based upon the assumed changes and forecasts.

Risk measurement at the managed state – The defined state lays a foundation for progressing to the managed state where risks are managed quantitatively and aggregated at the corporate level. At the managed state, we see such measurement techniques as:

- ***Monte Carlo value at risk***: Calculates value at risk by adjusting the distribution of possible values for what managers believe will be closer to reality (what will actually happen) than a distribution based solely on a historical sample.

- ***Earnings at risk***: Combines operating factors, such as load and capacity, with market changes to the calculation of value at risk to broaden the range of potential outcomes considered. It measures the extent to which earnings might fall short of expectations during the planning horizon, given management's assumptions around key risks.

- ***Integrated measurement methodologies***: Combines rigorous models and analytics to develop proprietary techniques that are continuously improved over time. These methodologies come in a myriad of types and degrees of complexity, including models of (a) individual risks, (b) groups of related risks and (c) the enterprise's aggregate risk profile. They may also address the enterprise's business environment, considering such factors as competitive and industry dynamics, political trends, customer demand, suppliers and broader market conditions (such as the interplay between demand and load on price-sensitive energy portfolios).

- ***Risk-adjusted performance measurement***: Measures business unit performance based on economic definitions of investment, capital and returns to provide a performance measurement and reporting tool that aligns incentives of shareholders, senior management and business unit management.

Risk measurement at the optimizing state – The organization is focused on continuous improvement at this stage. The extent of knowledge and understanding of risk at this stage leads to measurement methodologies which are focused on a portfolio view, or pools of risks. Instead of managing individual risks, management optimizes risk management by pooling risks into logical families where they are measured and managed as a portfolio. A portfolio is a natural grouping of risks sharing fundamental characteristics, e.g., common drivers, positive or negative correlations or other characteristics that make the risks susceptible to the application of common measurement methodologies and risk responses. If risks are aggregated and managed as a portfolio, the quantitative means to transfer and securitize risk are developed. Transfers of risk are also more efficient when risks are netted or offset. To illustrate, currency exposures can be pooled to determine the company's "net exposure" – when that practice corresponds with the organization's operating philosophy. This "total risk focus" leads managers to develop proprietary methodologies that optimize risk and return on a portfolio-wide basis, leading to higher confidence that decisions are based on a complete view of the business. For example, credit risks can be aggregated with currency risks so that a common measure is focused on how credit risk increases or decreases as currency rates change. Huge shifts in currency rates may cause shifts in exposure to particular counterparties because the market revaluations may affect their ability to pay their debts.

113. How does ERM influence management reporting?

Reporting is a critical element of ERM infrastructure. As organizations evolve toward more repeatable, sustainable and automated compliance and governance programs, technology will play a key role in improving the methods and tools enabling the two COSO components: Information and Communication, and Monitoring. Specifically, technology can facilitate the evolution of the risk management process. For example, a company's risk management may primarily consist of:

- ***Discrete activities***: These activities typically emphasize documentation within a single data repository.
- ***Periodic activities***: For many entities, these activities are typically driven through a self-assessment type capability.
- ***Continuous activities***: Limited to a single repository, these activities allow for continuous update sharing, and notification of information.
- ***Continuous enterprisewide activities***: These activities support process and control automation, real-time Key Risk Indicator (KRI) reporting and monitoring across disparate applications.

These activities embed risk management processes into the day-to-day business routine, thus providing greater assurance and more effective execution. The objective of ERM infrastructure is to further integrate these activities and improve them continuously. Management reporting represents an integration and improvement opportunity because it links risk and risk management performance with what's important.

As discussed in our response to Question 45, executive management needs information to make informed decisions with confidence regarding the priority risks that the organization faces. An enterprisewide view leads a company to integrate its information about risk and the performance of its risk management capabilities with other information used in the business. Thus the organization measures and reports on what matters – this means ALL of its critical information relating to quality, time, cost and risk should be integrated on its balanced scorecard. Companies committed to ERM work to make this integration happen.

Reporting is especially important, as well as inherently difficult, when managing risk using qualitative data. In the absence of robust quantitative methodologies, reports can be generated in a variety of ways, including standard report templates, filtered reports, searches and ad hoc queries. As discussed in Question 121, dashboards provide aggregated views of information, allowing users to drill down further into areas of interest or concern for additional details. When reporting is augmented through enterprise applications, the ERM solution becomes more comprehensive. Enterprise applications provide automation and workflow capabilities outside of specific governance requirements. They also provide content management, supporting enterprise-level document and knowledge sharing, and live transaction feeds for real-time monitoring of KRIs.

114. What risk management software products are currently available to assist companies with implementing ERM?

There are three primary categories of risk management software vendors: (1) enterprise risk assessment tools (e.g., decision support, survey and risk registers), (2) operational risk software tools (e.g., qualitative and quantitative) and (3) integrated compliance and risk management platform solutions. Each of these categories is discussed below.

Enterprise risk assessment (ERA) tools cover a broad range of decision support, survey and risk register tools. Decision support and survey vendors approach the market from their strength in enabling facilitated risk workshops, control self-assessments and/or entity-level risk assessments. These vendors continue to build out their solutions by adding web-based survey functionality to support risk assessments outside of a captive workshop setting. There are also several small vendors who offer risk register tools that: support one or more risk frameworks; provide a data repository for objective, process, risk and control information; support ongoing monitoring, testing and action planning; and provide basic reporting capabilities. These solutions are relatively simplistic and unsophisticated, and generally lack integration with other compliance and risk management activities.

There are more than a dozen software vendors who develop and sell specialized products for ***operational risk management (ORM)***. Primary components of an ORM solution include data collection and self-assessment tools, scenario and model building, operational risk exposure and capital calculators, and internal and regulatory reporting. Many of these solutions were initially developed by the vendors in collaboration with one or more clients, and enhanced over time. Some offer qualitative risk management solutions integrated with internal audit workflow and Sarbanes-Oxley compliance templates. Others tend to have a banking/Basel II compliance orientation. Still others offer sophisticated risk modeling and analytical tools, including frequency and severity estimation, exposure calculation, capital calculation, and scenario analysis as well as loss event tracking.

Finally, ***enterprise software vendors*** are aggressively entering the compliance and risk management market. These vendors are offering solutions initially designed to enable Sarbanes-Oxley compliance, but with clear intentions to extend capabilities beyond Sarbanes-Oxley into risk management and other compliance areas. The end game for these vendors is to develop a "total solution" for broader compliance, governance, and risk management, with assistance and subject matter contributions from consultancy alliance partners.

115. Has the ERM software market reached maturity such that there are established solutions and clear leaders?

Several factors are influencing the market as this publication goes to print:

(a) There is a mandate to focus on internal control over financial reporting from the Sarbanes-Oxley Act, providing further justification for technology investment.

(b) There is continued emphasis on improving internal audit performance from the New York Stock Exchange listing requirements.

(c) There is a stronger push to understand and quantify operational risk from European regulators.

(d) Many companies have a strategic intent to integrate synergistic compliance and risk management activities, enabled by a common risk management technology infrastructure and data.

Today, an increasing level of attention is being paid to operational risks as financial service regulators around the world focus on responding to the recommendations for capital adequacy coming out of the Basel II Accord by the Basel Committee on Bank Supervision, an international consortium of bank regulators. Several software vendors entered the operational risk management space in the late 1990s, motivated by innovation and automation taking place in other areas of risk management. More vendors entered the market after the Basel announcement that the next wave of capital adequacy recommendations would include operational risk. The entrance of vendors to the market is not surprising, given that more than 100 nations have agreed to the Basel II provisions.

Unfortunately, the market is maturing far more slowly than expected. The current providers are a combination of old guard and new entrant providers. Neither is especially well proven due to the relative lack of success for any of the established products. Newer players tend to have a more pragmatic approach to risk management, and have introduced solutions more aligned with current market requirements. Competing solutions are more comparable now in terms of functionality and price. At this time, no clear market leader exists, though several solutions are gaining market share.

Many solutions are relatively new to the market or in beta. Several vendors are still in the design phase. No truly integrated solution exists. It is possible the market is due for further consolidation, leaving only a handful of enterprise software vendors and operational risk specialists. Risk management software tends to be very different across geographies, with different factors driving adoption leading to different prioritizations of functionality. Software solutions that integrate compliance, risk management, and internal audit efforts are likely to be the most successful over time.

116. What criteria should we use to evaluate the software alternatives? Are there different prioritizations of functionality?

The criteria for evaluating ERM software and the relative priority of functionality may vary from company to company. The organization's requirements and approach typically drive the relative priority. The significant features and definitions of an end-to-end solution for risk management are summarized below to provide criteria for evaluating alternatives. (Note: ERA = Enterprise Risk Assessment; ERM = Enterprise Risk Management; ORM = Operational Risk Management; IA = Internal Audit):

FEATURE	DEFINITION OF FUNCTIONALITY	COSO ERM COMPONENT	SOLUTION
Entity definition and objectives	Document organizational hierarchy and identify business components for risk reporting structure	Internal environment, objective-setting	ERA, ERM and ORM
Risk identification	Incorporate a common risk model, identify potential threats and vulnerabilities, estimate likelihood and impact of events, source risk drivers, determine key risk indicators, and map risk types to business processes and units	Event identification, risk assessment	ERA, ERM and ORM
Framework support	Support several regulatory and/or proprietary risk frameworks	Various	ERA, ERM and ORM
Risk control and monitoring	Define required controls, respond to mitigate risk drivers, rate effectiveness of controls, test controls and estimate residual risk	Risk assessment, risk response, control activities	ERM and ORM
Risk workflow scheduling and notification	Monitor assessment schedules, risk profiles, and action plans in real time and generate automated and tiered escalation and notification, staff routing and exception handling (Note: The better systems will support custom workflow process to incorporate user requirements)	Risk assessment, risk response, control activities, monitoring	ERM and ORM
Risk and audit issue tracking	Deploy automated prompts for escalation of issues and control weaknesses for corrective action, and support monitoring of corrective action plans	Risk response, control activities, information and communication, monitoring	ERM and ORM

FEATURE	DEFINITION OF FUNCTIONALITY	COSO ERM COMPONENT	SOLUTION
Data collection/event tracking	Record internal, potential and external loss information; monitor potential future events that have not yet occurred; gather data to estimate potential for future losses; support workflow to route information	Information and communication, monitoring	ORM
Risk and control self-assessment	Use automated questionnaires enabling process and/or risk owners to enter information about their losses and exposures, including frequency and severity of potential future losses as well as evaluation of strengths and weaknesses of risk management capabilities; determine inherent risks; establish thresholds and limits; and create assessment models (Note: Flexibility to define categories, questions, respondents, and parameters for questionnaires and distribution mechanism for tracking and auditing processes related to these assessments are also important)	Risk assessment, risk response	ERA, ERM and ORM
KRI/KPI definition and tracking	Define a standard template for risk indicators/ performance indicators for use across the enterprise; relate KRI/KPI to specific business units or processes and/or to specific loss events; generate management alerts of threshold breaches; support comparison against benchmarks	Risk response, control activities, information and communication, monitoring	ERM and ORM
Frequency and severity estimation and other statistical analyses	Assess the importance of a particular exposure and recognize the likely frequency and severity of a loss; allow for these estimates to be input manually or derived based on historical data; basic functionality includes red-amber-green assessments; more advanced features provide ability to derive estimates based on historical data directly within the system, and allow for different scoring models across risk types	Risk assessment	ERM and ORM
Exposure calculation	Translate KRI, frequency and severity estimates and self-assessment information into quantified exposures, including probability distributions which provide visibility around a range of potential outcomes	Risk assessment, risk response, information and communication	ORM
Scenario analysis	Take the exposure calculation one step further by allowing the user to change the base assumptions and observe the impact of change on a potential risk exposure – "what if" functionality	Risk assessment, risk response, information and communication	ORM
Capital calculation	Change the exposure calculation into a capital attribution based upon either external regulatory guidelines or, in the case of economic capital, internal capital charge rules; provides the ability to support different definitions of capital	Risk response, information and communication, monitoring	ORM
RAROC analysis	Translate capital calculation into a performance assessment by adding another calculation that takes into account the revenue associated with a particular business unit and other costs (other than capital)	Risk response, information and communication, monitoring	ORM

FEATURE	DEFINITION OF FUNCTIONALITY	COSO ERM COMPONENT	SOLUTION
VaR model	Support distribution and scenario-based approach	Risk assessment, risk response, information and communication, monitoring	ERM
Internal reporting	Display results of various assessments and analyses to line and senior management; provide flexibility to address future yet-to-be-defined reporting requirements; reports are typically distributed via the web or email, and are generated in various forms including standard report builders, filtered reports, searches, dashboards, and integration with third party reporting tools	Internal environment, information and communication, monitoring	ERA, ERM and ORM
Regulatory reporting	Generate pre-defined risk reports for regulatory entities, investors and board	Internal environment, information and communication, monitoring	ORM
Risk response	Capture risk mitigation strategies and support gap analysis using relevant frameworks	Risk response	ERM
Compliance templates	Provide support templates for other compliance management activities such as Sarbanes-Oxley compliance	Various	ERM
Audit planning	Support annual risk assessment and audit plan development	Risk assessment, monitoring	IA
Project management	Deploy case management and project administration capabilities unique to internal audit planning and execution	Monitoring	IA

The above criteria provide a perspective as to the functionality to look for when evaluating software alternatives. As noted earlier, the company's requirements and selected ERM approach typically drive the relative priority of functional specifications.

117. Is specialized ERM software preferable to broader platforms for compliance, governance and risk management?

Yes, in the near term until such time that a genuine total solution emerges. This is particularly true for quantitative risk management solutions. However, those software solutions that integrate compliance, risk management, and internal audit efforts are likely to be the most successful over time.

118. How does software functionality support the goals of ERM?

Let's focus first on Operational Risk Management (ORM) for financial institutions because that is a niche market that software providers are actively addressing due to the requirements of the Basel II Accord. The goals of ORM efforts primarily center on two areas:

(a) Minimize losses due to operational risk by increasing the visibility of exposures and managing the efficiency of internal controls that mitigate these exposures.

(b) Provide management with estimates of potential losses to ensure that sufficient capital is available to protect institutional stability and an adequate return is achieved to justify losses taken.

The first of these goals is enabled by solution functionality that provides loss data collection, event tracking and monitoring, self-assessment and management reporting. The second of these goals is facilitated by key

risk indicator creation, frequency and severity estimation based on historical, external, or modeling techniques, scenario analysis, and exposure and capital calculators.

ERM builds on the functionality provided by software facilitating ORM. The goals of ERM primarily center on improving strategic decision-making by evaluating activities that are creating or destroying enterprise value. This goal is enabled by solution functionality that provides risk definition, risk management capabilities gap analysis, control activities documentation, entity-level monitoring, workflow scheduling and notification, risk and audit issue tracking, VaR modeling, risk response and management reporting. This expanded functionality will fulfill the requirements of most companies.

119. What are the primary categories and characteristics of successful ERM software vendors?

There are four primary categories of risk management vendors: risk management experts, process control experts, risk software specialists and consulting firms. Some general observations are provided below with respect to each of these categories.

Risk management experts approach the market from their strengths in market or credit risk. Their goal is to continue to build out their risk platforms and provide further support to clients by cross-selling additional functionality for operational risk. These vendors are typically strong in modeling and simulation techniques. They also understand the theory behind complex financial products and can effectively discuss risk with quantitative analysts employed by banks in their risk management departments.

Firms with ***internal audit or control expertise*** in the marketplace have also added risk management to their solution sets. These vendors may not have as much expertise in risk modeling or quantitative finance as risk management vendors, but they do understand how to identify potential process failures. This capability in processes, risks and controls tends to make these providers stronger in the areas of loss collection and tracking, incident monitoring and self-assessment.

There are relatively few vendors in the market that sell specialized products built solely for risk management, and even these ***risk software specialists*** are now attempting to reposition themselves as providers of broader solutions for SOA compliance. All of these solutions received third-party funding to build their respective packages, and in most cases, this funding came from a financial institution.

In general, while ***consulting firms*** may have a point of view with respect to technology, they may not actually offer a software solution to the marketplace. For example, at the time this publication went to print, the Big Four firms have divested their interests in proprietary technology solutions due to apparent conflicts of interests, and now prefer to partner with one or more software vendors to influence their ongoing product development.

While there are many characteristics differentiating successful vendors, we have summarized the following as particularly important:

- ***In-depth risk management knowledge***: Risk management is inextricably linked with business processes. The vendors that best understand an organization's processes, including how they are managed, and the organization's overall goals are best equipped to develop superior software solutions. The solutions may be integrated within an organization's existing structure and processes with minimal disruption to the business.
- ***Ability to educate prospects and customers***: Risk management is still more of an art than a science and oftentimes must be taught before it can be sold. Vendors that have a strong culture of thought leadership and evangelism are better positioned to provide solutions that will make a difference.
- ***Ability to execute and support***: Risk management solutions should not introduce more risk than they help to mitigate. If any vendor cannot assure its clients that it will provide high-quality software and post-implementation support, the product does not warrant further consideration.

- ***Professional services***: Risk management systems cannot be successfully implemented until risk is properly understood and the underlying business processes are properly defined. Software vendors that have in-house subject matter experts or alliance relationships with consulting firms have a distinct advantage in this regard.
- ***Global presence***: Larger companies need support from global vendors. While local firms may be able to assist smaller, domestic-based companies, only those vendors that can support global deployments merit consideration by multinationals.
- ***Dedication to market space***: Companies should focus on vendors committed to large, ongoing investments in product development.

Other key indicators include the importance of risk management revenue to the firm, the firm's overall size, its ability to leverage existing relationships to build technology, operational and financial risk expertise, and its market share and changes in share over time. Long-term success depends primarily on the extension of existing solutions into broader compliance, governance and risk management areas. While there are several vendors worthy of consideration, management should keep in mind that they have very different strengths and weaknesses. Management should be certain the company's long-term requirements will be supported by ongoing product development and enhancement of the solution selected. Because most solutions are not totally developed, management will be highly dependent upon future investments by the software vendor. Therefore, management should understand the vendor's future plans and product releases.

120. Is it better to design an ERM process first and then select the appropriate ERM software, or vice versa?

The ERM software should support the process and not the other way around. Management must be clear on goals and definitions. We don't believe it is a very good idea to select a vendor first, only to discover late its strengths and capabilities are not properly aligned with management's chosen methodology. For example, if management requires a scorecard approach, then they should select a solution that can actually automate a scorecard. The six elements of infrastructure introduced in Question 110 provide a context for the need to decide the process *before* choosing the software.

121. What is dashboard or scorecard reporting and how is it used in an ERM environment?

Models, risk analytics and web-enabled technologies make it possible to aggregate information about risks using common data elements to support the creation of a risk management dashboard or scorecard for use by risk owners, unit managers and executive management. Dashboard and scorecard reporting is flexible enough to enable the design of reports to address specific needs. Examples of dashboard reporting, which often features "heat maps" or "traffic light" indicators, are provided in the Application Techniques of the COSO ERM framework.

Dashboard reporting supports risk management across the enterprise by providing a framework for identifying, capturing and organizing risk data elements from external and internal sources that are readily available to risk owners. The dashboard houses enabling frameworks, templates, tools and reports to assist managers throughout the organization with managing risk in a consistent, uniform manner so the organization "learns once" rather than "reinvents the wheel" multiple times. It increases the effectiveness of and value contributed by assurance units (see Question 56), by providing them access to a data storehouse and "risk register" replete with risk management knowledge and information.

One function of a dashboard is to aggregate data and information about risks that are difficult to quantify. A dashboard provides a repository for data points and information about each business unit, risk unit and support unit, including their respective processes, risks, risk management capabilities, internal controls, near misses and loss events. While it does not replace other systems that provide unit managers and risk owners the hard numbers and analytics they need to manage and control risk against established limits, the dashboard may incorporate feeds from those systems. To illustrate, the dashboard provides, among other things:

- ***A common language for organizing risk management information***: A common language organizes information and data about risks, risk sources, risk metrics and risk management capabilities for extraction, analysis and reporting at the enterprise, unit and process levels.
- ***A timely feedback mechanism***: It is useful to generate periodic feedback on risks, risk management capabilities, risk incidents, loss events and other relevant matters through polling methodologies that engage unit managers, process and activity owners and risk owners throughout the enterprise. These polling exercises are useful for rating the severity and likelihood of risks and for prioritizing the gaps around managing the priority risks, so that the appropriate risk owners can be assigned on a timely basis and risk management capabilities can be improved in the appropriate areas. They are also useful when contrasting perspectives at different levels of the organization.
- ***A data repository***: Templates provide the means for managers and risk owners to document risk data at the organization, operating unit, process and sub-process levels using predetermined frameworks, and provide the means for managers and risk owners to keep that data current. They include:
  - Risk ratings, risk tolerances and residual risk
  - Self-assessments of the effectiveness of risk management capabilities and the critical internal controls
  - Risk responses and control activities to address priority risks
  - Gaps in risk management capabilities and performance
- ***Status reporting on initiatives***: This reporting stimulates continuous improvement of risk management capabilities and increases the visibility and instills the discipline across the organization to see implementation of planned improvements to completion.

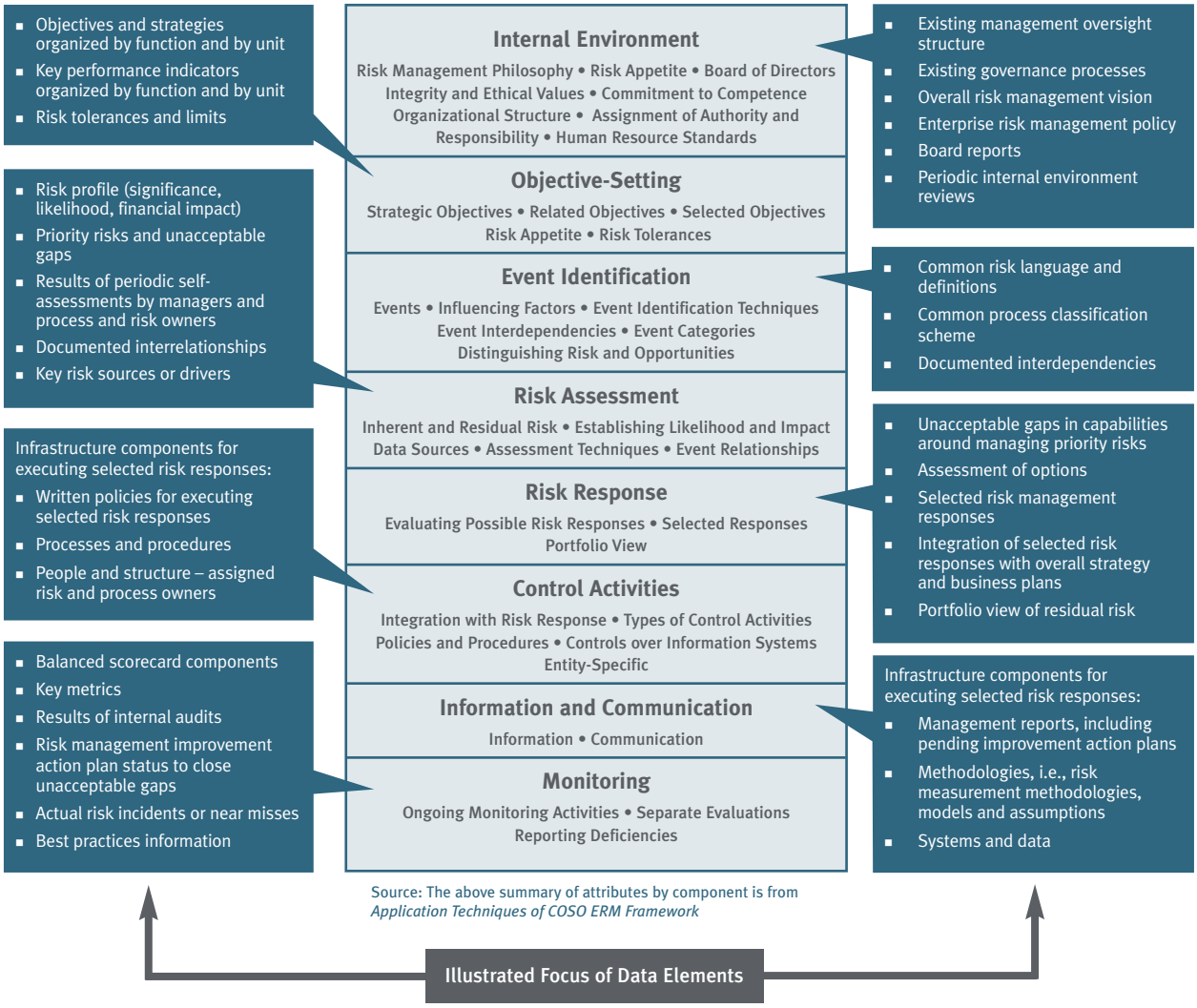
There are many ways for management to use the dashboard in an organization. Following are illustrative examples:

- Executive and unit management can use the dashboard to (a) facilitate and improve risk communication, oversight, compliance and monitoring and (b) align risk management with the achievement of business objectives, related strategies and key performance metrics.
- Risk and process owners throughout the organization can input data about risks, risk responses and internal controls and gain insights about risk management performance and best practices.
- A central Business Risk Management Function, an assurance unit or risk unit (see Question 56) can:
  - Roll up information using common data elements that support "scorecard reporting" of the organization's risk profile and risk management performance at appropriate levels of the enterprise and warehouse those data elements linking operating units, divisions, processes and functions.
  - Use data analytics and decision support tools to mine and analyze data to identify trends warranting attention, create relevant information and develop a myriad of different reports for management and the board.
  - Summarize relevant information on an enterprisewide, a business unit, a geographic and a product basis to enable decision-makers to evaluate trends monthly, weekly, daily or even in real-time (in those rare circumstances when this capability is warranted).
  - Develop internal and external benchmarking, knowledge sharing, early warning techniques, scenario assessment, risk aggregation and other applications.
  - Assist senior management in supporting an assertion that it is complying with the COSO ERM framework or other established frameworks (e.g., COSO internal control framework, Turnbull, Standards Australia, KonTrag, etc.).
  - Capture improvement opportunities identified by management, process and risk owners and internal audit, and facilitate identification of best practices for sharing across the organization. Support monitoring of the status of open action items to ensure execution of improvement action plans.

The information systems supporting risk management should be scalable so they can be enhanced over time as the organization's needs change and software enhancements become available (see Questions 114 through 120 for discussion of software alternatives and related issues). Management also needs to satisfy itself that data and information feeds are reliable and timely. As it evolves as a reporting, monitoring and reference tool, the "business risk management dashboard" creates value for the organization that its competitors cannot easily replicate.

Many types of data are relevant to the informational needs of executive management and risk managers, including historical data, transaction data, positional data and calculated data. Examples of data elements that support the activities of the risk management process and standardize terminology, definitions and measures are presented below using the eight components of the COSO ERM framework:

KEY ELEMENTS OF EACH COSO COMPONENT



Source: The above summary of attributes by component is from *Application Techniques of COSO ERM Framework*

Deployed in conjunction with web-based risk management systems and tools, risk management dashboards facilitate the organization's learning and stimulate continuous improvement of risk management capabilities by warehousing relevant data elements that provide a common link among the entity's business units, risk units and support units (see Question 56 for discussion of these terms). If risk and process owners throughout the organization feed data into the data warehouse about their processes, risks, risk management capabilities

and internal controls, the database can be used to extract information regarding the enterprise's risks and risk responses and provide the risk reporting requested by decision-makers. Ideally, these systems should build on or be integrated with the disclosure process in place to support compliance with the public reporting provisions of Sarbanes-Oxley.

122. For financial services companies, is economic capital measurement a prerequisite for adoption of ERM?

No, economic capital measurement is not a prerequisite for the adoption of ERM. However, economic capital measurement is a powerful tool that enables financial services companies to (a) obtain a consistent and comparable measure of exposure across the various types of risk taken and (b) fully leverage the benefits of an integrated risk management program.

"Economic capital" is defined as the amount of capital that is sufficient to adequately protect shareholders against default from all but extreme loss events. The calculation is based on an analysis of all risks to which the firm is exposed. Economic capital measurement methodologies range from simple standardized factor models to highly sophisticated statistical models.

For financial services firms, risk taking is their central business proposition – taking credit risk, market risk, liquidity risk and operational risk in providing financial services and products such as loans, deposits, investments and insurance. Economic capital provides a "common currency" across all types of risk. With economic capital, financial services firms can calculate risk-reward tradeoffs among strategic alternatives, price their products to adequately compensate for the risks undertaken, and set return standards to guide decisions to invest in new businesses, services and products.

The importance of economic capital, and its role in ERM, is expected to increase with the recent adoption of the Basel II Accord by the Basel Committee on Bank Supervision, an international consortium of bank regulators. More than 100 nations have agreed to the provisions of this accord, which mandates a range of economic capital measurement methodologies as well as risk management practices consistent with the precepts of ERM. Even though U.S. bank regulators are requiring only the largest banking organizations to adopt the Accord (restricting compliance to only the most sophisticated requirements of the Accord), there is a common recognition among the broader financial services industry that the Accord represents "best practice" for risk management. Basel II will also apply to some large investment banking firms.

123. How is continuous improvement applied to risk management?

Because continuous improvement applies to risk management just as it applies to any other process, ERM should be viewed as a systematic approach to building and improving risk management capabilities. Continuous improvement is vital to successful risk management because facts and circumstances are constantly changing over time, which means risks and management's assumptions about the environment can be expected to change over time. The question is, how is continuous improvement applied to risk management?

Management can expect the monitoring process to identify opportunities to improve risk management capabilities. However, there are other ways in which continuous improvement of capabilities is stimulated. Several examples follow:

A continuous improvement process supported by clearly stated policies, methodologies and tools and emphasized consistently across the organization is an effective catalyst for improving ALL processes, including risk management processes. Once the organization has determined the desired capabilities for managing a given risk or group of related risks and has successfully implemented those capabilities, it must be ever vigilant about improving them continuously as facts and circumstances change and the risk of significant external and internal events occurring in the future evolves. A "learning organization" can never afford to rest in the dynamic global marketplace.

An enterprise risk assessment process and gap analysis facilitates the identification of the priority risks and highlights unacceptable gaps in the capabilities around managing the priority risks. These activities lead to

focused risk responses which drive improvement in risk management policies, processes, competencies, reports and technology. See further discussion in Question 85.

Benchmarking compares risk management capabilities within business units, risk units, support units and assurance units (see Question 56 for an explanation of these terms) to the capabilities of peers or "best of class" performers. The better defined an organization's capabilities, the more likely an effective benchmarking process is in place. It is especially effective when the board and executive management sets or approves the priorities for benchmarking and is briefed on the results of the process. Benchmarking data can also be a catalyst for change when it is communicated to appropriate process owners and risk owners.

Four-way communications and knowledge sharing consists of the processes and supporting technologies by which there is a continuous transfer and exchange of information about risk and risk management capabilities up, down and across the enterprise. Facilitated by executive management, this four-way information exchange provides insights into the existence, nature, significance, likelihood, acceptability and manageability of risk as well as the organization's risk responses, measurement methodologies, control activities and monitoring processes. This ongoing exchange facilitates the sharing of best practices and identifies conditions that must be acted upon. It is a powerful catalyst for stimulating continuous improvement.

Employee learning assists managers throughout the enterprise in building awareness and achieving buy-in and ownership of the company's risk management vision, goals, objectives, policies and processes. Employee learning should emphasize the following areas:

- The enterprise's risk management vision, goals, objectives and policies
- The company's common language and other enabling frameworks
- The company's processes for identifying and sourcing risk and the methods and tools supporting those processes, including how those processes compare to the COSO Enterprise Risk Management – Integrated Framework
- The self-assessment processes in place and how they are integrated with day-to-day business activities
- The risk measurement methodologies selected by the company and how they are used
- The organization's priority risks and the enterprisewide risk assessment process for keeping the risk profile up-to-date
- The elements of ERM infrastructure and their importance and contribution in building and improving risk management capabilities
- The process by which gaps in risk management capabilities are determined
- Participation in established communications channels to enable the flow of risk management information within the enterprise
- The company's commitment to continuous improvement and what it means to risk management, to the enterprise's operating units and to the individual employee

Education and learning programs should be designed to address the above points and delivered to appropriate personnel.

Monitoring of implementation of improvements follows the identification and prioritization of improvement opportunities and development of action plans. Improvement efforts are tracked against established timetables and checkpoints. Audit activities (e.g., internal audits, risk compliance activities, external audits or regulatory audits) can provide assurances that improvements are being made in a timely manner. However, it is up to management to take the initiative to act on the results of continuous improvement activities, hold the responsible personnel accountable for follow-up and monitor the actions taken.

124. What are the synergies and differences between ERM and "quality initiatives" (e.g., Six Sigma, Lean, TQM, etc.)?

ERM is an enterprise-level process that is integral to strategy-setting. Quality initiatives, on the other hand, provide the methodology and tools to help organizations understand, measure and continuously improve the efficiency and quality of their processes at a detailed level. For example, the Six Sigma approach is based on the following activities – Define, Measure, Analyze, Improve and Control. These activities support and provide input in an ERM process. They provide detailed process-level information that must then be evaluated within the larger context of the enterprise to develop a portfolio view of risks and controls. ERM, on the other hand, must be applied in strategy-setting, or else its application becomes too detailed and cumbersome.

Quality initiatives can be viewed as methodologies, techniques and tools for application at a detailed process level to address specific process objectives. The operation of a quality program is a "control activity" (one of the components of the COSO Enterprise Risk Management – Integrated Framework) with measurable indicators of performance.

For example, the Six Sigma process can effectively augment the implementation of ERM in several ways:

- Six Sigma resources can be valuable in helping the ERM implementation team understand the current operating environment. The use of process classification schemes to decompose the business, the identification of key business processes, the sourcing of value drivers and other steps are integral to understanding the Internal Environment component of ERM.
- Six Sigma frameworks and skill sets can be especially useful in understanding risks that are operational in nature, including development of a current and future state gap analysis. This can be complementary to or replace certain ERM frameworks, such as the six elements of infrastructure and capability maturity model.
- Six Sigma resources can serve as a reference in understanding the interrelationships among risks, e.g., independent risk factors as well as risk factors dependent on other risk factors.
- One area in which Six Sigma can provide significant value is in risk response planning and analysis, e.g., the identification of risk owners, the sourcing of risks within key business processes, the gathering of a "current state" inventory and the analysis of the "future state" gap.
- Six Sigma places emphasis on identifying process-level performance indicators; these indicators should be translated into key risk indicators to understand the exposures to performance variability and potential loss drivers.

There are also challenges when integrating Six Sigma and ERM. The focus of Six Sigma tends to be driven by an operational perspective, sometimes leading Six Sigma proponents to lose the "big picture" linkage to strategy. In addition, it is important to maintain objectivity and impartiality during the risk assessment process. The management team should prioritize risk with the Six Sigma and ERM teams providing appropriate insight without steering the direction of risk rankings in any particular direction. Another issue is one of perception. If management sees Six Sigma personnel involved in the risk assessment process, it may send conflicting messages. An enterprise risk assessment should not be viewed as an exercise to drive a review of business processes and the related controls. An enterprise risk assessment should focus on strategic issues, with the emphasis on processes driven by the gap analysis around the priority risks.

TAKING IT TO THE NEXT LEVEL – ENHANCING CAPABILITIES

125. What steps does management take to enhance risk management capabilities?

Once companies have implemented risk management capabilities that are well-defined and consistently applied across the enterprise, they are positioned to enhance the process to address specific needs of the business. The steps required to enhance risk management capabilities apply to those priority risks for which management has decided to attain a "managed" or an "optimized" state of capability using the capability maturity model (see Question 111).

There are three steps to take when enhancing risk management capabilities. These steps are ***quantify risk enterprisewide***, ***improve enterprise performance*** and ***establish sustainable competitive advantage***. These steps may be taken concurrently. Representing the cutting-edge, these steps conclude the progression towards an ERM solution. The possible elements to consider when enhancing capabilities provide insight as to the ultimate direction of the ERM journey.

Following is a summary of examples of possible elements to consider when enhancing risk management capabilities:

ENHANCE CAPABILITIES

	Quantify Risk Enterprisewide	Improve Enterprise Performance	Establish Sustainable Competitive Advantage
Does the Entity Have:	The ability to measure risk or groups of related risks quantitatively and aggregate them at the enterprise level?	The ability to use risk management to demonstrably improve enterprise performance?	The ability to use risk management to establish sustainable competitive advantage?
Possible Capabilities:	■ Risk quantified to greatest extent possible ■ Better anticipation of losses through time-tested models ■ Established aggregate risk tolerances and limits allocated to operating units ■ Corrective actions taken when pre-defined limits are exceeded ■ More realistic business plans and forecasts with focused management of performance variability ■ Improved capital allocation to cover risks undertaken ■ Improved understanding of interrelationships among key risks ■ Measure and evaluate risk-adjusted performance ■ Focused risk avoidance, acceptance, reduction and sharing decisions	■ Improved understanding of how alternative risk responses impact business performance ■ Best practices routinely identified internally and externally, and shared across the enterprise ■ Organized efforts made to remove inefficiencies ■ Integration of risk measures with key performance indicators ("balanced scorecard") ■ Evaluation of risk appetite versus capacity to bear risk ■ Specific measures of success defined and monitored ■ Continuous improvement mindset fully embraced in risk management ■ More risk-sensitive and risk-aware culture	■ Risk-taking activities and control mechanisms are in balance ■ Designated risk units for evaluating and managing strategic risks ■ Risk responses determined on an enterprisewide basis ■ Seamless integration of risk management with business planning and value management ■ Risk responses tightly integrated with business strategy ■ Diversification effects across multiple risk types is understood and exploited ■ Appropriate risks are opportunistically viewed and confidently accepted ■ Risk taking (exploitation) is aligned with core competencies ■ Improved risk reporting to investors
Value Proposition:	■ Anticipate and manage risk better than competitors ■ Capital deployed more efficiently at lower cost ■ Reduced transfer and other costs	■ Improved trade-offs of return, risk and capital ■ Costs reduced below those of competitors ■ Highest confidence of board/senior management in risk management capabilities	■ Managed exploitation of risks to capitalize on market opportunities ■ Intrinsic value of company understood and appropriately valued by the market

The aforementioned examples of enhanced risk management capabilities are intended to be illustrative and not all-inclusive. Not all elements suggested in this publication for enhancing risk management capabilities need be selected when designing an ERM solution.

126. How does management decide on the appropriate enhancement capabilities?

With respect to enhancing risk management capabilities, it is a matter of judgment, culture, operating style, organizational needs, management's desired capability for managing specific risks and the nature of the risk. What works for one organization will not necessarily work for another organization. One important factor to consider relates to market and investment community expectations. Whether it is institutional investors, rating agencies, regulatory authorities or the standard set by competitors, management should factor these expectations into their decisions regarding the appropriate level of investment in enhanced risk management capabilities. In essence, enhanced capabilities are intended to deliver against market expectations and demands.

127. What is a "portfolio view" of risks and how is it practically applied?

Taking an entity-level portfolio view of risk when formulating risk responses is the essence of an enterprisewide approach. According to COSO:

> Risks in different units may be within the risk tolerances of the individual units, but, taken together, the risks might exceed the risk appetite of the entity as a whole, in which case additional or different risk response is needed to bring risk within the entity's risk appetite. Conversely, risks may naturally offset across the entity where, for example, some individual units have higher risk while others are relatively risk averse, such that overall risk is within the entity's risk appetite, obviating the need for a different risk response.

A portfolio view makes sense for activities directed at achieving a common enterprisewide purpose. There are several reasons why:

- ***Risks add up whether evaluated piecemeal or in total***: If risks are aggregated, managers are positioned to understand whether they are increasing or decreasing as conditions change, both relative to each other or in the aggregate versus the organization's risk appetite. While aggregation can present challenges from a technical standpoint, very little perspective is gained from examining gross versus net effects, or smaller exposures in isolation. A portfolio view is powerful because it can alter management's focus and allocation of resources. For example, it enables the organization to quicken its response time in addressing favorable opportunities or adverse changes in the environment. Acting on a portfolio view at the enterprise level gives management greater leverage, lower transaction or operating costs, and the ability to streamline and optimize operations as well as to plan contingent risk responses.
- ***Increased efficiency and better decisions***: A portfolio view provides the quantitative means to share and avoid risk. Sharing of risk, for instance, is more efficient when risks are netted or offset. For example, currency exposures can be pooled to determine the company's "net" exposure – when that practice corresponds with the organization's operations. When exposures are pooled, they form a portfolio that more accurately portrays the realities of the business. The goal, ultimately, is to evaluate total returns relative to total risks leading to more informed decisions. This "total risk focus" leads to increased confidence that management is making decisions based on a comprehensive view of the business.
- ***Improved reporting and capital allocation***: Analyses that are performed to identify the relationships between and among risks and their key drivers so that risks can be aggregated lead to more robust risk reporting. They help managers make better choices when allocating capital to those business activities providing the greatest prospects for attractive returns relative to all risks undertaken, and disallowing those activities that do not. The alternative is ineffective, intuitive guesswork, which will not get very far given the complex interrelationships among risks and the key variables affecting them.

- ***Simplicity***: If executives can effectively communicate the risk profile and health of the organization, they have a device that everyone can understand and apply. A portfolio view is a way of summarizing a complex set of relationships, i.e., the activities in the enterprise. The greater the ability to express in simple terms the organization's state of affairs, the greater will be the ability to effectively manage its course in an increasingly competitive marketplace.

Achieving a portfolio view is not easy. Some risks are more susceptible to rigorous measurement than others. COSO points out that a portfolio view may be obtained by focusing on major risks or event categories across operating units or on risk for the enterprise as a whole using such metrics as risk-adjusted capital or capital at risk. COSO explains that such "composite measures are particularly useful when measuring risk against objectives stated in terms of earnings, growth or other performance measures, sometimes relative to allocated or available capital." COSO suggests that such metrics can provide information useful in reallocating capital across business units and modifying strategic direction. To illustrate, COSO provides the following example:

> [A] manufacturing company…takes a portfolio view of risk in the context of its operating earnings objective. Management uses common event categories to capture risks across its business units. It then develops a graph showing, by category and business unit, the risk likelihood in terms of frequency on a time horizon, and the relative impacts on earnings. The result is a composite, or portfolio, view of risk the company faces, with management and the board positioned to consider the nature, likelihood, and relative size of risks, and how they may affect the company's earnings.

COSO provided a second example in the framework:

> [A] financial institution calls on business units to establish objectives, risk tolerances and performance measures all in terms of risk-adjusted return on capital. This consistently applied metric facilitates management's rolling up [the] units' combined risk assessments into a portfolio view for the institution as a whole, enabling management to consider the units' risks, by objective, and consider whether the entity is within its risk appetite.

In addition, reference is made to pages 60 through 62 of the Application Techniques for additional examples provided by COSO. One of the important advantages of a portfolio view is the ability to consider whether risk is within the entity's risk appetite. A portfolio view enables management to reevaluate the nature and type of risks it wishes and is willing to take. In cases where the entity shows risks significantly less than the entity's risk appetite, management may decide to incent individual business unit managers to accept greater risks in targeted areas, striving to enhance the enterprise's overall growth and return.

128. How does management quantify risks enterprisewide?

Aggregation of multiple risks is not the end result, but rather is the means to a desired end. From an enterprise perspective, the "desired end" is effective enterprisewide risk responses integrated with the business strategy that lead to improved performance. When evaluating whether realization of this objective justifies the effort in collecting and analyzing risk information, management must ask the question, "At what level are risks aggregated for quantification purposes?"

Choosing the right level of aggregation for a risk or group of related risks often depends on who will be using the measure. For example, operational level employees, such as traders, inventory control managers or marketing managers, need very specific information to execute their jobs. When taking an enterprisewide view of multiple interrelated risks, the organization's goals must be defined in terms of an aggregate measure for the group of related risks. When the aggregate measure is determined using a robust measurement methodology, it is possible to drive decision-making and manage the group of risks on an entity-wide basis affecting such things as performance incentives, cross-unit cooperation, cross-functional teamwork and enterprisewide knowledge sharing.

Another key factor influencing a decision to aggregate multiple risks is that it only makes sense to aggregate when the components included in the measure are directed towards the same common goal. If an organization's operating policy is to manage autonomous operating units, with each one a standalone profit center, then it may be inappropriate to develop an aggregate measure for common risks within these units. In

such circumstances, management has elected not to implement risk responses across operating units; therefore, having aggregate measures for key risks across the units is pointless in most circumstances. On the other hand, a bank holding company with multiple subsidiaries operating as separate profit centers may want to aggregate credit risk, enterprisewide, because it makes good business sense to do so. In essence, ERM is about (1) aligning enterprisewide goals and operating unit incentives and (2) delineating risk management tasks that must be executed centrally from tasks that must be executed locally. With effective alignment of objectives and incentives and clear delineation of responsibilities, aggregate risk measures are more effectively deployed.

There are several ways to aggregate multiple risk measures using a combination of a rigorous methodology and the application of judgment. The entity's navigation of the ERM journey will lead to other approaches.

- ***Risk-pooling approaches***: We suggest aggregation of risks whose interrelationships are well understood within logical families or pools. Using this approach, the entity first determines the interrelationships among its key risks. Risks are either positively or negatively correlated when they have common risk drivers. Otherwise, they are uncorrelated. Management then "pools" the different risks to assess the alternatives for managing the collective risks represented by the pool. The pooled risks could be managed as a portfolio. Alternatively, a hedge based on an aggregate index, such as a broad stock, bond or commodity index, could be used (as opposed, for instance, to hedging the individual component risks separately). If risks are insurable, subject to the availability and pricing of insurance products, it is often cheaper to hedge the entire pool of risks than to insure each risk separately. In the case where the exposures in the portfolio are uncorrelated, the net cost of transferring them to an independent party, such as through hedging or insurance, may be less due to the benefits of diversification.

- ***Enterprisewide risk appetite and specific risk tolerances***: Unbridled risks can result in excessive performance variability and unacceptable loss exposure. One method for achieving consistency of performance is articulating risk appetite for the entity as a whole, as envisioned by COSO's definition of ERM. In effect, risk appetite addresses the question, "How much variability are we willing to accept and how much loss are we willing to absorb as we pursue our overall business objectives and execute our strategies?" Guidance on this question is important as it helps management assess the exposure in terms of the acceptable downside risk as the company seeks the upside inherent in executing the business strategy. If a CEO is willing to bet the company in pursuing an acquisition, is the board willing to accept that level of risk?

  While enterprisewide risk appetite is a strategic assessment, it must be translated into specific policies to clarify the boundaries within which managers may operate and pursue opportunities. It may also be used as a context for establishing risk tolerances and limit structures to set the boundaries of acceptable risk that may be undertaken at individual units and in conjunction with specific activities. As managers pursue opportunities for growth and new sources of profitability, risk tolerances and limits are an effective tool, in combination with a methodology for aggregating risk measures, for countering "succeed at all costs" pressures on managers to produce expected results. Enterprisewide risk tolerances and limits should be sufficiently broad to permit operational flexibility, but at the same time ensure that the aggregate risk profile of the firm remains within management's risk appetite, as approved by the board. These tolerances and limits can be communicated in many ways. For example, they can be incorporated into the risk management policy statement made available to all managers and key employees.

- ***Hurdle rates***: While certainly not a new idea, organizations often set "hurdle rates" to screen capital projects when using discounted cash flow (DCF) techniques. This screening is a starting point for assessing the relative merits of multiple capital projects more systematically. It provides increased assurance that any project selected can be expected to generate returns at least equal to, if not exceeding, the cost of capital. There are issues to consider, however.

  - Sole reliance on and rigid application of financial models can cause entities to overlook difficult-to-quantify factors vital to sustaining competitive advantage, such as product innovation, quality, reputation and technological leadership.
  - It is not unusual for companies to set hurdle rates arbitrarily far above the cost of capital, leading to underinvestment. Some would argue that a "good" project is one that provides a return greater than the

cost of capital. On the other hand, the projection of expected cash flows isn't an exact science, so a higher hurdle rate raises the bar. The question, then, is how much higher? Admittedly, a high bar eliminates from consideration projects management would never approve anyway. But it can also screen out viable projects that should be considered. Part of the answer to this issue lies in the company's risk tolerance. The lower the risk tolerance, the higher the hurdle rate must be over the expected cost of capital. After incorporating its risk tolerance and margin for estimation error, management should be careful about setting the hurdle rate any higher, otherwise underinvestment may result.

- Hurdle rates must not be used as a hard and fast rule across all projects. If management has a single hurdle rate for the entire enterprise, the DCF model will not take into account appropriate project risks. While admittedly subjective and difficult to do, hurdle rates should be set on a project-by-project basis or at least on a business unit or divisional basis to reflect the different risk profiles. For example, in a business where the primary strategy is growth, projects with lower net present values are probably more acceptable than they would be in a business with a cash generation strategy. Companies should still take on their most attractive capital projects first and recognize that the cost of capital for subsequent projects, e.g., "maintenance" projects needed to sustain the implementation of existing strategies, might not be the same as the cost for their primary investment projects.

  Hurdle rates are not infallible. They cannot remain fixed over time as economic conditions change. In addition, potentially marginal investments can often be made to appear attractive as internal business units compete for capital.

- ***At risk frameworks***: Value at risk (VaR), earnings at risk (EaR), gross margin at risk (GMaR) and cash flow at risk (CFaR) methodologies are becoming more accepted by corporate enterprises and regulators as tools for: facilitating the allocation of capital based on risk; measuring performance taking into account the risks inherent in a portfolio; and strengthening the links between performance, accountability and established risk thresholds. These methodologies assist managers in considering critical factors when managing risk, e.g., the sensitivity of existing portfolio positions to market rate changes beyond specified limits, the liquidity of a portfolio, the contribution of each unit or product to both risk and return, and the interrelationships between risks. All told, these techniques help managers consider the exposure of earnings or cash flow to loss and achieve the entity's target leverage and desired return on allocated capital. They also facilitate formulation of forward-looking guidance.

- ***Risk-adjusted performance measurement***: Once an organization has quantified its exposures, such as by using a technique like VaR, what does management do with this information? One of the most meaningful uses of risk information is as a factor for adjusting the relative value of different business activities. Risk-adjusted return on capital is a technique incorporating the riskiness of a business activity, such as an investment, into the measurement of the expected returns from that activity. Hence, a more risky investment (say, an investment in a power plant operating in a developing foreign country) would have to generate a higher return than a less risky investment (say, U.S. treasuries) in order to be considered equivalent. Risk-adjusted return on capital, or RAROC, incorporates the cost of financing this risk into the measurement of performance. It tells management just how much greater the return would have to be, given the level of risk. It also provides insights to management as to whether the allocated capital is adequate to cover the risks undertaken.

  As with any technique, there are issues with respect to RAROC. Since there is no one correct way to compute the expected riskiness of a project or to adjust for risk, the precise number one gets will depend on the approach one takes in the computations. Using RAROC, risk is quantified based on probability distributions of returns observed in historical data, consistent with VaR and other statistical models. The intended result is to aggregate price risk and allocate capital based on the variability in expected returns. Thus RAROC provides a means of evaluating return, risk and capital trade-offs and comparing performance across different units or activities of the organization, which are subject to different levels of risk. RAROC is also a tool that can be useful in creating benchmarks for the organization. The power of RAROC, therefore, lies in consistency of application. A RAROC approach adjusts returns for the capital at risk across asset classes. Managers can then use that information to establish limits on trading, investing or other business activities.

This discussion of risk aggregation is not intended to suggest that companies should seek out the "holy grail" of risk measurement. There are practical limitations to measuring risk because risk, by nature, is about uncertainty in facing the future. The purpose of risk aggregation methodologies is to establish a common basis for organizing the array of information that managers need as they make critical choices. Therefore, the goal is to provide better information for decision-making through enhanced risk measurement capabilities. These enhanced capabilities achieve four things:

(1) More robust risk reporting – Risks are aggregated at multiple levels – by business unit, product or geography (aggregating multiple risk types), by risk (aggregating the same risk on an enterprisewide basis across all business units) and by specific investments and projects.

(2) Greater investment confidence – With enhanced risk measurement capabilities, the organization can pursue opportunities with greater confidence knowing that it understands the risks inherent in its normal future operations and that those risks are being managed effectively.

(3) Greater integration and alignment – As aggregate measures are effectively linked to enterprise performance, more integrated risk responses are possible.

(4) Higher valuation – All of this gives management a more compelling story to communicate to investors, which in turn may lead to higher price/earnings multiples in share valuations.

129. How does management use ERM to improve business performance?

The most important contribution of ERM to improving business performance is to help managers make better choices in protecting and enhancing enterprise value. Because companies face an increasingly uncertain future, this contribution can make or break the formulation and execution of a successful business strategy. Risk responses should support the organization's value creation objectives by managing and monitoring the performance variability inherent in its future operations, protecting accumulated enterprise value from unacceptable losses and leveraging existing core competencies to pursue market opportunities.

When managing enterprise value, organizations must develop an understanding of the sources and drivers of value using the business objectives and strategy as a context. This understanding provides the context for managing risk. As senior managers focus their attention on the enterprise's long-term prospects for generating superior returns, they must:

(1) Evaluate the key underlying variables in the business plan that are exposed to performance variability and that require specific risk responses;

(2) Understand the loss exposures or drivers inherent in the enterprise's business model that require specific risk responses; and

(3) Identify incongruities inherent in the business model where management has, either knowingly or unknowingly, accepted risks that should be avoided, given the entity's risk appetite.

ERM's focus on the critical risk management tasks – identify events, assess risk, formulate risk response, implement control activities, inform/communicate and monitor – provides a flexible framework for addressing these three strategically important issues. Failure to manage the enterprise's exposures to potential future events that can destroy value will reduce even the best-laid plans for creating value to waste.

To identify value drivers (or key underlying variables) effectively, a context is useful. For example, shareholder value is a generally accepted measure of value and is, therefore, an example of a useful context for defining enterprise value. Economic Value Added (EVA) is an example of such a measure. Other examples providing a context for defining value drivers inherent in the business model include business objectives and strategies, key performance goals and key success factors linked to value creation. Value drivers can be linked to the variables that influence the achievement of the business plan, e.g., they may be defined in terms of the key underlying variables that cause revenues and expenses to go up and down.

Once the key value drivers are defined, key performance indicators are developed. These KPIs translate concept into action in the business plan, as they are the metrics by which performance against plan is evaluated and ultimately rewarded. KPIs are converted into reports and are used to monitor performance over time. Managing and monitoring the business will surface opportunities to improve processes, products and services to enhance enterprise value.

There are several issues to consider when applying ERM to improve business performance. To illustrate, EVA is a useful framework for measuring corporate performance that takes into account a capital charge reflecting the total cost of capital deployed in the business. This framework is used to establish accountability of managers for creating value. The basic formula for calculating EVA is as follows:

EVA = *NOPAT* less *WACoC*,

Where, *NOPAT* is Net Operating Profit After-Tax and *WACoC* is Weighted-Average Cost of Capital.

There are at least four ways to increase enterprise value under the EVA framework:

- ***Create new opportunities***: The enterprise invests in new business activities promising attractive returns that are expected to exceed the *WACoC*.
- ***Improve performance***: The enterprise improves performance and increases returns of existing business activities by improving policies, processes, competencies, reporting, technology and/or knowledge in ways that achieve this desired result.
- ***Harvest existing value***: The enterprise withdraws from existing business activities generating inadequate returns, i.e., these activities have generated (or are expected to generate) returns that do not exceed the *WACoC*.
- ***Adjust and align cost of capital***: The enterprise takes specific steps to reduce *WACoC* and/or ensure risks taken are consistent with the enterprise's risk appetite.

By applying an ERM perspective, we can identify several opportunities for enhancing risk management processes to improve business performance using the application of EVA, as described above, as a context:

- ***Create new opportunities***: *NOPAT* only reflects expected losses that are reasonably estimable. Unless specifically adjusted for risk, an overall *WACoC* ignores the relative risks inherent in individual business units and activities. To address these inherent risks, management should insist that the methodology used to calculate EVA considers the risk equivalency of alternative activities. Under ERM, a process must be in place to identify the primary risks inherent in individual business units and activities.

  Every successful business takes risk in the pursuit of value-added opportunities. For example, when management decides to enter new markets, introduce new products, acquire another entity or exploit other market opportunities, inherent in these decisions are choices to take on additional risk. When risk management is integrated with strategy-setting, these choices are transparent because directors and executive management have full knowledge of the consequences of taking risk. That knowledge is a result of the organization's efforts to understand, monitor and track risk during the strategy-setting process. Under ERM, a process is in place to identify the priority risks inherent in management's planned actions and price the acquisitions, transactions and deals resulting from those actions to appropriately compensate the enterprise for the risks it is assuming. Failure to make this assessment may result in management committing to undertake activities in which there are significant undesirable risks that exceed risk appetite, i.e., unacceptable performance variability, loss exposure and/or business model incongruities. The objective is to fully understand the good things that can happen, the bad things that can happen and the various scenarios in between.

  In addition, following the consummation of acquisitions, transactions and deals, a process is in place to monitor the risks and mitigate them if they are subsequently determined to be different than originally contemplated by the strategy. Effectively integrated with strategy-setting, risk management should invigorate opportunity-seeking behavior by helping managers develop the confidence that they truly understand the risks and have

the capabilities at hand within the organization to manage those risks. The result: Management and the board fully understand the downside and how much it might hurt. They also know what to watch over time.

Given the future is unpredictable, management should determine that the enterprise has allocated sufficient capital to provide a cushion for unexpected or unknown extreme losses incurred by individual activities. Herein lies a logical connection between ERM and value creation. If there were no risks, there would be no need for equity capital. Thus, equity capital is the price of exposure to uncertainty. If there were no exposure to uncertainty, every organization would be able to fund their activities with AAA bonds. Since this fantasyland does not exist in the real world, equity capital is needed to cover unexpected risks. Anything that can be covered by traditional insurance or with insurance-like structures becomes more certain if the insuring counterparty has an outstanding credit rating and there is an absence of legal loopholes clouding the settlement process. In such conditions, the need for equity capital may be reduced. What's the point? Because the board and CEO must ultimately assume responsibility for allocating capital effectively, a risk assessment can be useful in differentiating risk profiles by unit, activity or project.

- ***Improve performance***: A robust, comprehensive risk assessment of a given business unit or activity may identify priority risks that expose future revenue streams and cash flows to unacceptable performance variability or loss exposure. Once a consistent risk assessment framework is implemented enterprisewide, comparison and aggregation across the operating and support units become possible. Capital allocation becomes more meaningful and investment choices become clearer. A more robust risk assessment process reduces the chance of overlooking key risks and incurring unacceptable opportunity costs due to risk-averse behavior. Risk responses can then be evaluated to reduce the priority risks to an acceptable level. In making such assessments, identification of potential events or scenarios may provide useful insights as to the soft spots in the enterprise's or unit's business strategy as well as opportunities to improve performance.

- ***Harvest existing value***: Decisions to exit a market or geographic area or to sell, liquidate or spin off a product group or business must be evaluated carefully. Managers need to understand the "relative riskiness" of different units, geographies, products or markets. If performance is measured without considering the risks assumed by managers in generating returns for the enterprise through their respective activities, an exit decision could result in withdrawal from a business that is generating superior risk-adjusted returns, even though its gross returns, unadjusted for risk, may appear lackluster relative to other activities. The analysis supporting this assessment could be as simple as a risk map prepared for each business unit or as sophisticated as deploying risk-adjusted performance measurement. Furthermore, management must assess during strategy-setting the consequences of taking action to mitigate one risk, as that action could create another risk. An effective risk assessment will facilitate an evaluation of alternatives.

- ***Adjust and align cost of capital***: Under EVA, this step is a difficult one to take in a way that results in a substantive change that really makes a difference. One reason is that WACoC is more relevant to the enterprise's specific units and activities than it is for the enterprise as a whole, if those units and activities have unique risk profiles. Companies may get around this issue by assigning different units with a specific WACoC relevant to their specific activities, based upon benchmarks from a market-based surrogate such as a specific public company or a group of companies with the equivalent activities and risks. If a business unit engages in high-risk activities, its cost of capital should be higher than lower-risk businesses. If its activities are low risk, the enterprise's cost of capital invested in the unit should be correspondingly lower. Market valuations at the corporate level often do not provide sufficient transparency as to the risks undertaken by different units and activities.

  During the strategy-setting process, companies that are serious about risk management strive to configure their risk taking with their core competencies, or what they do best, avoiding unduly constraining risk-averse behavior. The business model of every successful organization exploits to the maximum extent possible the areas in which the company excels relative to its competitors. In leveraging these advantages, however, management needs assurance that the company is not gambling its future. An ERM infrastructure (as discussed in Questions 37 and 56) provides the discipline, focus and control by which management (a) capitalizes on competitive strengths while protecting enterprise value, and (b) ensures the company only

takes those risks it is best equipped to handle within the parameters of its risk appetite, while minimizing exposure to those areas considered "off-strategy" because of the lack of competence to manage.

In summary, the linkage of ERM to improved enterprise performance is achieved in different ways. By evaluating the effects on business performance of changes to a firm's risk profile from implementing alternative risk responses, management is able to focus on improving the expected return for the enterprise as a whole, or alternatively holding the expected return constant and altering the organization's risk characteristics. Management alters an entity's risk characteristics by reducing:

(a) The enterprise's net exposure;

(b) The variability of the enterprise's expected returns caused by specific sources of uncertainty (such as exposure to fluctuating currency rates);

(c) The likelihood of financial distress in the event of realized changes in key variables (such as changes in interest rates for a highly leveraged company); or

(d) Other uncertainties in the attainment of expected returns.

In effect, improving business performance arises from integrating risk management with strategy-setting. Such integration means two things. First, it means the risk profile of strategic decisions is evaluated early in the strategy-setting process, leading to a more robust business strategy. Second, it means that policies, procedures, measures and monitoring are established and continuously improved to provide assurance to management and the board that the company is on target with achieving its expected return while controlling its accepted exposure to risk. These two aspects of an integrated process lead to a stronger focus on improving business performance. The bottom line is that the organization only "learns once" and shares knowledge and experiences so that risk management capabilities are continuously improved and exposure to unacceptable risks and strategic error is reduced.

130. How should we integrate our ERM approach with our strategic planning process?

One way is to integrate specific ERM capabilities with the various phases of the strategy-setting process. This thinking is illustrated below:

PHASE OF STRATEGY-SETTING	EXPLANATION OF STRATEGY-SETTING PHASE	EXPLANATION OF ERM COMPONENT TO INTEGRATE WITH STRATEGY-SETTING
Strategic assessment	Attain a general understanding of the organization and its operating environment	*Internal environment*, *event identification* and *risk assessment* all contribute significantly to this phase, which includes conducting a comprehensive enterprisewide risk assessment and inventorying the current state of risk management capabilities to identify and source risk
Strategy development	Identify strategy alternatives, select the appropriate strategic activities to undertake and design improvements needed in the organization	*Risk response* relates to this phase because it entails the measurement of risk, the design of desired risk management capabilities and the evaluation of the impact of these capabilities on residual risk
Formulate plan	Articulate a comprehensive approach to implement the organizational design and specific activities to execute the strategy, including the definition of resource requirements and functional plans	*Control activities*, *information/ communication* and *monitoring* are complementary to this phase of the process as they address managing and monitoring of risk and provide an overview of the actions, metrics and milestones enabling the organization to close the gaps in its capabilities and achieve its objectives

In strategy-setting, management often focuses on selecting key value drivers by decomposing the drivers of value down to an appropriate level that is sufficiently granular to measure and manage. For example, under a shareholder value framework, share price is a function of earnings, management experience, investor confidence, the economic outlook and other factors. One of these variables – earnings – is a function of revenues, direct and indirect costs and taxes on pre-tax earnings. The drivers of revenue might include such factors as predictable volume, price competitiveness, customer liquidity, customer diversification, existence of entry barriers and an attractive industry providing room for additional growth. These factors are value drivers of revenue. They can be further decomposed. For instance, if predictable volume is a priority driver, we can determine additional drivers, e.g., an appropriately segmented market, scalable productive capacity and an effectively functioning distribution channel.

Once the drivers of value are defined at the desired level of decomposition, management selects the most critical drivers and defines the sources of uncertainty associated with each of those drivers. This can be accomplished by first prioritizing the value drivers based upon their contribution to the success of the business. Then, management selects the priority drivers for purposes of event identification and risk assessment. Thus the drivers of value provide a context for both strategy-setting AND risk assessment, which is why ERM should be integrated with strategy-setting.

131. Should we complete our strategic planning process prior to conducting our first enterprisewide risk assessment, or vice versa?

The intent of the ERM process is to incorporate risk appetite and risk management into strategy-setting. An enterprisewide risk assessment can help management determine whether there are risks that are inconsistent with or in excess of the organization's risk appetite. Because the environment is constantly changing, strategy-setting is a dynamic process that never ends. The same applies to risk assessment. Therefore, we do not believe management should ever formulate strategy without evaluating risk. If risk is not considered during strategy-setting, managers will naturally gravitate to the opportunities with the highest return regardless of the risk. Risk evaluation must be performed when strategy is developed, because the two processes enhance each other.

In those situations when a risk assessment is conducted after the business strategy is developed, the strategy must be reevaluated to consider important risks identified during the risk assessment IF such risks were not considered when the strategy was originally formulated. Business strategies often warrant revisiting once the risks inherent in those strategies are fully understood. Thus the entity's goals and objectives may be further refined when an enterprisewide risk assessment is conducted.

132. Is it possible to successfully merge together the risk assessments that companies perform as a result of ERM, Sarbanes-Oxley compliance, business continuity planning, internal audit and various compliance activities related to workplace, environmental and other regulations?

Yes, IF a common language and uniform process is deployed in performing those assessments. A point to remember, however, is that several of the areas noted in the question – Sarbanes-Oxley compliance, business continuity planning, workplace regulatory compliance and environmental regulatory compliance – represent specific areas, whereas ERM addresses the enterprise's total risk profile. Internal audit may perform either comprehensive or specifically focused risk assessments, and can assist in the merging of these multiple assessments across multiple areas, provided a common language and uniform process are used.

133. How does management use ERM to establish a sustainable competitive advantage?

When deployed as an integral part of the strategic management process, an ERM infrastructure can help management establish sustainable competitive advantage. Following are examples as to how:

- ***Integrate risk management with business planning and strategy-setting***: Integration with key processes, and in particular with business planning and strategy-setting, is a common theme in implementing ERM. COSO's definition of ERM includes a reference to "applied in strategy-setting." Effective risk management translates risk assessments into specific actionable risk responses, driving changes in control activities, information/communication processes and monitoring.

- ***Implement more rigorous risk assessment process***: Rigorous event identification and risk assessment enhances the quality of the assessments supporting strategy-setting and business plans. Once a consistent risk assessment framework is implemented and used across the enterprise by business units, support units, risk units and assurance units (see Question 56), comparison and aggregation across the enterprise become possible. Capital allocation becomes more meaningful and investment choices become clearer. A more robust risk assessment process reduces the chance of overlooking key risks and incurring unacceptable opportunity costs due to risk-averse behavior.

- ***Improve management of common risks across the enterprise***: Whenever there are common risks across the enterprise, there is an opportunity to share knowledge and best practices. A common language makes this possible.

- ***Improve capital deployment and resource allocation***: One objective of ERM is to optimize risk, return and capital. This objective leads to rigorous analyses to identify the relationships between and among risks and their key drivers so that risks can be aggregated to provide more robust risk reporting. These reports help managers make better choices when allocating capital to those business activities providing the greatest prospects for attractive returns relative to risks undertaken, and disallowing those activities that are not as attractive. The alternative is ineffective intuitive guesswork, which will not get managers very far given the complex interrelationships among risks and the variables affecting them. Therefore, improving returns via a superior capital allocation process is vital to an effective implementation of ERM. Management decides whether risk taking should be aggressive or in moderation relative to available capital and alternative risk–return opportunities.

- ***Configure the enterprise's risk taking with its core competencies***: Companies that are serious about their risk management configure their risk taking with their core competencies, or what they do best, avoiding off-strategy and risk-averse behavior. The business model of every successful organization exploits to the maximum extent possible the areas in which the company excels relative to its competitors. In leveraging these advantages, however, management needs assurance that the company is not gambling with its future. An ERM infrastructure provides the discipline by which management capitalizes on competitive strengths while simultaneously protecting enterprise value. In fact, ERM facilitates a company taking those risks it is best equipped to handle within the parameters of its risk appetite, while minimizing exposure to those areas which it considers "off-strategy" and lacks the competence to manage.

- ***Seize opportunities through rational assumption of risk***: At the highest level of capability, ERM helps companies understand their risks and risk management capabilities so thoroughly, that they can move rapidly to pursue opportunities that might be cause for trepidation in less sophisticated organizations. It is inevitable that every successful business must take risks. But risk taking should be wise and measured, and not cavalier. Risk management provides the transparency and assurance to directors and the CEO that risks are taken with knowledge – knowledge of the business, knowledge of the risks and knowledge of markets. That knowledge is a result of the persistent efforts of management to understand, monitor and track risk.

These are examples of how management uses ERM to establish sustainable competitive advantage. Formulation of an enterprisewide risk management strategy is something any organization can do at anytime regardless of how far it travels along the ERM journey. The important point is this: The enterprisewide strategy formulation process is more meaningful when risk measures are aggregated on an enterprisewide basis and management clearly understands how risk management improves business performance. That is why the step of establishing sustainable competitive advantage is the last one to take along the pathway to ERM.

Understanding and effectively managing the relationship between capital, risk and reward within the boundaries of an organization's risk strategy create a significant risk management opportunity. One approach for developing this capability is to evaluate the capacity to bear risk and the appetite to take risk, and allocate capital based on this analysis. The organization's risk appetite or willingness to take risk reflects both its capacity to bear risk as well as a broader understanding of the level of risk it can safely and successfully manage for an extended period of time. Risk appetite is the extent to which a firm is willing to expose its capital to the exploitation of strategic opportunities and retention of performance variability and loss exposure. It is further explained in Question 66.

Prudence and common sense are vital when evaluating risk appetite. For example, does it make sense to take all of the risk an organization is capable of undertaking without reserving capital for new investment opportunities? Is it appropriate to retain a significant risk when options for transferring that risk are available at reasonable cost? From a strategy standpoint, it may be useful to have a notion of the point at which the organization's capacity for bearing risk would be encroached upon.

BUILDING A COMPELLING BUSINESS CASE

134. How do we build a compelling business case for ERM?

Once the ERM vision and risk management objectives are defined and the relevant capabilities are selected, management is ready to prepare a business case to proceed. Risk management objectives address "the what." The business case is concerned with "the why" and articulates the ERM value proposition. The business case provides the economic justification for the overall effort to build and enhance the organization's ERM infrastructure and risk management capabilities. It includes a point of view as to what the ERM solution will look like (i.e., the selected capabilities), why the sponsoring organization must build the solution, the incremental value it expects from the solution and the projects necessary to make progress in realizing the expected benefits.

A sufficiently granular value proposition is not possible without knowledge of the organization's priority risks and the significant gaps around managing those risks. Question 85 discusses the importance of an enterprisewide risk assessment to obtaining this understanding. There can be many reasons to build and improve risk management capabilities. Each organization must make its own assessment of the expected benefits to justify the required investments in ERM infrastructure and the time frame in which those investments will be made. A business case documents that assessment and describes how the expected capabilities and the related benefits will be realized over time as the ERM solution is implemented.

The business case:

- ***Defines the ERM vision***: The business case reiterates the company's "shared vision" as to the role of risk management in the business. See Questions 64 and 65.
- ***Describes the overall effort***: The business case describes the ERM change imperative, i.e., it describes the change journey and the effort required to see that journey to a conclusion. As further explained in Question 85, an understanding of the priority risks and of the significant gaps around managing those risks is vital to effectively articulate the change effort.
- ***Analyzes the related costs and benefits***: Change under any circumstance is difficult to initiate, but unless the need to change is clearly understood, it will not happen. The business case details the ERM value proposition and provides a value impact analysis, including the measures of success. As further discussed in Question 4, a generic value proposition must be supplemented with a more granular articulation made possible by an enterprise risk assessment and a gap analysis around the entity's capabilities in place to manage its priority risks. The greater the gap between the current state and the desired future state of the organization's risk management capabilities, the greater the need for ERM infrastructure to facilitate the advancement of those capabilities over time. The business case must make this point clearly.
- ***Provides a context for monitoring progress over time***: The business case provides the business context for making the change to ERM. It sets forth the predefined success measures, which provide quantitative and qualitative targets against which to evaluate performance. A value impact analysis (see the next point) also provides a context for monitoring progress against the baseline projections and expected future net benefits. Success measures are important because they provide the means of knowing that the ERM solution "makes a difference." Examples of success measures are provided in Question 136.

- ***Explains the economic justification for going forward***: Executive management needs facts before committing to implementing ERM. The business case provides a quantitative and qualitative framework of the expected ERM benefits and costs for use by sponsors to obtain management approval to proceed. If feasible, a value impact analysis is provided, supported with a credible economic model that projects the expected net benefits resulting from the requested changes so project sponsors can make the most informed decisions as to whether or not to make investments in ERM infrastructure and risk management capabilities. Such quantitative analyses, if available, supplement the qualitative assessment. For example, will the ERM infrastructure improve the decision-making process on matters of significance to the enterprise as a whole and make it more cost-effective?

The business case supports executive management's commitment to move forward with the implementation process. While there are no hard and fast rules as to what the business case looks like, it must be defined at the top and managed with active participation and involvement from the top. The business case may be developed for the overall ERM journey or it may be developed for each major phase of the ERM journey. It is a "living document" that provides a road map for managing the overall effort against expectations. Therefore, it should be updated from time to time as the change journey progresses.

The business case development process builds stakeholder buy-in and commitment to the ERM change journey and assists management with achieving an understanding of the requirements for its success. When the sponsoring organization embraces critical aspects of the business case and is prepared to commit to build and test the capabilities that deliver the desired outcomes, the design and implementation process may begin.

The following schematic illustrates the key questions a business case must address:

Note that the COSO Enterprise Risk Management – Integrated Framework is used as the context for understanding the entity's "current state" as well as articulating its "future state." As discussed in Questions 110 and 111, the six elements of infrastructure and capability maturity model may also be used for analyzing gaps in capabilities around managing the priority risks.

The business case should be integrated with the journey management plan, as discussed in Question 137, for implementing the various ERM capabilities that deliver management's desired outcomes. It is important that the critical change issues are identified, understood and fully addressed.

135. How do we select the appropriate capabilities for our ERM solution?

It is a matter of judgment, culture, operating style, organizational needs and desired capability for specific risks. What works for one organization will not necessarily work for another organization. Management must decide on the capabilities that best meet the needs of the organization. Business risk management should become an integral part of the enterprise agenda.

Our advice when designing an ERM solution:

- ***Begin with risk***: Begin with an enterprisewide risk assessment and a gap analysis around the capabilities in place to manage the priority risks.
- ***Start somewhere, anywhere***: Begin with improving the capabilities for managing one or two key risks that management knows require improvements.
- ***Get out of the box***: Refocus the ad hoc, reactive and fragmented risk management activities of functions and departments operating as independent silos. Integrate these activities with a common risk management dashboard reporting capability.
- ***Think and manage strategically***: Integrate risk management with strategy-setting. Seek to understand the interrelationships between risks from a top-down enterprisewide point of view and, based on that understanding, organize risks into appropriate families and pools. Develop more integrated risk responses to skillfully apply appropriate analytical frameworks and measurement methodologies to each significant risk family or pool. Make sure someone owns the risks.
- ***Never be satisfied***: Practice a continuous improvement mindset.
- ***Remember, it is not rocket science***: COSO asserts that managers within an enterprise "should consider how they are conducting their responsibilities in light of the ERM framework and discuss with more senior personnel ideas for strengthening enterprise risk management." That is not a difficult process.

As introduced in Question 68, the eight steps for improving risk management capabilities, organized into three phases, provide guidance on the proper sequencing during the ERM implementation process. For example, when designing an ERM solution, the project team should ***set the foundation*** first, and then proceed to ***build risk management capabilities***. Effectively functioning capabilities then provide a basis for ***enhancing risk management capabilities*** over time. The more enhancement capabilities management puts in place, the more value-added the ERM solution and the greater the alignment of risk management strategy, processes, people, technology and knowledge.

The illustrated elements provided in this publication for each of the eight steps add to the enterprise's risk management capabilities and to the value proposition (benefits) of risk management. Accompanying every advance in risk management capabilities is a corresponding increase in the degree of sophistication and the extent of commitment required. Thus management must decide – consciously – just how far to go in systematically aligning the organization's strategies, processes, people, technology and knowledge through staged improvements over time.

As the organization progresses to the enhance capabilities phase, the degree of integration of risk management with strategic and operating processes increases. As noted in Question 85, the enterprise's priority risks and the significant gaps around managing those risks provide the context for deciding how far to take the ERM solution. The organization's business model and culture, the relative maturity of its existing risk management capabilities, the current initiatives funded and underway to improve capabilities, the degree of centralization or decentralization, the comparability of the risk profiles relating to different business units within the enterprise and other factors must be considered when deciding the level of maturity of the capabilities around managing the enterprise's priority risks.

When selecting the desired capabilities, management must recognize that ERM is a journey, not a destination. In Question 85, we introduced and explained five steps for getting started with implementing ERM:

STEP 1: Conduct an enterprise risk assessment (ERA) to assess and prioritize the critical risks. In this step, management understands the risks.

STEP 2: Articulate the risk management vision and support it with a compelling value proposition using gaps around the priority risks. In this step, management defines the direction.

STEP 3: Advance the risk management capability of the organization for one or two priority risks. Here is where management focuses the line of sight on closing unacceptable gaps.

STEP 4: Evaluate the existing ERM infrastructure capability and develop a strategy for advancing it. Through the ERM infrastructure, management establishes accountability and control over continuous improvement of risk management capabilities.

STEP 5: Update the ERA for change and advance the risk management capabilities for key risks. At this point, management broadens the focus.

When planning the desired capabilities to build and enhance in conjunction with Step 2 through Step 5 above, the suggested sequence of phases and steps introduced in Question 68 will provide insights as to where to begin and why. While there are no hard and fast rules, ERM is best achieved in stages beginning with the development of a common language and uniform processes. To illustrate:

- ***Set the foundation***: Once senior management is committed to explore the ERM value proposition, a working group of senior executives (a risk management executive committee [RMEC], for example), supported by a chief risk officer (or equivalent senior executive), is empowered to build and enhance the organization's risk management capabilities. These executives should be supported by a small, focused central staff function, such as a business risk management function. When chartering the RMEC and CRO, the CEO, executive committee and board of directors define the scope of ERM, e.g., what does "enterprisewide" mean and what are its implications? Working with the priority risks identified by the enterprise risk assessment and the significant gaps around the capabilities for managing the priority risks, the RMEC and CRO plan and coordinate the development of capabilities that close the unacceptable gaps. The organization's risk language and business process classification scheme provide a useful starting point for identifying and sourcing its risks. Other "Set the Foundation" elements are illustrated in Question 96.

- ***Build capabilities***: Based on the enterprise risk assessment and gap analysis, the RMEC identifies the areas that require the most attention. The current state of risk management capabilities related to the priority risks is formally documented to provide the baseline for identifying needed improvements. Risk ownership is assigned. Suggested elements to consider when building capabilities are illustrated in Question 103. The RMEC ensures there are clear accountabilities for managing the priority risks and identifies areas for achieving "quick hits" and successful results to build momentum for the ERM initiative.

- ***Enhance capabilities***: Once the foundation is set in the form of appropriate elements of ERM infrastructure and once capabilities around managing priority risks are in place, management decides on the necessary enhancements that are needed to accomplish the risk management vision and the related goals and objectives. Suggested elements to consider when enhancing capabilities are illustrated in Question 125.

Through this sequenced process of building and enhancing capabilities, management is able to put in place the ERM "building blocks" for the organization. Management should use the COSO ERM framework to benchmark the organization's risk management at various stages along the ERM journey.

136. What are the key success factors or measures of success when evaluating the effectiveness and impact of ERM implementation, i.e., how can we know whether an ERM approach has been successful?

The underlying premise for ERM is to help senior and operating managers make better decisions about how risks should be managed, enterprisewide. If good decisions are made, how do we know whether the decision would have been different had the entity's ERM process not been in place? On the other hand, if management makes a poor decision, how do we know whether a better decision would have been made had the organization implemented ERM? Would an ERM solution have made a difference in improving the decision-making process? Proofs are illusive on this score.

Following are examples of measures of success that companies have used:

- ***Integration of risk assessment into strategic and operating processes***: As managers make business risk an integral part of their agenda when they evaluate alternative deal structures, possible process improvements, new systems, new products and alternative markets, they become more anticipatory and forward-looking in their decision-making. An example is integration of risk management with the business planning and strategic management processes. Risk is assessed explicitly in an open, transparent manner.

- ***Improved risk identification***: Risk mapping, coupled with a common language, provides a highly visible means of initiating and sustaining a dialogue about risks at all levels of the organization. Process and activity owners armed with the appropriate tools and processes are able to identify risks more effectively and contribute more to the enterprise's performance over time (as opposed to process and activity owners who approach the issue of risk as an afterthought). Better risk identification reduces the risk of retaining risk out of ignorance, thereby reducing the company's exposure to unacceptable surprises that can affect the financial market's assessment of its performance.

- ***Implementation of more effective analytical and early warning techniques***: Increased emphasis on more systematic, quantitative and predictive analytics leads to more informed decisions. Better decisions, in turn, lead to improved business performance over time. Greater use of methodologies for anticipating risk and assessing the impact of alternative scenarios on future expected results leads to increased effectiveness in escalating emerging issues to the attention of appropriate executives.

- ***Improvement in specific risk measures, metrics and monitoring***: The shift from "guessing" to "knowing" (or at least "understanding") is a clear improvement, as is from "reacting" to "being prepared." Management reporting which tracks key risks provides evidence of improved performance over time. Information about risk – risk responses, risk measures, risk processes, risk incidents, best practices, status of improvement plans and other relevant matters – made available at all levels of the organization through web-enabled data repositories facilitates the knowledge-sharing aspects of an ERM approach. Use of risk aggregation tools replaces intuitive guesswork with fact-based analysis.

- ***Reduced number or avoidance of risk incidents***: If a firm can demonstrate fewer risk incidents or loss events than the industry average, it has clear evidence of superior performance. Workplace safety is a good example of a risk where such benchmarking is possible. In some cases, Y2K for example, the expectation is compliance – no more, no less. Some questioned the level of Y2K expenditures when planes didn't fall out of the sky, elevators didn't drop and nuclear weapons didn't trigger. But consider the impact on reputation and image had a company's mission-critical systems not been Y2K-compliant. It is paradoxical thinking to invest in a risk reduction response and then be disappointed when "nothing happens."

- ***Reduced performance variability***: If a firm encounters fewer surprises in reported results due to (a) a more systematic and proactive risk evaluation process, (b) improved measures and (c) preventive internal controls that preempt risk incidents at the source, this experience may be attributed to the firm's risk management. Reduced variability in revenues, earnings and cash flows over time may, all other things being equal, contribute to higher price/earnings multiples versus peer companies that sustain greater volatility in reported results. Of course, the difficulty with this measure is delineating the contribution of risk management from other management disciplines.

- ***Reduction in cost of capital and improvement in shareholder value***: As analysts, rating agencies, regulators and other institutions learn to differentiate between various firms' risk management capabilities, organizations able to put in place the capabilities articulated in this publication should enjoy a lower cost of capital over time in relation to the firms choosing to do nothing. If a firm's risk management is viewed in the marketplace as a differentiating skill relative to its peers, then the company's borrowing costs should decline and its share valuations should increase accordingly. While admittedly there is an absence of empirical support for this assertion, it is nevertheless a strong hypothesis that some companies have as they implement ERM.

- ***Increased risk sensitivity and risk awareness***: A cultural shift in the organization leading to an increased focus on and reinforcement of risk management goals and objectives is an indicator of effectiveness. For example, to achieve a demanding goal for an historically high target of injury-free days in a manufacturing organization, a cultural shift may be needed to modify behavior. Another situation is when a utility plans the implementation of a process to prevent future power outages. In these instances, risk management is actually integral to managing the business as it addresses obstacles that may prohibit the achievement of a business imperative declared by management.
- ***Integration with KPI reporting***: We see a number of firms integrating risk management with key performance indicators (KPIs). For example, one company prepares risk maps for each of the KPIs on its balanced scorecard. This innovative approach offers executives a comprehensive prioritization of risks by KPI. Steps are then taken to address the significant risks that could cause the firm to fall short of its performance goals. This linkage can only help improve performance over time.
- ***The continued success of the firm***: Finally, some believe that building and sustaining competitive advantage and producing incremental increases in cash flows and earnings per share are, in themselves, indirect measures of risk management effectiveness. Other traditional measures used in this regard include ROI, ROE and shareholder-value-added. Useful nonfinancial measures include customer satisfaction and retention, employee satisfaction, channel throughput, market share and brand image. Whatever measures are used, the firm should track its performance relative to its competitors over time. The notion is that if the organization manages its risks effectively and continues to be successful in a competitive marketplace, the two are related. Again, there are other management disciplines contributing to the organization's success.

MAKING IT HAPPEN

137. What is journey management and why is it relevant to ERM implementation?

Once management approves the ERM vision, value proposition and business case, the ERM implementation process begins. ERM implementation is a journey. As with any journey, the implementation process must be managed. Journey management organizes the capabilities defining management's ERM solution into a plan that (1) builds the capabilities needed to deliver the desired outcomes and (2) addresses change management issues associated with executing the plan. Program management (as discussed in Question 138) distills the journey management plan into a more granular project plan that designs and implements the ERM capabilities management decides to build and enhance. Journey management provides sponsors a high level view at a point in time as to where the ERM program is headed. Program management breaks the program down for assigning responsibilities and monitoring execution.

The journey management process summarizes the ERM journey as management chooses to define it. Because each organization's ERM solution is unique, the journey management process is also unique. A customized ERM journey management plan identifies, prioritizes and sequences the overall effort required to make the ERM solution a reality.

The ERM vision, goals and objectives, as described in the business case, articulate the desired future state. The journey management plan describes how that vision, and the related goals and objectives, will be achieved over time. As a high-level plan, it organizes the ERM solution capabilities selected by management into a logically sequenced plan with targeted milestones and checkpoints. Management uses this plan to assess journey progress and, if necessary, periodically refine the journey definition.

Many key factors must be considered when organizing the ERM journey. Following are examples:

- ***Sponsor expectations***: What do sponsors want in terms of business results? What do they expect with respect to benefits, investments, working relationships and protocol? What is the timing of those expectations?

- ***Change readiness issues***: Change must start at the top and cascade downward into the organization. The internal sponsors and influencers of an organization's ERM journey and the relationships among them must be profiled and understood to plan the scope of the journey and its goals and the related communications to the organization. Stakeholder roles and expectations provide a context for sponsors to begin thinking about change readiness issues. A change enablement plan is an integral part of journey management and provides a basis for sponsors to engage key stakeholders throughout the organization.

- ***Journey risks and constraints***: Sponsors must understand the risk factors and organizational constraints that could impede journey progress. These risks and constraints require careful consideration and monitoring. They provide input to the journey management plan. As organizations are dynamic, these risks and constraints can be expected to change over time. Therefore, management's assessment of them should be periodically updated as the organization achieves milestones and begins new initiatives.

- ***Journey communications plan***: Communications should not be ad hoc. The senior management team must visibly endorse and support the change process at key implementation checkpoints. A well articulated plan is needed to outline how this will happen. That plan should address the major activities specific to the journey and the anticipated capabilities. In addition to addressing key journey risks, the plan should designate the individuals expected to fulfill the necessary roles and their respective responsibilities.

- ***Journey coordination plan***: This plan defines executive management's position on how the change journey will be planned and managed, taking into account the extent, nature and timing of the planned ERM capabilities and the expected change. The plan consists of journey guidelines and a journey map that coordinate all planned activities so they are aligned with the business case and directed toward achieving the risk management vision, goals and objectives.

- ***Journey performance assessment***: Over the life cycle of the journey, the various planned programs and projects must be monitored and evaluated. The designated journey milestones, performance targets and measures provide a context for monitoring performance so ERM sponsors can determine whether the change journey is realizing the anticipated results and, if not, why not. Periodic management checkpoints also give sponsors an opportunity to reaffirm the commitment to sustain the journey and achieve expected performance targets.

- ***Journey impact analysis***: Over time, sponsors need to know the impact of the change effort, pace, timing and approach on the organization and the risks, if any. Based on their understanding, sponsors evaluate the immediate actions to take, such as further assessments, communications, interventions and alternative directions to take. An impact assessment should be periodically updated throughout the journey life cycle and preventive actions taken, if necessary, to reposition the ERM journey toward success.

- ***Solution capability sequencing***: We recommend following the sequencing of implementing selected foundation capabilities first, then proceeding with building appropriate risk management capabilities for priority risks and concluding with implementing selected enhancements to those capabilities over time.

Effective journey management provides solution sponsors assurance that the ERM journey is effectively managed. It ensures that the appropriate ownership, sponsorship, commitment and leadership for the change journey is achieved within the organization. Most importantly, it determines that sponsor and stakeholder expectations are met or exceeded. The success of the ERM journey is inextricably linked to the ability of sponsors to sustain senior executive support. That continued support provides momentum for implementing the additional ERM solution capabilities needed to fully realize management's ERM vision. That will only happen if the organization's leaders are poised to sustain the ERM journey.

Because they are interrelated, the business case and journey management plan may be developed concurrently. The ERM journey is focused by the shared vision, goals and objectives articulated by the business case. Further, the journey is subject to change. For example, the journey management plan is exposed, at all times, to the effects of changes in external and internal forces on business requirements and the related impact on the ERM business case. Consequently, sponsors must anticipate and accommodate potential modifications to the journey management plan with proactive planning, effective communications, flexible design methodologies and periodic journey assessment.

138. What is program management and why is it relevant to ERM implementation?

For some companies, the ERM implementation may be a relatively straightforward project. For other companies, ERM is achieved in stages in the form of multiple, related projects. To be implemented successfully, these projects require a disciplined and methodical approach. How does management know that the related project deliverables and capabilities are all working together in unison to achieve the end goals and objectives of management's ERM vision? For simple ERM solutions, the answer may be obvious. For more complex solutions, a program management discipline is needed.

Program management provides the oversight and discipline necessary to ensure effective integration and coordination of multiple projects over the ERM journey life cycle. Under the direction of the program office, appropriate processes, procedures, techniques and tools are used to (1) plan and organize the work and (2) manage the delivery of the planned ERM solution over time. While the CRO may provide this oversight, a program office can assist the CRO in managing the myriad of details around the design and implementation process. Thus the program office may report to the CRO (or to an equivalent executive). The objective is to support the design and implementation of the capabilities that deliver the outcomes envisioned by the organization's ERM solution.

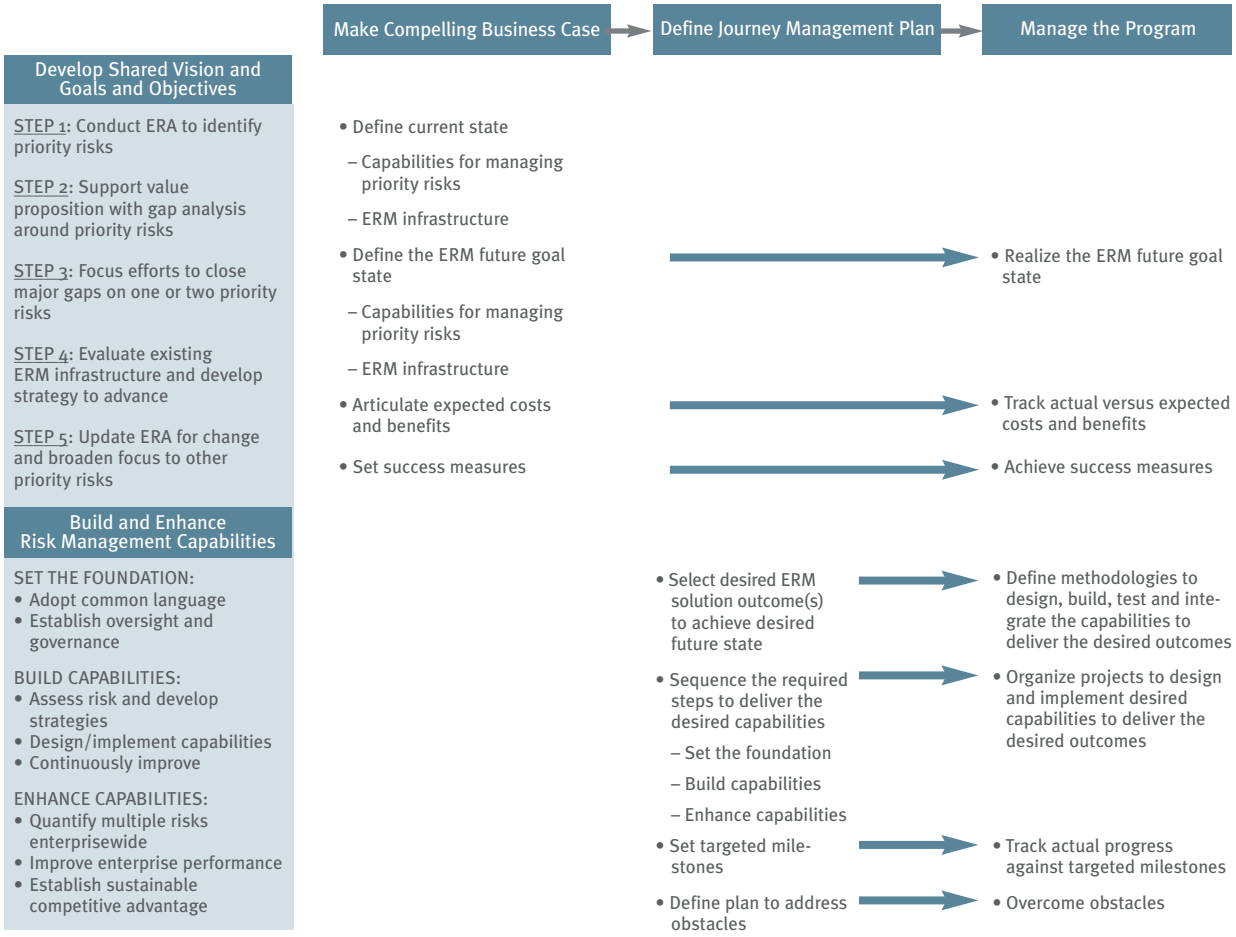
The program office converts the journey management plan, as discussed in Question 137, into logically sequenced, discrete projects that build the needed capabilities to make the organization's future state goal and vision a reality. Once the broad outlines of the ERM journey is laid out in the journey management plan, project management discipline is needed if there are multiple solution capabilities requiring multiple projects. The more complex the effort, the more likely a program management function is needed. If the ERM journey is comprised of multiple related projects, these projects must work in unison and be integrated effectively to achieve management's ERM vision, goals and objectives. Depending on the complexity of management's ERM solution, the journey could even consist of two or more discrete programs, with each program consisting of multiple projects.

Whereas the journey management plan is strategic and visionary, program management is tactical. The program management process, among other things:

- Supports an ongoing assessment of program and project status, project risks and constraints, the expected project capabilities and the effectiveness of change enablement activities.
- Lays out the methodologies by which the capabilities that deliver ERM solution outcomes are designed, built, tested and implemented through multiple initiatives and projects.
- Operationalizes management's ERM vision by transforming it into a well-defined program of discrete but integrated projects that are organized and sequenced in the most effective manner to maximize the chances of success against established milestones and checkpoints.
- Determines that the various projects are adequately resourced at the right time.
- Tracks progress against established milestones and ensures that appropriate corrective action is taken, if necessary.
- Reports implementation status to sponsors, management and the board.

Appropriate processes, procedures, techniques and tools are used to plan and organize the work, and to manage the delivery of the ERM solution that will realize the benefits set forth in the business case.

The following summary illustrates how management's ERM business case, the ERM journey management plan and program management are interrelated:



The program office can also function in a continuous improvement capacity once the ERM solution is in place. When gaps arise in the ERM infrastructure and in capabilities for managing priority risks, action plans must be developed to implement the needed improvements. These improvement efforts should be prioritized and incorporated into the business planning process. For serious gaps and other issues, the situation must be brought under control on a timely basis. Accountable risk and process owners execute action plans in accordance with established timelines. The program office oversees the execution of these action plans and ensures that assurance units – such as internal audit – satisfy themselves that the action plans are carried out effectively. The program office reports implementation status to executive management and to the board.

Program management discipline is vital for more complex implementations. ERM can potentially represent a sea change in organizational attitude and behavior. As with any significant change, the adoption of ERM is fundamentally a process of building awareness, developing buy-in and ultimately driving the acceptance of ownership throughout the organization to the appropriate managers. Change enablement is, therefore, a significant aspect of an ERM initiative because everyone's perspective about risk can vary significantly.

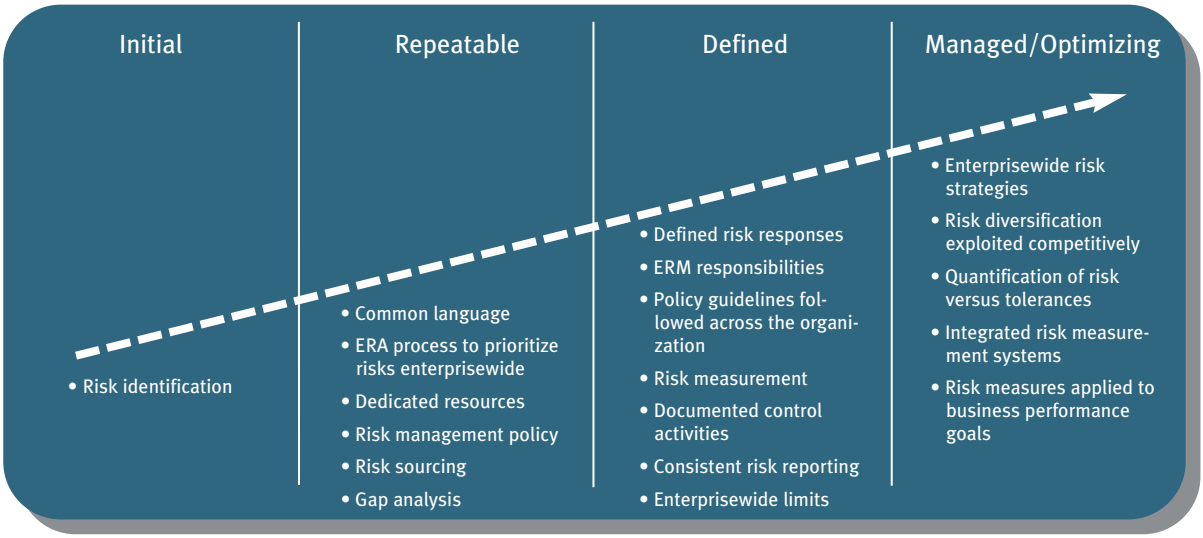
The ERM journey is a growth process, which leads the firm to improve its risk management capabilities. As it navigates its ERM journey, the organization becomes more sensitive to changes in the environment and within its business processes. This sensitivity in the culture is important because opportunities and risks will continue to surface and change rapidly in the global economy. Thus developing an effective, enterprisewide view of business risk management will always be a journey of continuous learning and improvement.

139. How can we quantitatively and qualitatively evaluate the benefits of implementing ERM in terms of improving performance?

For those risks where management has chosen to attain a "managed" or an "optimized" state on the capability maturity model, there are three steps to enhancing capabilities. These steps are ***quantify risk enterprisewide, improve enterprise performance*** and ***establish sustainable competitive advantage***. These capabilities conclude the progression towards an ERM solution. Enhanced capabilities provide insight into the ultimate direction of the ERM journey.

The capability maturity model illustrates how enhancing risk management capabilities requires the adoption of new risk management practices over time:

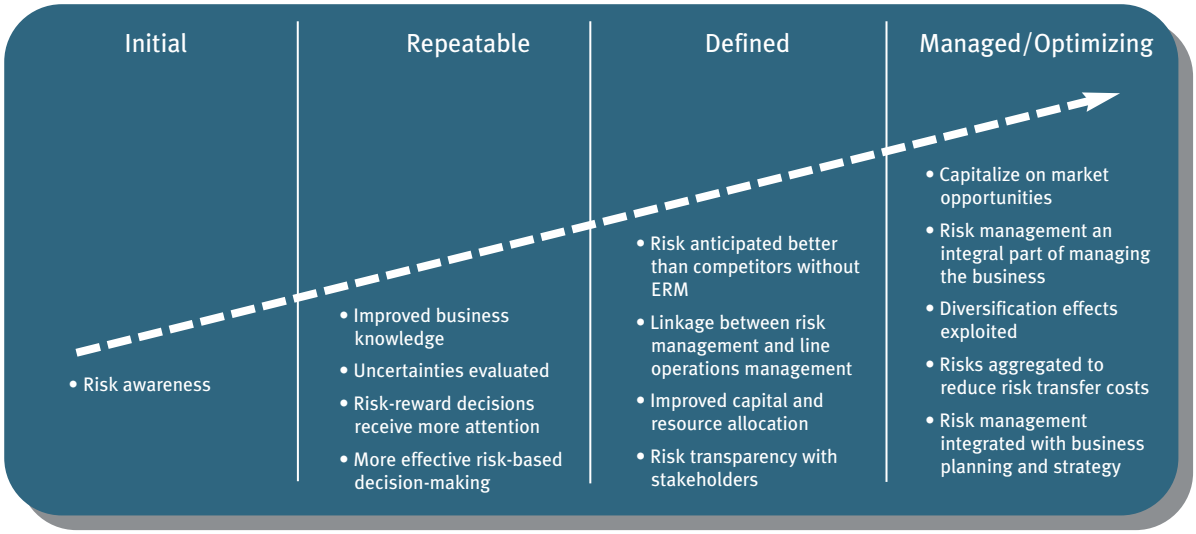
IMPROVED RISK MANAGEMENT CAPABILITIES



Implementing an ERM solution is not something that occurs overnight. The continuum illustrates the progression that is necessary in order to improve risk management capabilities over time.

The benefits of ERM also accumulate as risk management capabilities are enhanced, fully realizing the value proposition articulated in the business case:

ACCUMULATION OF BUSINESS PERFORMANCE BENEFITS



140. How is the ERM implementation managed?

The ERM sponsor should track progress over time to make sure the implementation process is on track with expectations. Four things make this monitoring possible:

- First, the sponsor should ensure that the implementation process is focused on the right things by using a gap analysis around the capabilities for managing the enterprise's priority risks. Integrating risk management activities with the execution of the business strategy helps ensure the proper focus. See Question 85.
- Second, the sponsor should insist on having a plan outlining logically sequenced, discrete activities to build the capabilities desired by management and defining the milestones and checkpoints to monitor progress over time. See Questions 137 and 138.
- Third, the sponsor should monitor execution of the plan against the established milestones and checkpoints. See Question 138.
- Finally, the sponsor should evaluate the benefits from ERM against the expected benefits articulated in the business case. See Questions 134 and 136.

141. How do we know when we are done?

The ERM implementation is completed when the implementation plan is fully executed and the expected benefits articulated in the business case are realized. As further discussed in Question 138, the program management office provides the oversight necessary to bring the effort to closure. The CEO and executive committee also provide oversight.

142. Given that we have so many other things going on, how can we take on something like ERM implementation?

This is a prioritization issue that starts at the top of the organization. Ultimately, the CEO and the board of directors must decide what is important. As we have stated throughout this publication, integration is an effective theme when implementing ERM, e.g., integration with business planning, strategic management, Six Sigma, capital allocation management, R&D management, marketing and business development, etc. Therefore, rather than create an appendage, the emphasis is on integrating risk management improvements into existing management structure and processes.

143. What standards should companies use to evaluate their ERM approach?

COSO provided broad criteria to guide organizations, public and private, large and small, for-profit and not-for-profit, and avoided a one-size-fits-all approach. The "standards" lie within the organization's objectives and are impacted by the application of the COSO framework components. The ERM definition provided by COSO provides key points of focus for organizations to address. It is reasonable to expect that more explicit "best practice" standards or examples might arise within different industry sectors as experience is gained applying the COSO framework.

144. Are there any pitfalls to avoid when implementing an ERM approach?

The primary pitfall to avoid is failure to understand the purpose of ERM implementation. It is not unusual for companies to inquire about or even proceed with implementing ERM without understanding the problem they are trying to solve. Failure to clarify the value proposition ultimately leads to frustration when hard costs are incurred to realize benefits that are perceived as soft. Failure to clarify the purpose of ERM leads to endless searches for one-size-fits-all solutions, unnecessary implementation activities and false starts.

There are other pitfalls to avoid when implementing ERM. We list ten of them below:

- ***Lack of support from the top***: Establishing ownership of ERM (as opposed to providing lip service) at the highest level of the organization is critical. Without the support and commitment of the CEO and the board of directors, ERM cannot be effectively implemented. Lack of support manifests itself in a number of

ways, e.g., ERM is not viewed as a priority, the absence of a shared vision and compelling business case, the lack of engagement by the CEO, earnest but unsuccessful efforts by lower level management to sell ERM upward, lack of senior management presence in status meetings, etc. Commitment from the top is where everything starts. Without it, momentum is lost, the project becomes unfocused and the initiative stalls.

- ***Lack of stakeholder ownership and buy-in***: Ownership and commitment by key stakeholders is vital to the success of ERM implementation. If there is inadequate attention given to change management and keeping people engaged and there is an absence of performance metrics driving the implementation process, the initiative will flounder.
- ***Failure to integrate ERM with what matters***: If there are attempts to implement ERM without an understanding of the value drivers and business issues on the CEO's screen, the ERM implementation will not succeed. Linkage to business issues on the executive management agenda is vital to success. An enterprise risk assessment with the business strategy as a context is an excellent way to begin this linkage. When the enterprise risk assessment is followed by focused risk responses addressing the priority risks using the business strategy as a context, the ERM initiative is more effectively linked with the value drivers of the business. This linkage increases the emphasis on improving metrics, measures and monitoring. Unless integrated with processes already institutionalized in the organization, ERM is often viewed as an appendage. Strategic management, business planning, performance management, capital expenditures, quality management, Sarbanes-Oxley compliance and other compliance management are examples of processes already in place that management may choose to integrate with ERM.
- ***Getting immersed in details***: When ERM sponsors allow the implementation to deteriorate to the point where risk assessments get mired down into business processes or where management must wade through lengthy lists of risk factors, the implementation process is in trouble. COSO stated that ERM must be applied across the enterprise, not at the process level. COSO also stated that ERM must be applied in strategy-setting, so the assessment process needs to focus on the "big picture" issues to retain the confidence and attention span of senior and operating management.
- ***Failure to define roles and responsibilities***: Clarifying roles and responsibilities has always been a challenge in risk management and is particularly so with ERM. Because current risk management approaches are too firmly rooted in the command and control era, they often lead to silo behavior that spawns gaps (no owner of a risk) and overlaps (too many owners of a risk) over time.
- ***Failure to consider the cultural issues***: ERM is a cultural change. The issues associated with culture and the impact of the risk awareness and risk sensitivity of the organization on behavior are discussed in our response to Question 102. While this area is often viewed as a "soft benefit," it is nonetheless important.
- ***Failure to balance market making and control activities***: The result is rarely good when the entrepreneurial activities and the control mechanisms of an organization are out of balance. Unbridled opportunity seeking to create enterprise value without setting reasonable boundaries through checks and balances can lead to disastrous consequences. The swing of the pendulum all the way to risk-averse behavior can lead to poor performance relative to competitors. The ultimate objective of the oversight structure is to provide assurance to the board and CEO that the entrepreneurial activities of the business and the control activities of the business are reasonably in balance so that the risks inherent in opportunity-seeking behavior are understood and managed. See our response to Question 53 for further discussion.
- ***Failure to manage conflicts of interests***: Conflicts of interest create challenges because the typical internal control structure is based on the presumption that independent parties are operating at arm's length with each other. If that isn't happening, either because of the existence of related parties or a waiver or violation of the entity's "conflict of interests" policy, significant problems can arise. It is up to the board to ensure that responsible business behavior is taking place in the organization.
- ***Failure to apply management's ERM approach across the enterprise***: As COSO defines it, management can't implement ERM unless it is applied across the enterprise (or across a specific operating unit). Uneven application typically leads to transparency in some parts of the organization and obscurity elsewhere in the organization. Call it whatever you want, but it is not ERM as defined by COSO.

- ***Getting ahead of the enterprise's capabilities***: ERM is not about implementing the most sophisticated techniques. It is a progressive approach to implement the eight components of the COSO framework to address the organization's priority risks. Entities often are tempted to implement enhanced capabilities (as described in Question 125) before they have set the proper foundation (as described in Question 96) and built basic risk management capabilities (as described in Question 103). Or they start building capabilities before they have set the foundation. In other words, they get ahead of themselves, often looking for the "quick fix." Often, it doesn't work and leads to waste.

RELEVANCE TO SARBANES-OXLEY COMPLIANCE

145. Does the Sarbanes-Oxley Act of 2002 (SOA) require companies to adopt ERM? Are there any other laws and regulations mandating ERM?

No, SOA does not mandate ERM. There aren't any specific laws and regulations requiring ERM, to our knowledge. However, implementation of ERM would facilitate compliance with applicable laws and regulations, including SOA.

146. Can ERM assist certifying officers with the discharge of their SOA Section 302 certification and Section 404 assessment responsibilities?

Long after the projects to implement the requirements of Sarbanes-Oxley are completed, certifying officers need to keep the disclosure process from going stale. Enterprisewide risk management will surface new and emerging risks for timely action and disclosure. Therefore, ERM will assist certifying officers with the discharge of their quarterly SOA Section 302 certification and annual Section 404 assessment responsibilities.

147. How is ERM related to SOA compliance?

While SOA compliance efforts are vitally important, necessary and worthwhile, ERM is broader. While SOA compliance focuses on reliable financial and public reporting as well as other aspects of governance to restore investor confidence in the capital markets, ERM addresses the full spectrum of risks the organization faces, including the risks associated with strategic, operational, internal reporting and other compliance objectives. Most public companies in the United States use the Internal Control – Integrated Framework to facilitate their compliance with Section 404. The Enterprise Risk Management – Integrated Framework is broader than the internal control framework and encompasses that framework.

Because both the SEC and PCAOB have endorsed a risk-based approach to evaluating internal control over financial reporting in accordance with Section 404, ERM can provide benefits from an SOA compliance standpoint. ERM assists companies in keeping their disclosure process fresh through a process-based chain of accountability that involves unit managers and process owners in communicating issues requiring action and possible disclosure. More importantly, a focus on operating efficiency and effectiveness with emphasis on increasing quality, compressing time and reducing costs while simultaneously controlling financial reporting risk will result in increased emphasis on automated controls (versus ad hoc manual controls) and preventive controls (versus costly "find and fix" detective controls). ERM gives executives and directors more confidence that the internal control structure is sustainable during times of significant change. An effective ERM process also gives executives and directors greater confidence their organizations are identifying and managing all potentially significant business opportunities and risks.

148. Should a decision to implement ERM consider the effort to comply with SOA?

ERM supports and builds on the Sarbanes-Oxley compliance efforts. While ERM can enhance the quality of internal and external reporting, integrity in reporting is a prerequisite for, not a result of, ERM. A full and honest commitment to fair and truthful reporting, which is the primary goal of SOA, surfaces the vital signs of change, which management must consider when evaluating whether strategies and objectives remain

market-facing, customer-focused and competitive. An organization cannot effectively manage its risks when it suppresses information about business realities.

ERM focuses on business risk and internal controls with an objective to preserve as well as create enterprise value. ERM aligns strategy, people, processes, technology and knowledge. The emphasis is on strategy. And the application is enterprisewide. By managing risks strategically across the enterprise, an organization not only supports Sarbanes-Oxley compliance but also brings to light new risks as they emerge. Transparency is not only the name of the game, it is vital to sustaining SOA compliance. While there is no question the disclosure process is critical, so too is the process of managing other business risks. ERM instills the discipline needed to improve risk management capabilities continuously, including financial reporting risks.

149. Should management broaden the focus on compliance to managing business risk?

The short answer is "yes." Managing risk is all about managing the enterprise. The COSO framework suggests that management should take advantage of the opportunity to use the ERM framework to build on the foundation laid by SOA compliance and evaluate whether there are opportunities to improve the organization's risk management. Following are reasons why:

- Compliance with Sarbanes-Oxley lays a foundation for implementing ERM infrastructure that did not previously exist for many companies. Those companies that have implemented improved disclosure processes and internal control over financial reporting should take a closer look at how they can expand these capabilities to encompass ALL business activities so that executives and directors alike can gain greater confidence that their organizations are identifying and managing ALL potentially significant business opportunities and risks.
- Successful companies take risk when seeking new opportunities. Risks are constantly changing in the global marketplace, whether organizations choose to do anything to manage them or not. As executives examine the risks their companies face today, they will see a different profile than what existed even a few years ago. And, more importantly, they can expect to see even different risks just a few years from now. The pace of change and increasing complexity of business are raising the bar continuously for risk management.
- An effectively implemented enterprisewide approach to assessing and managing risk will surface risks more timely for decision-makers to consider alternative actions and required disclosures. ERM will help the organization create and protect enterprise value as well as better equip management in communicating in a public forum what the company's risks are and how effectively they are being managed.

Managers must have a more comprehensive understanding of the critical risks they face and, more specifically, the effectiveness of the strategies and capabilities their organizations have in place to respond to those risks.

150. As a public company, why would we want to take on ERM on the heels of Section 404 compliance?

We discussed the ERM value proposition in our response to Question 4. ERM helps management with establishing sustainable competitive advantage, optimizing risk management costs and improving business performance. Section 404 compliance requires the implementation of an ongoing process to address financial reporting risk. Because most companies are using the COSO Internal Control – Integrated Framework as criteria for complying with Section 404, many elements of the Section 404 compliance process also apply to the implementation of ERM. Therefore, Section 404 compliance provides a foundation for implementing ERM.

As companies implement self-assessment processes to drive accountability down to process owners (see Question 151) and integrate Section 302 and Section 404 compliance activities (see Question 152), SOA compliance takes on more of an ERM-like appearance. As companies broaden the compliance focus to other applicable laws and regulations (see Question 153), the result is implementation of the COSO framework to the compliance objective, one of the four objectives of the framework. As the focus broadens to improving quality, compressing time and reducing cost of the processes feeding financial reporting (see Question 154), the result is an expansion to operational effectiveness and efficiency, another objective of the COSO framework. Therefore, all of these steps logically build on the foundation laid by SOA compliance.

While not every organization begins its evolution to ERM with Section 404 compliance, most public companies in the United States, in effect, do because (1) the initial compliance investment is significant and (2) a company cannot have sound governance without transparency in financial reporting. Therefore, a focus on reliable financial reporting is a good foundation on which to build ERM capabilities. SOA compliance lays a foundation by, in essence, providing a framework for managing other risks enterprisewide. For example, it requires a common language, a risk assessment, an evaluation of the design effectiveness of internal controls in place, the validation of the operating effectiveness of those controls as well as effective monitoring. These elements – common language, assess risk, evaluate design, validate operation and monitor – are elements that can be applied to other risks. The addition of self-assessment, the existence of a disclosure committee (in accordance with Section 302) and senior management involvement are additional elements.

Whether an organization begins its ERM journey with SOA compliance, with one or two priority financial or operational risks, or with some other priority risk, the focus of ERM infrastructure is the same, i.e., to advance the maturity of risk management capabilities for the organization's priority risks. Whatever the starting point, there are five steps for organizations choosing to broaden their focus to ERM:

(a) Conduct an enterprise risk assessment to identify and prioritize the organization's critical risks. This step provides a context for performing a gap analysis of the current and desired capabilities around managing the key risks. Refer to Questions 69 through 84.

(b) Articulate the risk management vision (see Question 64) and support it with a compelling value proposition (refer to Questions 4 and 134 through 136) using gaps around the priority risks (see Question 111). This step provides the economic justification for going forward.

(c) Advance the risk management capability of the organization for one or two critical risks, e.g., financial reporting or some other vital risk. This step focuses the organization on improving its risk management capability in an area where management knows improvements are needed.

(d) Understand and evaluate the existing ERM infrastructure capability and develop an effective strategy to advance. It is expected that advancing the capabilities around managing one or two critical risks will require some level of infrastructure, so this step should take into account the advances in ERM infrastructure resulting in step (3). Possible elements of the ERM infrastructure are illustrated in Question 37.

(e) Update the assessment of the enterprise's business risks for change, prioritize the additional key risks and develop strategy for evaluating and advancing the risk management capabilities for those key risks. This step begins with selecting the priority risks and determining the current state of risk management capability for each of those risks. Once the current state is determined for each of the key risks, then the desired future state is assessed with the objective of advancing the maturity of the capabilities around managing those risks. See Question 111 for examples illustrating risk management capabilities at different stages of maturity.

The above steps provide a simplified view of the task of implementing ERM. They are more fully discussed in Question 85. These steps allow management to proceed in a practical manner.

ERM implementation does not occur overnight and, for certain, is not easy to accomplish. ERM is a journey. The next four questions provide commentary regarding the evolution from Section 404 compliance to ERM, as described above. This commentary addresses four intermediary phases illustrating the evolution from Section 404 compliance to ERM.

151. How does self-assessment build on Section 404 compliance? Why does self-assessment contribute to the evolution to ERM?

Because its application is often enterprisewide, self-assessment contributes to the kind of open environment and upward communications that facilitate an evolution to ERM. While not required, self-assessment is a recognized best practice and has been applied to risks and controls for many years. It is sanctioned by the Public Company Accounting Oversight Board (PCAOB) as a tool for management's use, along with entity-level monitoring and independent tests of controls, in developing the body of evidence supporting a

conclusion as to the effectiveness of internal control over financial reporting. While external auditors generally cannot rely on self-assessment results for purposes of Section 404 compliance, management can. The PCAOB staff explained this distinction by pointing out that, when supporting a conclusion regarding the effectiveness of internal control over financial reporting, management has available procedures that the auditor does not. Self-assessment is an example of what the staff was talking about.

Systematically applied across the organization at the entity and process levels, self-assessment is a pre-determined approach whereby "in the know" individuals self-assess their risks and self-review or self-audit the controls for which they are responsible and communicate the results to appropriate management. In response to the upward reporting of process owner assessments, follow-up is taken where necessary. Used in combination with an effective entity-level monitoring process and periodic controls testing, self-assessment is a powerful and flexible element of an ongoing compliance program because it enables management to receive a comprehensive statement that key controls are in place and operating effectively from the people who are best positioned to know. For example, as the internal control report required under SOA Section 404 provides assertions from certifying officers, a self-assessment process reports upward relevant assertions from managers and process owners regarding the internal controls for which they are responsible.

Self-assessment may be applied to many risk areas, including operational risks and compliance areas other than Sarbanes-Oxley. It lends itself very well to an ERM culture, because it fosters an open environment that facilitates upward communication of assessments, good as well as bad, within the organization. This is the type of culture that supports an evolution to ERM.

When applied to any process or to any risk area, an effective self-assessment process addresses the following principles:

- Self-assessment is a management tool that drives the "tone at the top" down to process owners by reinforcing their responsibility and accountability for internal control over financial reporting.
- Because process owners are the men and women closest to the critical control points within the organization, they are the ones who know what's working and what isn't and when process changes are occurring. They recognize, often before anyone else does, the impact of systems, workforce and other pervasive changes on process performance and capability.
- The self-assessment process is aligned with defined roles, responsibilities and authorities relating to key business objectives and the management of the risks affecting those objectives.
- Self-assessments are desirably completed for many, if not all, of the company's primary controls, i.e., those controls that are especially critical to the mitigation of risk and the ultimate achievement of one or more business objectives. The underlying process, risk assessment and other management documentation (for example, as required by Section 404 compliance) lays the baseline for ongoing self-assessment. That documentation addresses such questions as:
  - What are the key controls at the entity and process levels?
  - What risks do they address?
  - Who owns them?
  - How are they rated as to design effectiveness? Are they adequate in mitigating the risks they are intended to address?
  - How are they rated in relation to operational effectiveness? Do testing results provide evidence that they are operating as intended?

The primary controls selected as most critical and significant for purposes of achieving the stated business objectives should be the focus of an ongoing self-assessment program.

In summary, self-assessment is a versatile process that can be applied to ALL types of business risks. Once a self-assessment process is in place, it instills discipline, reinforces accountability and promotes transparency, all of which are important building blocks towards ERM.

152. What does it mean to integrate compliance with Sections 404 and 302? How does such integration build on an established self-assessment process and on Section 404 compliance? Why does such integration contribute to a company's evolution to ERM?

Integrating Section 404 and Section 302 compliance is a likely point of focus for most companies after they file their first internal control report, because it makes business sense to do it. It logically builds on an effective self-assessment program (see Question 151). Going forward, management should think of compliance with Sections 302 and 404 as a SINGLE requirement of continuous reporting. The following reasons support this point of view:

- ***The company's 302 executive certification changes after the first internal control report is issued to incorporate more explicit recognition of management's responsibility for internal control over financial reporting***. For example, the new language states that management is responsible for establishing and maintaining internal control over financial reporting. It also states that management has designed internal control over financial reporting, or caused such internal control over financial reporting to be designed under their supervision, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles.

- ***There is significant overlap between "disclosure controls and procedures" and "internal control over financial reporting," as the SEC defines the two terms***. Therefore, since Section 302 and Section 404 address, in substance, similar policies and procedures, management should view the compliance process as a continuous one.

- ***There are important interrelationships between Sections 302 and 404 with respect to timely reporting of significant deficiencies in internal control over financial reporting to auditors and audit committees and timely disclosure of material weaknesses to investors***. In the quarterly executive certification, the certifying officers must represent they "have disclosed, based on their most recent evaluation of internal control over financial reporting, to the auditors and to the audit committee, all significant deficiencies and material weaknesses in the design or operation of internal control over financial reporting which are reasonably likely to adversely affect the company's ability to record, process, summarize and report financial information." Therefore, when company personnel identify deficiencies relating to internal control over financial reporting, they must escalate these matters in a timely manner, through a systematic process, to enable management to promptly consider the potential severity and evaluate whether specific action and disclosure is appropriate.

- ***The current quarterly executive certification already addresses the implications of change on internal control over financial reporting***. The specific language in the certification is as follows:

  > [The certifying officers]…have…disclosed in the report any change in the issuer's internal control over financial reporting that occurred during the issuer's most recent fiscal quarter (the fourth fiscal quarter in the case of an annual report) that has materially affected, or is reasonably likely to materially affect, the issuer's internal control over financial reporting.

  This representation is not only in play for every company regardless of its Section 404 compliance status, but it is also a major reason why hundreds of companies have disclosed internal control related issues during the months preceding issuance of their first internal control report.

- ***Quarterly reporting is as important as annual reporting because material weaknesses in internal control over financial reporting can arise from risks of misstatement to both***. As management reports under Section 302 quarterly and under Section 404 annually, it is important to realize that restatement risk applies as much to interim reporting as it does to annual reporting. Therefore, companies should coordinate their self-assessment activity, entity-level monitoring and independent controls testing with the reporting required under Sections 302 and 404.

Thus, going forward, many companies should think of Sections 302 and 404 as a SINGLE compliance process requiring continuous reporting. This thinking results in improved "sustainability" which, from an SOA

compliance standpoint, refers to continuing effectiveness of two interrelated management imperatives over time – (1) the repeatability and effectiveness of the internal control structure, and (2) the cost-effectiveness of the organization's SOA compliance capabilities, particularly with respect to Sections 302 and 404. Simply stated, a sustainable compliance approach is one that will withstand scrutiny over time as change occurs. While first-year Section 404 compliance is important; it is even more important to recognize that Section 404 compliance is ongoing. For many companies, the initial year administrative burden in terms of resource commitment and third-party expenses is unacceptable, so efficiency and effectiveness is the order of the day.

To address the interrelated issues of sustainability and efficiency, many companies will address four key themes to integrate their compliance with Sections 404 and 302 successfully over time:

- ***First, implement an organizational infrastructure facilitating ongoing compliance***: This theme is discussed in depth in Issue 12 of Volume 1 of Protiviti's *The Bulletin*, which introduces various alternative structures for ongoing compliance. It is about the transition from "project to process" so that the compliance activity is more repeatable, clearly defined and better managed. It is about institutionalizing the compliance process through:

  - Defining the ongoing program infrastructure support and formulating a longer-term plan to resource and budget that support so that appropriate expectations and action items are incorporated into the business plan
  - Achieving unit management buy-in and acceptance, including absorption of program costs into unit budgets
  - Continued strengthening of the organization's entity-level controls, including its anti-fraud program and companywide monitoring processes
  - Remediating unresolved significant control deficiencies as soon as possible so that the ongoing compliance infrastructure is focused on managing change versus repairing prior year control issues

  These steps require an enterprise view, and therefore contribute to an ERM environment.
- ***Second, establish accountability of process owners and others for internal control***: The Section 404 compliance activity should be process-owner driven, not project-team driven as it is for most companies during the initial year of compliance. The transition of establishing accountability is about driving desired behaviors through:

  - Understanding, acceptance and ownership of roles and responsibilities for all critical controls
  - Defining appropriate methodologies and integrating them into business routines
  - Articulating escalation policies and protocols, with emphasis on timeliness
  - Articulating remediation and retesting protocols, with emphasis on timeliness
  - Developing and delivering process owner guidance, training and support

  Because clarifying roles and responsibilities and establishing accountability are vital to the implementation of ERM, these steps contribute to the evolution to an ERM infrastructure.
- ***Third, implement an effective change recognition process***: To keep the disclosure process fresh, certifying officers need a change-recognition procedure that surfaces new developments and events timely for subsequent follow-up and possible disclosure. An important aspect of change recognition is to ensure that the impact of changes in policies, procedures and systems on the internal control structure is accurately reflected in controls documentation so that updates can be made to the controls design effectiveness evaluation and to the testing plan for evaluating controls operating effectiveness. This particular theme drives the company's transition from initial documentation in the first year to an ongoing process of document management. Steps management should take include:

  - Articulating and communicating responsibilities for identifying and reporting change timely
  - Establishing protocols for updating controls documentation for change

- Examining disclosure committee performance versus charter
- Recognition of and creating sensitivity to change is what ERM is all about

- ***Fourth, identify and capitalize on additional improvement opportunities***: This theme is about transitioning over a reasonable period of time from excess reliance on manual and detective controls to an appropriate mix of automated and preventive controls. It includes the transition from comprehensive testing to targeted testing as a result of improved "filtering" of controls. This theme is also largely about alignment and efficiency issues, and looking at opportunities to transition from the "unpredictable costs" environment of the first year to a "managed costs" environment going forward. In effect, this theme is about three things – (1) achieving value-add by improving the quality, time and cost performance of financial reporting processes, (2) improving the sustainability of the internal control structure and (3) improving the cost-effectiveness of the compliance process by making it risk-based and top-down. This theme includes, among other things, the following:

  - Optimizing testing plans, including selection, scope, timing, remediation, retesting and refresh testing as well as effective integration of independent controls testing with self-assessment and entity-level and process-level monitoring
  - Deciding a long-term data repository strategy, including understanding and selecting an appropriate point or platform technology solution to achieve efficiency and effectiveness in documenting, updating and archiving internal control documentation
  - Defining process improvement and re-engineering needs and priorities
  - Benchmarking processes to improve efficiency, articulate clearer job descriptions, effectively train people, design improved metrics, eliminate nonessentials and simplify, focus and automate manual activities
  - Formalizing the process to timely assess, classify and dispose of deficiencies to address the requirements of Sections 302 and 404
  - Understanding the interdependencies of IT general and application controls and effectively integrating that understanding into the Section 404 controls documentation and evaluation

  As these steps broaden the improvement emphasis to quality, time and cost performance, they expand the compliance focus to operational effectiveness and efficiency. These steps therefore contribute to the evolution of ERM.

  Other aspects to this theme include:

  - Working with the external auditor to streamline the external audit process and optimize the "use of work of others"
  - Defining the ongoing role of internal audit and aligning audit plans and resources with the expectations of management and the audit committee
  - Ensuring that regulatory compliance and risk management functions are performing effectively for large, complex entities
  - Aligning the cycle for new systems conversions and upgrades with the Section 404 compliance process
  - Renegotiating contractual outsourcing arrangements

  With respect to the external audit, most companies have been in the position of reacting to requirements asserted by their external auditors as the internal control attestation standards have evolved. Now that the rules are on the table for all to see and the SEC has issued guidance to registrants following its April 2005 Roundtable on Implementation of Internal Control Reporting Provisions, management will want to manage the audit relationship proactively and constructively so that the audit process is more risk-based and top-down.

In summary, integration of Section 404 and Section 302 compliance recognizes that companies can't succeed in complying with one without also complying with the other. A more efficient and effective compliance process will result as management addresses the four themes above for achieving sustainability of the internal control structure, achieving value-add in financial reporting processes, and increasing the cost-effectiveness of compliance with Sections 404 and 302. The more sustainable the control environment, the more capable the organization's processes and controls in dealing with change, including significant turnover, the influx of new people, mergers and acquisitions, new systems and new processes. Integrated compliance with Sections 302 and 404 also provide the "launching pad" for improving processes and the internal control structure and for enhancing entity-level and process-level monitoring of the financial reporting process. All of these things build infrastructure and processes that contribute to the evolution of ERM.

153. How does compliance with other applicable laws and regulations build on compliance with Sections 404 and 302? Why does such compliance contribute to the evolution to ERM?

Integrating Section 404 and Section 302 compliance, as discussed in Question 152, is not the end game. While SOA Sections 404 and 302 are important, there are other laws and regulations with which companies must comply. According to COSO, compliance with applicable laws and regulations is one of the four groups of objectives in the Enterprise Risk Management – Integrated Framework. Failure to conform with laws and regulations at the international, country, state and local level that apply to a business can damage reputation and brand image and lead to loss of markets, revenues and profits.

For many companies, the opportunity exists to apply the infrastructure established to facilitate ongoing SOA compliance to address compliance with other legal and regulatory areas. Any decisions around a broader compliance framework should involve the chief legal officer (CLO), or an equivalent executive, charged with the responsibility to monitor changes in laws and regulations and actions by national, state or local regulators, and assist the executive team with assessing the impact of significant changes in laws and regulations on the business. In the absence of a CLO (or equivalent executive), the executive committee must vest someone or some function with this responsibility. A well-connected CLO (or equivalent executive) is ideally positioned to recognize the inefficiencies of silo behavior and the potential synergies to be gained from a common compliance framework and infrastructure. In effect, a common compliance framework and infrastructure is an enterprisewide approach to managing the entity's risks around applicable laws and regulations. It applies the eight components of the COSO ERM framework to the compliance objective.

Because technology is a key enabler for SOA compliance, and there is a wide range of software tools available in the marketplace, many companies will evaluate whether to retain their "point solutions" designed specifically for SOA compliance or, alternatively, adopt broader "platform solutions." The so-called platform solutions are software infrastructure designed for another purpose such as business process automation, document management, financial management, or broader compliance, and are adapted for SOA compliance. Point solutions typically support deeper analysis and reporting requirements for SOA compliance, whereas platform solutions provide extended capabilities and could serve as infrastructure for broader compliance, governance, and risk management activities over time. Companies that are adopting platform solutions are taking yet another step along the journey to ERM because those solutions can be leveraged to other compliance areas.

154. How does operational effectiveness and efficiency build on compliance initiatives? Why does operational effectiveness and efficiency contribute to the evolution to ERM?

In Questions 152 and 153, we discuss risk management activities around compliance. Over time, companies will migrate from a "compliance-driven" (short-term) to a "value-driven" (long-term) approach to their SOA compliance initiative and will broaden their focus to other business risks. ERM will help companies accomplish this task. According to COSO, operational effectiveness and efficiency is one of the four groups of objectives in the Enterprise Risk Management – Integrated Framework.

Process performance issues become evident as companies work to comply with SOA. For example, many companies find they must complete untold numbers of time-consuming account reconciliations, process thousands of manual journal entries, plow though hundreds of spreadsheets, wade through and test thousands of controls and inadvertently ignore systems-based controls embedded within financial management solutions that, if properly implemented and executed, would support compliance. Simply stated, for most companies, the compliance process is difficult and painful.

Many companies are responding to this issue by making their compliance process more top-down and risk-based resulting in, among other things, scoping out low-risk accounts, reducing the number of controls tested and perhaps implementing a self-assessment program. While these steps are appropriate and recommended, they do not address the quality of the controls themselves. Further, they only lead to incremental improvements that will not satisfy cost-conscious executives.

The good news is that SOA only sets compliance objectives. When it issued its rules to implement SOA, the SEC did not prescribe detailed compliance methods. Thus there are no restrictions on "working smarter, not harder." The compliance process doesn't have to be as costly as many companies are making it, especially when one recognizes that a lot of rework occurs in the normal routine of the financial reporting process. By understanding why time-consuming tasks are required to execute financial reporting processes, by identifying root causes and improving processes upstream at the source, and by eliminating nonessential procedures and simplifying, focusing and automating manual activities, there is a significant opportunity to leverage investments from SOA compliance.

A point that is often missed in this conversation is that there is considerable linkage between improving quality, time and cost process performance on the one hand and the effectiveness of internal control over financial reporting on the other hand. Management can't improve one without also improving the other. The message: Companies have opportunities to improve process performance by building-in (versus inspecting-in) quality, compressing time and reducing costs within their processes – and all of this while simultaneously reducing financial reporting risks. For example:

- ***As organizations eliminate nonessentials***, they will sharpen their focus on how they know specific objectives are achieved and examine the need for redundant controls.
- ***As companies simplify, standardize and automate their processes***, there will be greater emphasis on preventive controls (versus the detective controls that institutionalize costly and non-value-added rework into processes) and increased emphasis on systems-based controls (versus the more costly people-based controls).
- ***As efforts to eliminate rework and build quality into processes occur***, companies will reduce the number of manual journal entries required to close the books, streamline account reconciliation activity, deploy available automated controls and reduce the number of spreadsheets by transferring spreadsheet functionality into the organization's ERP system where it belongs.
- ***By improving and taking time out of the financial reporting process***, larger organizations will facilitate continuing compliance with the SEC's accelerated filing requirements.
- ***As all of the above changes occur***, there will be a better mix of preventive and detective controls as well as of automated and manual controls. The result: The internal control structure will become more sustainable over time and the compliance process will be more cost-effective.

The vision is clear: Incremental progress from wrapping the compliance process around the existing internal control structure is not enough. Companies should improve the quality of their processes and controls to maximize the cost-effectiveness of the compliance process. This "project to process" shift in emphasis is where the real value lies and broadens the focus from compliance to operational objectives. While the "total" solution for broader compliance, governance, and risk management does not currently exist, it will likely emerge over time through efforts to integrate several applications and platforms and as companies evolve toward ERM.

OTHER QUESTIONS

155. Will implementation of the COSO Enterprise Risk Management – Integrated Framework prevent fraud?

Think of the COSO Enterprise Risk Management – Integrated Framework as an enhancement to the Internal Control – Integrated Framework. To the extent that elements of internal control are in place to prevent, deter or detect fraud, ERM is intended to enhance internal control in the management of all risks, including fraud risk. For example, the components outlined in the Enterprise Risk Management – Integrated Framework augment the risk assessment process, making it more effective. Risk assessment is vital to an antifraud program. Of course, there are other aspects to an antifraud program that are not explicitly addressed by the ERM framework. See Questions 77 through 81 in Protiviti's *Guide to the Sarbanes-Oxley Act: Internal Control Reporting Requirements*, *Frequently Asked Questions Regarding Section 404*, for a discussion of relevant considerations dealing with fraud. That publication is available at www.protiviti.com.

156. Have any of the companies that have publicly disclosed their ERM processes received any positive feedback from analysts?

Since COSO released the new ERM framework in September of 2004, it is premature to draw conclusions on this point at the time this publication went to print. To date, while there are many examples of companies disclosing risk management practices in place to address specific risks, few companies have disclosed they have implemented enterprise risk management. With time, we expect that to change.

157. Have analysts and others within the investment community or rating agencies expressed their views on how an effectively functioning ERM approach would impact their views of a company?

Since the new ERM framework was released in September of 2004, there hasn't been sufficient time for financial analysts and rating agencies to weigh in with a point of view regarding ERM, as defined by COSO. In the framework, COSO expressed the view that an organization's communications to its stakeholders, to regulators, to financial analysts and to other external parties provides information pertinent to their needs, so they can understand readily the circumstances and risks the entity faces. As entities provide such disclosure, financial analysts and rating agencies will come to expect it.

An entity's dialogue with financial analysts and bond rating agencies can also be an iterative one, in which useful insights may be obtained about perceptions, accurate or inaccurate, regarding the entity. On this point, COSO states the following:

> Financial analysts and bond rating agencies consider many factors relevant to an entity's worthiness as an investment. They analyze management's strategy and objectives, historical financial statements and prospective financial information, actions taken in response to conditions in the economy and marketplace, potential for success in the short and long term, and industry performance and peer group comparisons. The print and broadcast media, particularly financial journalists, also may undertake similar analyses.
>
> The investigative and monitoring activities of these parties can provide insights as to how others perceive the entity's performance, industry and economic risks the entity faces, innovative operating or financing strategies that may improve performance and industry trends. This information is sometimes provided in face-to-face meetings between the parties and management, or indirectly in analyses for investors, potential investors, and the public. In either case, management should consider the observations and insights of financial analysts, bond rating agencies, and the news media that may enhance enterprise risk management.

158. Can all of the information about risk and risk management be classified as attorney-client privileged information, and therefore not be discoverable?

While this is a question for counsel, as a general rule it is doubtful that information about risk and risk management can be classified as "privileged" because that information is so intertwined with the fundamentals of managing the business. Risk management, as an activity, is not often reduced to the narrow

confines of an investigation, but is ordinarily an activity to integrate with the processes of the organization. Managing a business and managing risk should be inextricably tied to each other. That said, situations may arise where some risk issues related to specific compliance matters may be subject to attorney-client privilege. If this is the result a company wants, then management needs to consult with counsel.

159. Since all of this information is presumed to be discoverable, does ERM create more litigation risk for companies?

ERM is designed to help executives better manage the business by making issues and risks within the organization more transparent to management and the board. Admittedly, increased transparency is a double-edged sword that everyone, including the plaintiff bar, can use to achieve his or her purpose. But the real message regarding ERM is that the increased transparency it provides can help management make better choices over time. Nothing will change management's exposure to litigation should something go wrong.

160. Are there any court cases in which a company's management or its board was viewed as deficient because they did not have an adequate risk management system in place?

To our knowledge, we are not aware of the court's taking this point of view on a broad scale. We are aware of court cases in which a company's board was alleged to have failed to have properly supervised the organization's interest rate hedging activities. Risk management has only recently begun to receive emphasis as a tool for augmenting the governance process. It is prudent for management and boards to carefully evaluate their organization's risk management capabilities using the COSO Enterprise Risk Management – Integrated Framework. This would strengthen their assertion that they have designed and implemented an effective risk management process.

161. Are there risks associated with not having an ERM process in place and, if so, what are they?

COSO suggests that CEOs assess their entity's ERM capabilities. COSO also asserts that managers within an enterprise "should consider how they are conducting their responsibilities in light of this framework and discuss with more senior personnel ideas for strengthening enterprise risk management." In addition, COSO encourages internal auditors to "consider the breadth of their focus on enterprise risk management." Without ERM in place, management and directors face the prospect of not having sufficient processes in place that will provide them high confidence that their organization is identifying and managing all potentially significant risks.

162. Is it possible to link an ERM system to an employee's performance and compensation? Are any companies doing this?

Human resource standards are an integral part of the Internal Environment, one of the eight components of the COSO ERM framework. These standards address, among many other things, performance evaluations and compensation programs. Because ERM requires an assessment of the entity's human resource standards, it is appropriate to assess the effectiveness of the organization's processes for setting performance expectations, monitoring and evaluating performance and aligning compensation with performance. In addition, when managing specific risks, an entity's risk response will often require the design and introduction of performance measures to gain further traction in implementing that risk response. With respect to risks susceptible to quantification, it is obviously easier to articulate performance expectations that can be integrated with the reward system. For other risks, a surrogate metric (see Question 112) may be appropriate.

163. Does a third-party certification, rating or other assessment mechanism exist for ERM?

At the present time, a third-party certification, rating or other assessment mechanism has not been established for ERM. We do not expect that to happen for a long time.

164. How does ERM relate to the Basel Capital Accord requiring financial institutions to report on operational risk?

The Basel Committee on Banking Supervision's New Basel Capital Accord (Basel II) updates the 1988 Basel Capital Accord (Basel I) that determines the level of regulatory capital international banks must hold to offset unforeseen risks. This Basel II Accord, negotiated by international banking supervisors, revises the rules for allocating capital for credit risk and introduces a new capital allocation requirement for operational risk. The intent is to foster capital requirements that are more sensitive to risk, so that banks will have greater flexibility to calibrate their capital levels to more accurately reflect the level of risk they face.

The Basel II Capital Accord requires financial institutions to report on operational risk. Although an ERM process would facilitate compliance with these requirements, COSO decided that comparing the ERM framework to the Basel Committee on Banking Supervision's New Basel Capital Accord was beyond the scope of its project. There are many events within the scope of Basel that are highly skewed to capturing those risks that can be most easily quantified, primarily as operating losses for reporting purposes. This is not surprising given that the underlying data is critical for purposes of establishing a statistical basis for the measurement of economic capital requirements. There are risks, however, that may not be as susceptible to such quantification. Because the COSO ERM framework is intended to address all events that could potentially have a significant adverse effect on the achievement of the entity's objectives, including the events falling within the scope of Basel, it is envisioned that compliance with Basel results in an appropriate step toward implementing ERM in financial institutions.

165. What is the difference between ERM and an international standard such as ISO?

COSO included the *International Organization for Standardization, ISO/IEC Guide*, in its bibliography. Thus, the ISO standard provided a source of input to the development of the ERM framework. However, COSO decided that comparing the ERM framework to other frameworks was beyond the scope of the project.

166. How does the COSO Enterprise Risk Management – Integrated Framework integrate with such frameworks as CobiT, ISO 17799, BITS, NIST Special Publication 800-53 and ITIL?

The COSO ERM framework is a broad framework, which encompasses more specific frameworks relating to IT. Once key risks are identified, including IT risks, the organization can utilize the appropriate frameworks, best practices, processes and measures that are best suited to managing and monitoring those risks. COSO decided that comparing the ERM framework to other frameworks was beyond the scope of the project.

167. What is happening in other countries with respect to risk management? Are these developments positively impacting company performance and corporate governance?

Firms listed on the London Stock Exchange and incorporated in the United Kingdom are required to report to shareholders on a set of defined principles relating to corporate governance (known as the Combined Code, and supported with guidance provided by the "Turnbull Report," which was recently updated at the time this publication went to print). The KonTrag legislation in Germany requires large companies to establish risk management supervisory systems and report controls information to shareholders. In addition, there is legislation relating to internal control and risk management in Australia, Canada, France, South Africa, Japan and other countries. Sarbanes-Oxley type legislation continues to arise in countries outside the United States. Whether these developments are positively impacting company performance and corporate governance remains to be proven.

168. Is there a format for communicating our risk management process to our customers in order to align and comply with their requirements?

In the financial services industry, it is not unusual to find risk committee charters on a bank's website. This information is available to anyone who needs it. Outside of financial services, there is not currently a widespread trend of companies requesting information about the risk management processes of other companies, whether they are customers or suppliers. Should that trend emerge, it will be possible to track examples of such reporting.

About Protiviti Inc.

Protiviti is a leading provider of independent internal audit and business and technology risk consulting services. We help clients identify, assess and manage operational and technology-related risks encountered in their industries, and assist in the implementation of the processes and controls to enable their continued monitoring. We also offer a full spectrum of internal audit services focused on bringing the deep skills and technological expertise to enable business risk management and the continual transformation of internal audit functions.

Protiviti has been designated by an independent research firm as a "leader" along with three other consulting firms offering ERM and compliance services. Our enterprise risk management offerings help companies align their strategies, processes, technology and knowledge with the objective of improving their capabilities to evaluate and manage, enterprisewide, the uncertainties they must address as they execute their business model. We offer services in enterprise risk assessments and in specific risk areas around issues companies face as they improve governance and manage technology, operational, compliance and financial risks. Our internal audit services are flexible enough to align our work with the ERM and compliance capabilities our clients have and choose to put in place.

Protiviti's approach to ERM implementation is to offer practical and proven ideas for getting started and help companies develop and implement their own customized approach. Protiviti views ERM as a journey in which organizations redefine the value proposition of risk management by integrating it with strategy-setting. Protiviti's ERM offerings focus on assessing risks enterprisewide, identifying gaps in risk management capabilities and closing gaps by improving risk management capabilities, formulating effective risk responses, improving the ERM infrastructure and training internal staff to ensure continuing effectiveness.

Protiviti has more than 40 locations in North America, Europe, Asia and Australia. The firm is a wholly owned subsidiary of Robert Half International Inc. (NYSE symbol: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

Notes

Notes

North America

UNITED STATES
+1.888.556.7420
protiviti.com

CANADA
+1.416.350.2181
protiviti.ca

Latin America

MEXICO
+52.9171.1501
www.protiviti.com.mx

Europe

FRANCE
+33.1.42.96.22.77
protiviti.fr

ITALY
+39.02.655.06.301
protiviti.it

THE NETHERLANDS
+31.20.346.04.00
protiviti.nl

UNITED KINGDOM
+44.207.930.8808
protiviti.co.uk

Asia-Pacific

AUSTRALIA
+61.3.9948.1200
protiviti.com.au

CHINA
+86.21.63915031
protiviti.cn

JAPAN
+81.3.5219.6600
protiviti.jp

SINGAPORE
+65.6220.6066
protiviti.com.sg

Protiviti is a leading provider of internal audit and risk consulting services. We help clients identify, assess and manage operational and technology-related risks encountered in their industries, and assist in the implementation of the processes and controls to enable their continued monitoring. We also offer a full spectrum of internal audit services focused on bringing the deep skills and technological expertise to enable business risk management and the continual transformation of internal audit functions.

Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.

protiviti.com

1.888.556.7420