Enterprise Risk Management — Integrated Framework

Executive Summary
Framework

September 2004

The Committee of Sponsoring Organizations
of the Treadway Commission

Additional copies of Enterprise Risk Management – Integrated Framework: Executive Summary and Framework and Enterprise Risk Management – Integrated Framework: Application Techniques, 2 vol. set, item #99015 *may be obtained by calling toll free 1-888-777-7077 or visiting www.cpa2biz.com.*

Committee of Sponsoring Organizations of the Treadway Commission (COSO)

Oversight	Representative
COSO Chair	John J. Flaherty
American Accounting Association	Larry E. Rittenberg
American Institute of Certified Public Accountants	Alan W. Anderson
Financial Executives International	John P. Jessup Nicholas S. Cyprus
Institute of Management Accountants	Frank C. Minter Dennis L. Neider
The Institute of Internal Auditors	William G. Bishop, III David A. Richards

Project Advisory Council to COSO

Guidance

Tony Maki, Chair
Partner
Moss Adams LLP

Mark S. Beasley
Professor
North Carolina State University

Jerry W. DeFoor
Vice President and Controller
Protective Life Corporation

James W. DeLoach
Managing Director
Protiviti Inc.

Andrew J. Jackson
Senior Vice President of Enterprise Risk Assurance Services
American Express Company

Steven E. Jameson
Executive Vice President, Chief Internal Audit & Risk Officer
Community Trust Bancorp, Inc.

John P. Jessup
Vice President and Treasurer
E. I. duPont de Nemours and Company

Tony M. Knapp
Senior Vice President and Controller
Motorola, Inc.

Douglas F. Prawitt
Professor
Brigham Young University

PricewaterhouseCoopers LLP

Author

Principal Contributors

Richard M. Steinberg
Former Partner and Corporate Governance Leader (Presently Steinberg Governance Advisors)

Frank J. Martens
Senior Manager, Client Services
Vancouver, Canada

Miles E.A. Everson
Partner and Financial Services Finance, Operations, Risk and Compliance Leader
New York

Lucy E. Nottingham
Manager, Internal Firm Services
Boston

FOREWORD

Over a decade ago, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued *Internal Control – Integrated Framework* to help businesses and other entities assess and enhance their internal control systems. That framework has since been incorporated into policy, rule, and regulation, and used by thousands of enterprises to better control their activities in moving toward achievement of their established objectives.

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. In 2001, COSO initiated a project, and engaged PricewaterhouseCoopers, to develop a framework that would be readily usable by managements to evaluate and improve their organizations' enterprise risk management.

The period of the framework's development was marked by a series of high-profile business scandals and failures where investors, company personnel, and other stakeholders suffered tremendous loss. In the aftermath were calls for enhanced corporate governance and risk management, with new law, regulation, and listing standards. The need for an enterprise risk management framework, providing key principles and concepts, a common language, and clear direction and guidance, became even more compelling. COSO believes this *Enterprise Risk Management – Integrated Framework* fills this need, and expects it will become widely accepted by companies and other organizations and indeed all stakeholders and interested parties.

Among the outgrowths in the United States is the Sarbanes-Oxley Act of 2002, and similar legislation has been enacted or is being considered in other countries. This law extends the long-standing requirement for public companies to maintain systems of internal control, requiring management to certify and the independent auditor to attest to the effectiveness of those systems. *Internal Control – Integrated Framework*, which continues to stand the test of time, serves as the broadly accepted standard for satisfying those reporting requirements.

This *Enterprise Risk Management – Integrated Framework* expands on internal control, providing a more robust and extensive focus on the broader subject of enterprise risk management. While it 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.

Among the most critical challenges for managements is determining how much risk the entity is prepared to and does accept as it strives to create value. This report will better enable them to meet this challenge.

John J. Flaherty
Chair, COSO

Tony Maki
Chair, COSO Advisory Council

Table of Contents

Enterprise Risk Management — Integrated Framework

Executive Summary

September 2004

EXECUTIVE SUMMARY

The underlying premise of enterprise risk management is that every entity exists to provide value for its stakeholders. All entities face uncertainty, and the challenge for management is to determine how much uncertainty to accept as it strives to grow stakeholder value. Uncertainty presents both risk and opportunity, with the potential to erode or enhance value. Enterprise risk management enables management to effectively deal with uncertainty and associated risk and opportunity, enhancing the capacity to build value.

Value is maximized when management sets strategy and objectives to strike an optimal balance between growth and return goals and related risks, and efficiently and effectively deploys resources in pursuit of the entity's objectives. Enterprise risk management encompasses:

- *Aligning risk appetite and strategy* – Management considers the entity's risk appetite in evaluating strategic alternatives, setting related objectives, and developing mechanisms to manage related risks.
- *Enhancing risk response decisions* – Enterprise risk management provides the rigor to identify and select among alternative risk responses – risk avoidance, reduction, sharing, and acceptance.
- *Reducing operational surprises and losses* – Entities gain enhanced capability to identify potential events and establish responses, reducing surprises and associated costs or losses.
- *Identifying and managing multiple and cross-enterprise risks* – Every enterprise faces a myriad of risks affecting different parts of the organization, and enterprise risk management facilitates effective response to the interrelated impacts, and integrated responses to multiple risks.
- *Seizing opportunities* – By considering a full range of potential events, management is positioned to identify and proactively realize opportunities.
- *Improving deployment of capital* – Obtaining robust risk information allows management to effectively assess overall capital needs and enhance capital allocation.

These capabilities inherent in enterprise risk management help management achieve the entity's performance and profitability targets and prevent loss of resources. Enterprise risk management helps ensure effective reporting and compliance with laws and regulations, and helps avoid damage to the entity's reputation and associated consequences. In sum, enterprise risk management helps an entity get to where it wants to go and avoid pitfalls and surprises along the way.

Events – Risks and Opportunities

Events can have negative impact, positive impact, or both. Events with a negative impact represent risks, which can prevent value creation or erode existing value. Events with positive impact may offset negative impacts or represent opportunities. Opportunities are the possibility that an event will occur and positively affect the achievement of objectives, supporting value creation or preservation. Management channels opportunities back to its strategy or objective-setting processes, formulating plans to seize the opportunities.

Enterprise Risk Management Defined

Enterprise risk management deals with risks and opportunities affecting value creation or preservation, defined as follows:

> *Enterprise risk management is 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.*

The definition reflects certain fundamental concepts. 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 that, if they occur, will affect the entity and to manage risk within its risk appetite
- Able to provide reasonable assurance to an entity's management and board of directors
- Geared to achievement of objectives in one or more separate but overlapping categories

This definition is purposefully broad. It captures key concepts fundamental to how companies and other organizations manage risk, providing a basis for application across organizations, industries, and sectors. It focuses directly on achievement of objectives established by a particular entity and provides a basis for defining enterprise risk management effectiveness.

Achievement of Objectives

Within the context of an entity's established mission or vision, management establishes strategic objectives, selects strategy, and sets aligned objectives cascading through the enterprise. This enterprise risk management framework is geared to achieving an entity's objectives, set forth in four categories:

- *Strategic* – high-level goals, aligned with and supporting its mission
- *Operations* – effective and efficient use of its resources
- *Reporting* – reliability of reporting
- *Compliance* – compliance with applicable laws and regulations

This categorization of entity objectives allows a focus on separate aspects of enterprise risk management. These distinct but overlapping categories – a particular objective can fall into more than one category – address different entity needs and may be the direct responsibility of different executives. This categorization also allows distinctions between what can be expected from each category of objectives. Another category, safeguarding of resources, used by some entities, also is described.

Because objectives relating to reliability of reporting and compliance with laws and regulations are within the entity's control, enterprise risk management can be expected to provide reasonable assurance of achieving those objectives. Achievement of strategic objectives and operations objectives, however, is subject to external events not always within the entity's control; accordingly, for these objectives, enterprise risk management can provide reasonable assurance that management, and the board in its oversight role, are made aware, in a timely manner, of the extent to which the entity is moving toward achievement of the objectives.

Components of Enterprise Risk Management

Enterprise risk management consists of eight interrelated components. These are derived from the way management runs an enterprise and are integrated with the management process. These components are:

- *Internal Environment* – The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.
- *Objective Setting* – Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that

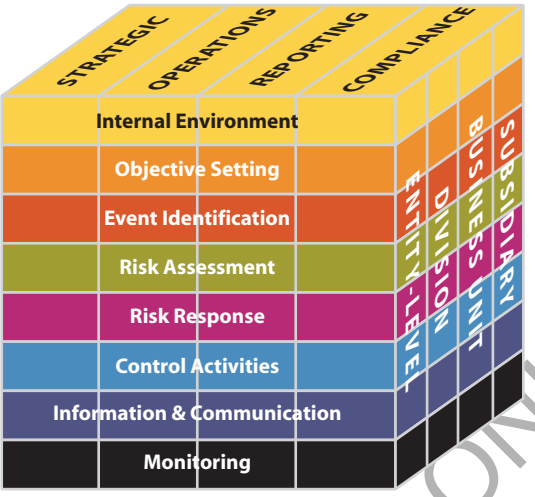
management has in place a process to set objectives and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite.

- *Event Identification* – Internal and external events affecting achievement of an entity's objectives must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management's strategy or objective-setting processes.
- *Risk Assessment* – Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.
- *Risk Response* – Management selects risk responses – avoiding, accepting, reducing, or sharing risk – developing a set of actions to align risks with the entity's risk tolerances and risk appetite.
- *Control Activities* – Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.
- *Information and Communication* – Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across, and up the entity.
- *Monitoring* – The entirety of enterprise risk management is monitored and modifications made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.

Enterprise risk management is not strictly a serial process, where one component affects only the next. It is a multidirectional, iterative process in which almost any component can and does influence another.

Relationship of Objectives and Components

There is a direct relationship between objectives, which are what an entity strives to achieve, and enterprise risk management components, which represent what is needed to achieve them. The relationship is depicted in a three-dimensional matrix, in the form of a cube.



The four objectives categories – strategic, operations, reporting, and compliance – are represented by the vertical columns, the eight components by horizontal rows, and an entity's units by the third dimension. This depiction portrays the ability to focus on the entirety of an entity's enterprise risk management, or by objectives category, component, entity unit, or any subset thereof.

Effectiveness

Determining whether an entity's enterprise risk management is "effective" is a judgment resulting from an assessment of whether the eight components are present and functioning effectively. Thus, the components are also criteria for effective enterprise risk management. For the components to be present and functioning properly there can be no material weaknesses, and risk needs to have been brought within the entity's risk appetite.

When enterprise risk management is determined to be effective in each of the four categories of objectives, respectively, the board of directors and management have reasonable assurance that they understand the extent to which the entity's strategic and operations objectives are being achieved, and that the entity's reporting is reliable and applicable laws and regulations are being complied with.

The eight components will not function identically in every entity. Application in small and mid-size entities, for example, may be less formal and less structured. Nonetheless, small entities still can have effective enterprise risk management, as long as each of the components is present and functioning properly.

Limitations

While enterprise risk management provides important benefits, limitations exist. In addition to factors discussed above, 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 by collusion of two or more people, and management has the ability to override enterprise risk management decisions. These limitations preclude a board and management from having absolute assurance as to achievement of the entity's objectives.

Encompasses Internal Control

Internal control is an integral part of enterprise risk management. This enterprise risk management framework encompasses internal control, forming a more robust conceptualization and tool for management. Internal control is defined and described in *Internal Control – Integrated Framework*. Because that framework has stood the test of time and is the basis for existing rules, regulations, and laws, that document remains in place as the definition of and framework for internal control. While only portions of the text of *Internal Control – Integrated Framework* are reproduced in this framework, the entirety of that framework is incorporated by reference into this one.

Roles and Responsibilities

Everyone in an entity has some responsibility for enterprise risk management. The chief executive officer is ultimately responsible and should assume ownership. Other managers 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. A risk officer, financial officer, internal auditor, and others usually have key support responsibilities. Other entity personnel are responsible for executing enterprise risk management in accordance with established directives and protocols. The board of directors provides important oversight to enterprise risk management, and is aware of and concurs with the entity's risk appetite. A number of external parties, such as customers, vendors, business partners, external auditors, regulators, and financial analysts often provide information useful in effecting enterprise risk management, but they are not responsible for the effectiveness of, nor are they a part of, the entity's enterprise risk management.

Organization of This Report

This report is in two volumes. The first volume contains the *Framework* as well as this *Executive Summary*. The *Framework* defines enterprise risk management and describes principles and concepts, providing direction for all levels of management in businesses and other organizations to use in evaluating and enhancing the effectiveness of enterprise risk management. This *Executive Summary* is a high-level overview directed to chief executives, other senior executives, board members, and regulators. The second volume, *Application Techniques*, provides illustrations of techniques useful in applying elements of the framework.

Use of This Report

Suggested actions that might be taken as a result of this report depend on position and role of the parties involved:

- *Board of Directors* – 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. The board should consider seeking input from internal auditors, external auditors, and others.

- *Senior Management* – This study suggests that the chief executive assess the organization's enterprise risk management capabilities. In one approach, the chief executive brings together business unit heads and key functional staff to discuss an initial assessment of enterprise risk management capabilities and effectiveness. Whatever its form, an initial assessment should determine whether there is a need for, and how to proceed with, a broader, more in-depth evaluation.
- *Other Entity Personnel* – Managers and other personnel 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. Internal auditors should consider the breadth of their focus on enterprise risk management.
- *Regulators* – This framework can promote a shared view of enterprise risk management, including what it can do and its limitations. Regulators may refer to this framework in establishing expectations, whether by rule or guidance or in conducting examinations, for entities they oversee.
- *Professional Organizations* – Rule-making and other professional organizations providing guidance on financial management, auditing, and related topics should consider their standards and guidance in light of this framework. To the extent diversity in concepts and terminology is eliminated, all parties benefit.
- *Educators* – This framework might be the subject of academic research and analysis, to see where future enhancements can be made. With the presumption that this report becomes accepted as a common ground for understanding, its concepts and terms should find their way into university curricula.

With this foundation for mutual understanding, all parties will be able to speak a common language and communicate more effectively. Business executives will be positioned to assess their company's enterprise risk management process against a standard, and strengthen the process and move their enterprise toward established goals. Future research can be leveraged off an established base. Legislators and regulators will be able to gain an increased understanding of enterprise risk management, including its benefits and limitations. With all parties utilizing a common enterprise risk management framework, these benefits will be realized.

Enterprise Risk Management — Integrated Framework

Framework

September 2004

1. DEFINITION

Chapter Summary: All entities face uncertainty, and the challenge for management is to determine how much uncertainty it is prepared to accept as it strives to grow stakeholder value. Enterprise risk management enables management to identify, assess, and manage risks in the face of uncertainty, and is integral to value creation and preservation. Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise. It is designed to identify potential events that may affect the entity, and manage risk to be within the entity's risk appetite, to provide reasonable assurance regarding the achievement of entity objectives. It consists of eight interrelated components, which are integral to the way management runs the enterprise. The components are linked and serve as criteria for determining whether enterprise risk management is effective.

A key objective of this framework is to help managements of businesses and other entities better deal with risk in achieving an entity's objectives. But enterprise risk management means different things to different people, with a wide variety of labels and meanings preventing a common understanding. An important goal, then, is to integrate various risk management concepts into a framework in which a common definition is established, components are identified, and key concepts are described. This framework accommodates most viewpoints and provides a starting point for individual entities' assessment and enhancement of enterprise risk management, for future initiatives of rule-making bodies, and for education.

Uncertainty and Value

An underlying premise of enterprise risk management is that every entity, whether for-profit, not-for-profit, or a governmental body, exists to provide value for its stakeholders. All entities face uncertainty, and the challenge for management is to determine how much uncertainty the entity is prepared to accept as it strives to grow stakeholder value. Uncertainty presents both risk and opportunity, with the potential to erode or enhance value. Enterprise risk management enables management to effectively deal with uncertainty and associated risk and opportunity and thereby enhance the entity's capacity to build value.

Enterprises operate in environments where factors such as globalization, technology, restructurings, changing markets, competition, and regulation create uncertainty. Uncertainty emanates from an inability to precisely determine the likelihood that events will occur and the associated impacts. Uncertainty also is presented and created by the entity's strategic choices. For example, an entity has a growth strategy based on expanding operations to another country. This chosen strategy presents risks and opportunities associated with the stability of the country's political environment, resources, markets, channels, workforce capabilities, and costs.

Value is created, preserved, or eroded by management decisions in all activities, from strategy setting to operating the enterprise day-to-day. Value creation occurs through deploying resources, including people, capital, technology, and brand, where the benefit derived is greater than resources used. Value preservation occurs where created value is sustained through, among other things, superior product quality, production capacity, and customer satisfaction. Value can be eroded where these goals are not achieved due to poor strategy or execution. Inherent in decisions is recognition of risk and opportunity, requiring that management consider information about internal and external environments, deploy precious resources, and recalibrate activities to changing circumstances.

Value is maximized when management sets strategy and objectives to strike an optimal balance between growth and return goals and related risks, and efficiently and effectively deploys resources in pursuit of the entity's objectives. Enterprise risk management encompasses:

- *Aligning risk appetite and strategy* – Management considers the entity's risk appetite first in evaluating strategic alternatives, then in setting objectives aligned with the selected strategy and in developing mechanisms to manage the related risks. For example, a pharmaceutical company has a low risk appetite relative to its brand value. Accordingly, to protect its brand, it maintains extensive protocols to ensure product safety and regularly invests significant resources in early-stage research and development to support brand value creation.
- *Enhancing risk response decisions* – Enterprise risk management provides the rigor to identify and select among alternative risk responses – risk avoidance, reduction, sharing, and acceptance. For example, management of a company that uses company-owned and operated vehicles recognizes risks inherent in its delivery process, including vehicle damage and personal injury costs. Available alternatives include reducing the risk through effective driver recruiting and training, avoiding the risk by outsourcing delivery, sharing the risk via insurance, or simply accepting the risk. Enterprise risk management provides methodologies and techniques for making these decisions.
- *Reducing operational surprises and losses* – Entities gain enhanced capability to identify potential events, assess risk, and establish responses, thereby reducing the occurrence of surprises and related costs or losses. For example, a manufacturing company tracks production parts and equipment failure rates and deviation around averages. The company assesses the impact of failures using multiple criteria, including time to repair, inability to meet customer demand, employee safety, and cost of scheduled versus unscheduled repairs, and responds by setting maintenance schedules accordingly.

- *Identifying and managing cross-enterprise risks* – Every entity faces a myriad of risks affecting different parts of the organization. Management needs to not only manage individual risks, but also understand interrelated impacts. For example, a bank faces a variety of risks in trading activities across the enterprise, and management developed an information system that analyzes transaction and market data from other internal systems, which, together with relevant externally generated information, provides an aggregate view of risks across all trading activities. The information system allows drilldown capability to department, customer or counterparty, trader, and transaction levels, and quantifies the risks relative to risk tolerances in established categories. The system enables the bank to bring together previously disparate data to respond more effectively to risks using aggregated as well as targeted views.
- *Providing integrated responses to multiple risks* – Business processes carry many inherent risks, and enterprise risk management enables integrated solutions for managing the risks. For instance, a wholesale distributor faces risks of over- and under-supply positions, tenuous supply sources, and unnecessarily high purchase prices. Management identified and assessed risk in the context of the company's strategy, objectives, and alternative responses, and developed a far-reaching inventory control system. The system integrates with suppliers, sharing sales and inventory information and enabling strategic partnering, and avoiding stock-outs and unneeded carrying costs, with longer-term sourcing contracts and enhanced pricing. Suppliers take responsibility for replenishing stock, generating further cost reductions.
- *Seizing opportunities* – By considering a full range of potential events, rather than just risks, management identifies events representing opportunities. For example, a food company considered potential events likely to affect its sustainable revenue growth objective. In evaluating the events, management determined that the company's primary consumers are increasingly health conscious and changing their dietary preferences, indicating a decline in future demand for the company's current products. In determining its response, management identified ways to apply its existing capabilities to developing new products, enabling the company not only to preserve revenue from existing customers, but also to create additional revenue by appealing to a broader consumer base.
- *Improving deployment of capital* – Obtaining robust information on risk allows management to effectively assess overall capital needs and enhance capital allocation. For example, a financial institution became subject to new regulatory rules that would increase capital requirements unless management calculated credit and operational risk levels and related capital needs with greater specificity. The company assessed the risk in terms of system development cost versus additional capital costs, and made an informed decision. With existing, readily modifiable software, the institution developed the more precise calculations, avoiding a need for additional capital sourcing.

These capabilities are inherent in enterprise risk management, which helps management achieve the entity's performance and profitability targets and prevent loss of resources. Enterprise risk management helps ensure effective reporting. And it helps ensure that the entity complies with laws and regulations, avoiding damage to its reputation and associated consequences. In sum, enterprise risk management helps an entity get to where it wants to go and avoid pitfalls and surprises along the way.

Events – Risks and Opportunities

An event is an incident or occurrence from internal or external sources that affects achievement of objectives. Events can have negative impact, positive impact, or both. Events with negative impact represent risks. Accordingly, risk is defined as follows:

> *Risk is the possibility that an event will occur and adversely affect the achievement of objectives*.

Events with adverse impact prevent value creation or erode existing value. Examples include plant machinery breakdowns, fire, and credit losses. Events with an adverse impact can derive from seemingly positive conditions, such as where customer demand for product exceeds production capacity, causing failure to meet buyer demand, eroded customer loyalty, and decline in future orders.

Events with positive impact may offset negative impacts or represent opportunities. Opportunity is defined as follows:

> *Opportunity is the possibility that an event will occur and positively affect the achievement of objectives.*

Opportunities support value creation or preservation. Management channels opportunities back to its strategy or objective-setting processes, so that actions can be formulated to seize the opportunities.

Definition of Enterprise Risk Management

Enterprise risk management deals with risks and opportunities to create or preserve value. It is defined as follows:

> *Enterprise risk management is 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 reflects certain fundamental concepts. 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

This definition is purposefully broad for several reasons. It captures key concepts fundamental to how companies and other organizations manage risk, providing a basis for application across types of organizations, industries, and sectors. It focuses directly on achievement of objectives established by a particular entity. And, the definition provides a basis for defining enterprise risk management effectiveness, discussed later in this chapter. The fundamental concepts outlined above are discussed in the following paragraphs.

A Process

Enterprise risk management is not static, but rather a continuous or iterative interplay of actions that permeate an entity. These actions are pervasive and inherent in the way management runs the business.

Enterprise risk management is different from the perspective of some observers who view it as something added on to an entity's activities. That is not to say effective enterprise risk management does not require incremental effort, as it may. In considering credit and currency risks, for example, incremental effort may be required to develop needed models and make necessary analyses and calculations. However, these enterprise risk management mechanisms are intertwined with an entity's operating activities and exist for fundamental business reasons. Enterprise risk management is most effective when these mechanisms are built into the entity's infrastructure and are part of the essence of the enterprise. By building in enterprise risk management, an entity can directly affect its ability to implement its strategy and achieve its mission.

Building in enterprise risk management has important implications for cost containment, especially in the highly competitive marketplaces many companies face. Adding new procedures separate from existing ones adds costs. By focusing on existing operations and their contribution to effective enterprise risk management, and integrating risk management

into basic operating activities, an enterprise can avoid unnecessary procedures and costs. And, a practice of building enterprise risk management into the fabric of operations helps identify new opportunities for management to seize in growing the business.

Effected by People

Enterprise risk management is effected by an entity's board of directors, management and other personnel. It is accomplished by the people of an organization, by what they do and say. People establish the entity's mission, strategy, and objectives, and put enterprise risk management mechanisms in place.

Similarly, enterprise risk management affects people's actions. Enterprise risk management recognizes that people do not always understand, communicate, or perform consistently. Each individual brings to the workplace a unique background and technical ability, and has different needs and priorities.

These realities affect, and are affected by, enterprise risk management. Each person has a unique point of reference, which influences how he or she identifies, assesses, and responds to risk. Enterprise risk management provides the mechanisms needed to help people understand risk in the context of the entity's objectives. People must know their responsibilities and limits of authority. Accordingly, a clear and close linkage needs to exist between people's duties and the way in which they are carried out, as well as with the entity's strategy and objectives.

An organization's people include the board of directors, management and other personnel. Although directors primarily provide oversight, they also provide direction and approve strategy and certain transactions and policies. As such, boards of directors are an important element of enterprise risk management.

Applied in Setting Strategy

An entity sets out its mission or vision and establishes strategic objectives, which are the high-level goals that align with and support its mission or vision. An entity establishes a strategy for achieving its strategic objectives. It also sets related objectives it wants to achieve, flowing from the strategy, cascading to entity business units, divisions, and processes.

Enterprise risk management is applied in strategy setting, in which management considers risks relative to alternative strategies. For instance, one alternative may be to acquire other companies in order to grow market share. Another may be to cut sourcing costs in order to realize higher gross margin percentage. Each of these strategic choices poses a number of risks. If management selects the first strategy, it may have to expand into new and unfamiliar markets, competitors may be able to gain share in the company's existing markets, or the company might not have the capabilities to effectively implement the strategy. With the

second, risks include having to use new technologies or suppliers, or form new alliances. Enterprise risk management techniques are applied at this level to assist management in evaluating and selecting the entity's strategy and related objectives.

Applied Across the Enterprise

In applying enterprise risk management, an entity should consider its entire scope of activities. Enterprise risk management considers activities at all levels of the organization, from enterprise-level activities such as strategic planning and resource allocation, to business unit activities such as marketing and human resources, to business processes such as production and new customer credit review. Enterprise risk management also applies to special projects and new initiatives that might not yet have a designated place in the entity's hierarchy or organization chart.

Enterprise risk management requires an entity to take a *portfolio view* of risk. This might involve each manager responsible for a business unit, function, process, or other activity developing an assessment of risk for the activity. The assessment may be quantitative or qualitative. With a composite view at each succeeding level of the organization, senior management is positioned to make a determination whether the entity's overall risk portfolio is commensurate with its risk appetite.

Management considers interrelated risks from an entity-level portfolio perspective. Risks for individual units of the entity may be within the units' risk tolerances, but taken together may exceed the risk appetite of the entity as a whole. Or, conversely, potential events may represent an otherwise unacceptable risk in one business unit, but with an offsetting effect in another. Interrelated risks need to be identified and acted on so that the entirety of risk is consistent with the entity's risk appetite.

Risk Appetite

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, moderate, 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.

Risk appetite is directly related to an entity's strategy. It is considered in strategy setting, as different strategies expose an entity to different risks. Enterprise risk management helps management select a strategy that aligns anticipated value creation with the entity's risk appetite.

Risk appetite guides resource allocation. Management allocates resources among business units and initiatives with consideration of the entity's risk appetite and the unit's plan for generating desired return on invested resources. Management considers its risk appetite as it aligns its organization, people, and processes, and designs infrastructure necessary to effectively respond to and monitor risks.

Risk tolerances relate to the entity's objectives. 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.

In setting risk tolerance, management considers the relative importance of the related objective and aligns risk tolerances with risk appetite. Operating within risk tolerances helps ensure that the entity remains within its risk appetite and, in turn, that the entity will achieve its objectives.

Provides Reasonable Assurance

Well-designed and operated enterprise risk management can provide management and the board of directors reasonable assurance regarding achievement of an entity's objectives. Reasonable assurance reflects the notion that uncertainty and risk relate to the future, which no one can predict with precision.

Reasonable assurance does not imply that enterprise risk management frequently will fail. Many factors, individually and collectively, reinforce the concept of reasonable assurance. 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. Furthermore, the normal everyday operating activities and responsibilities of people functioning at various levels of an organization are directed at achieving the entity's objectives. Indeed, among a cross-section of well-controlled entities, it is likely that most will be apprised regularly of movement toward their strategic and operations objectives, will achieve compliance objectives regularly, and consistently will produce – period after period, year after year – reliable reports. 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.

Achievement of Objectives

Within the context of the established mission, management establishes strategic objectives, selects strategy, and establishes other objectives cascading through the enterprise and aligned with and linked to the strategy. Although many objectives are specific to a particular entity, some are widely shared. For example, objectives common to virtually all entities are achieving and maintaining a positive reputation within the business and consumer communities, providing reliable reporting to stakeholders, and operating in compliance with laws and regulations.

This framework establishes four categories of entity objectives:

- *Strategic* – relating to high-level goals, aligned with and supporting the entity's mission
- *Operations* – relating to effective and efficient use of the entity's resources
- *Reporting* – relating to the reliability of the entity's reporting
- *Compliance* – relating to the entity's compliance with applicable laws and regulations

This categorization of entity objectives allows a focus on separate aspects of enterprise risk management. These distinct but overlapping categories – a particular objective can fall under more than one category – address different entity needs and may be the direct responsibility of different executives. This categorization also allows distinctions between what can be expected from each category of objectives.

Some entities use another category of objectives, "safeguarding of resources," sometimes referred to as "safeguarding of assets." Viewed broadly, these deal with prevention of loss of an entity's assets or resources, whether through theft, waste, inefficiency, or what turns out to be simply bad business decisions – such as selling product at too low a price, failing to retain key employees or prevent patent infringement, or incurring unforeseen liabilities. These are primarily operations objectives, although certain aspects of safeguarding can fall under other categories. Where legal or regulatory requirements apply, these become compliance issues. When considered in conjunction with public reporting, a narrower definition of safeguarding of assets often is used, dealing with prevention or timely detection of unauthorized acquisition, use, or disposition of an entity's assets that could have a material effect on the financial statements.

Enterprise risk management can be expected to provide reasonable assurance of achieving objectives relating to the reliability of reporting, and compliance with laws and regulations. Achievement of those categories of objectives is within the entity's control and depends on how well the entity's related activities are performed.

However, achievement of strategic objectives, such as attaining a specified market share, and operations objectives, such as successfully launching a new product line, is not always within the entity's control. Enterprise risk management cannot prevent bad judgments or decisions, or external events that can cause a business to fail to achieve operations goals. It does, however, enhance the likelihood that management will make better decisions. For these objectives, enterprise risk management can provide reasonable assurance that management, and the board in its oversight role, are made aware, in a timely manner, of the extent to which the entity is moving toward achievement of the objectives.

Components of Enterprise Risk Management

Enterprise risk management consists of eight interrelated components. These are derived from the way management runs a business and are integrated with the management process. These components are:

- *Internal Environment* – Management sets a philosophy regarding risk and establishes a risk appetite. The internal environment sets the basis for how risk and control are viewed and addressed by an entity's people. The core of any business is its people – their individual attributes, including integrity, ethical values, and competence – and the environment in which they operate.
- *Objective Setting* – Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite.
- *Event Identification* – Potential events that might have an impact on the entity must be identified. Event identification involves identifying potential events from internal or external sources affecting achievement of objectives. It includes distinguishing between events that represent risks, those representing opportunities, and those that may be both. Opportunities are channeled back to management's strategy or objective-setting processes.
- *Risk Assessment* – Identified risks are analyzed in order to form a basis for determining how they should be managed. Risks are associated with objectives that may be affected. Risks are assessed on both an inherent and a residual basis, with the assessment considering both risk likelihood and impact.
- *Risk Response* – Personnel identify and evaluate possible responses to risks, which include avoiding, accepting, reducing, and sharing risk. Management selects a set of actions to align risks with the entity's risk tolerances and risk appetite.
- *Control Activities* – Policies and procedures are established and executed to help ensure the risk responses management selects are effectively carried out.
- *Information and Communication* – Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Information is needed at all levels of an entity for identifying, assessing, and responding to risk. Effective communication also occurs in a broader sense, flowing down, across, and up the entity. Personnel receive clear communications regarding their role and responsibilities.
- *Monitoring* – The entirety of enterprise risk management is monitored, and modifications made as necessary. In this way, it can react dynamically, changing as conditions warrant. Monitoring is accomplished through ongoing management activities, separate evaluations of enterprise risk management, or a combination of the two.

Enterprise risk management is a dynamic process. For example, the assessment of risks drives risk response and may influence control activities and highlight a need to reconsider information and communication needs or the entity's monitoring activities. Thus, enterprise risk management is not strictly a serial process, where one component affects only the next. It is a multidirectional, iterative process in which almost any component can and will influence another.

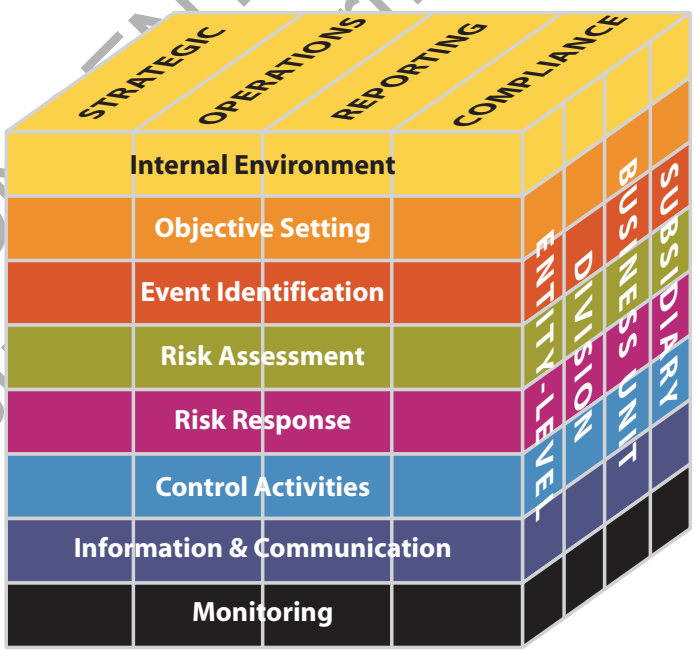
No two entities will, or should, apply enterprise risk management in the same way. Companies and their enterprise risk management capabilities and needs differ dramatically by industry and size, and by management philosophy and culture. Thus, while all entities should have each of the components in place and operating effectively, one company's application of enterprise risk management – including the tools and techniques employed and the assignment of roles and responsibilities – often will look very different from another's.

Relationship of Objectives and Components

There is a direct relationship between objectives, which are what an entity strives to achieve, and the enterprise risk management components, which represent what is needed to achieve them. The relationship is depicted in a three-dimensional matrix, in the shape of a cube, shown in Exhibit 1.1.

Exhibit 1.1

- The four objectives categories – strategic, operations, reporting, and compliance – are represented by the vertical columns
- The eight components are represented by horizontal rows
- The entity and its units are depicted by the third dimension of the cube



Each component row "cuts across" and applies to all four objectives categories. For example, financial and non-financial data generated from internal and external sources, which is part of the information and communication component, is needed to set strategy, effectively manage business operations, report effectively, and determine that the entity is complying with applicable laws.

Similarly, looking at the objectives categories, all eight components are relevant to each. Taking one category, effectiveness and efficiency of operations, for example, all eight components are applicable and important to its achievement.

Enterprise risk management is relevant to an entire enterprise or to any of its individual units. This relationship is depicted by the third dimension, which represents subsidiaries, divisions, and other business units. Accordingly, one could focus on any one of the matrix's cells. For instance, one could consider the top right back cell, representing the internal environment as it relates to compliance objectives of a particular subsidiary.

It should be recognized that the four columns represent categories of an entity's objectives, not parts or units of the entity. Accordingly, when considering the category of objectives related to reporting, for example, knowledge of a wide array of information about the entity's operations is needed. But in that case, focus is on the right-middle column of the model – the reporting objectives – rather than the operations objectives category.

Effectiveness

While enterprise risk management is a process, its effectiveness is a state or condition at a point in time. Determining whether enterprise risk management is "effective" is a judgment resulting from an assessment of whether the eight components are present and functioning effectively. Thus, the components are also criteria for effective enterprise risk management. For the components to be present and functioning properly there can be no material weaknesses, and risk needs to have been brought within the entity's risk appetite.

When enterprise risk management is determined to be effective in each of the four categories of objectives, respectively, the board of directors and management have reasonable assurance that:

- They understand the extent to which the entity's strategic objectives are being achieved
- They understand the extent to which the entity's operations objectives are being achieved
- The entity's reporting is reliable
- Applicable laws and regulations are being complied with

While in order for enterprise risk management to be deemed effective all eight components must be present and functioning properly – applying the principles described in the following chapters – some trade-offs may exist between components. Because enterprise risk management techniques can serve a variety of purposes, techniques applied relative to one component might serve the purpose of techniques normally present in another. Additionally, risk responses can differ in the degree to which they address a particular risk, so that complementary risk responses and controls, each with limited effect, together may be satisfactory.

The concepts discussed here apply to all entities, regardless of size. While some small and mid-size entities may implement component factors differently than large ones, they still can have effective enterprise risk management. The methodology for each component 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.

Enterprise risk management usually is considered in the context of an enterprise as a whole, which involves considering its application in significant business units. There may, however, be circumstances where the effectiveness of enterprise risk management is to be evaluated separately for a particular business unit. In such circumstance, in order to conclude that enterprise risk management for the unit is effective all eight components must be present and functioning effectively in the unit. Thus, for example, because having a board of directors with specified attributes is part of the internal environment, enterprise risk management for a particular business unit may be judged effective only when the unit has in place an appropriately functioning board of directors or similar body (or the entity-level board of directors applies requisite oversight directly to the business unit). Similarly, because the risk response component describes taking a portfolio view of risk, for enterprise risk management to be judged effective there must be a portfolio view of risk for that business unit.

Encompasses Internal Control

Internal control is an integral part of enterprise risk management. This enterprise risk management framework encompasses internal control, forming a more robust conceptualization and tool for management. Internal control is defined and described in *Internal Control – Integrated Framework*. Because *Internal Control – Integrated Framework* is the basis for existing rules, regulations, and laws, and has stood the test of time, that document remains in place as the definition of and framework for internal control. While only portions of the text of *Internal Control – Integrated Framework* are reproduced in this framework, the entirety of *Internal Control – Integrated Framework* is incorporated by reference into this framework. Appendix C describes the relationship between enterprise risk management and internal control.

Enterprise Risk Management and the Management Process

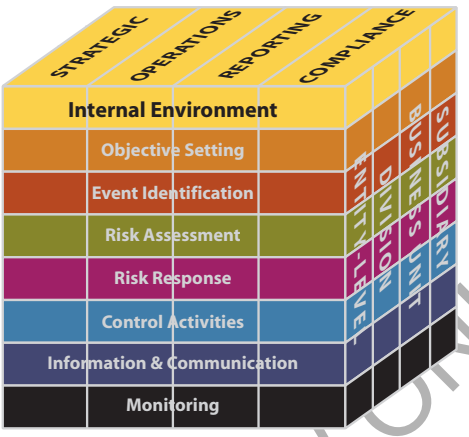
Because enterprise risk management is part of the management process, the enterprise risk management framework components are discussed in the context of what management does in running a business or other entity. But not everything management does is a part of enterprise risk management. Many judgments applied in management's decision making and related management actions, while part of the management process, are not part of enterprise risk management. For example:

- Ensuring there is an appropriate process for objective setting is a critical component of enterprise risk management, but the particular objectives selected by management are not part of enterprise risk management.
- Responding to risks, based on an appropriate assessment of the risks, is a part of enterprise risk management, but the specific risk responses selected and the associated allocation of entity resources are not.
- Establishing and executing control activities to help ensure the risk responses management selects are effectively carried out is a part of enterprise risk management, but the particular control activities chosen are not.

In general, enterprise risk management involves those elements of the management process that enable management to make informed risk-based decisions, but the particular decisions selected from an array of appropriate choices do not determine whether enterprise risk management is effective. However, while the specific objectives, risk responses, and control activities selected are a matter of management judgment, the choices must result in reducing risk to an acceptable level, as determined by risk appetite and reasonable assurance regarding achievement of entity objectives.

2. INTERNAL ENVIRONMENT

Chapter Summary: The internal environment encompasses the tone of an organization, influencing the risk consciousness of its people, and is the basis for all other components of enterprise risk management, providing discipline and structure. Internal environment factors include an entity's risk management philosophy; its risk appetite; oversight by the board of directors; the integrity, ethical values, and competence of the entity's people; and the way management assigns authority and responsibility, and organizes and develops its people.



The internal environment is the basis for all other components of enterprise risk management, providing discipline and structure. It influences how strategies and objectives are established, business activities are structured, and risks are identified, assessed, and acted upon. And it influences the design and functioning of control activities, information and communication systems, and monitoring activities.

The internal environment is influenced by an entity's history and culture. It comprises many elements, including the entity's ethical values, competence and development of personnel, management's philosophy for managing risk, and how it assigns authority and responsibility. A board of directors is a critical part of the internal environment and significantly influences other internal environment elements.

Although all elements are important, the extent to which each is addressed will vary with the entity. For example, the chief executive of a company with a small workforce and centralized operations might not establish formal lines of responsibility and detailed operating policies. Nevertheless, the company could have an internal environment that provides an appropriate foundation for enterprise risk management.

Risk Management Philosophy

An entity's risk management philosophy is the set of shared beliefs and attitudes characterizing how the entity considers risk in everything it does, from strategy development and implementation to its day-to-day activities. Its risk management philosophy reflects the entity's values, influencing its culture and operating style, and affects how enterprise risk management components are applied, including how risks are identified, the kinds of risks accepted, and how they are managed.

A company that has been successful accepting significant risks is likely to have a different outlook on enterprise risk management than one that has faced harsh economic or regulatory consequences as a result of venturing into dangerous territory. While some entities may work to achieve effective enterprise risk management to satisfy requirements of an external stakeholder, such as a parent company or regulator, more often it is because management recognizes that effective risk management helps the entity create and preserve value.

When the risk management philosophy is well developed, understood, and embraced by its personnel, the entity is positioned to effectively recognize and manage risk. Otherwise, there can be unacceptably uneven application of enterprise risk management across business units, functions, or departments. But even when an entity's philosophy is well developed, there nonetheless may be cultural differences among its units, resulting in variation in enterprise risk management application. Managers of some units may be prepared to take more risk, while others are more conservative. For example, an aggressive selling function may focus its attention on making a sale, without careful attention to regulatory compliance matters, while the contracting unit's personnel focus significant attention on ensuring compliance with all relevant internal and external policies and regulations. Separately, these different subcultures could adversely affect the entity. But by working well together the units can appropriately reflect the entity's risk management philosophy.

The enterprise's risk management philosophy is reflected in virtually everything management does in running the entity. It is captured in policy statements, oral and written communications, and decision making. Whether management emphasizes written policies, standards of behavior, performance indicators, and exception reports, or operates more informally largely through face-to-face contact with key managers, of critical importance is that management reinforces the philosophy not only with words but also with everyday actions.

Risk Appetite

Risk appetite is the amount of risk, on a broad level, an entity is willing to accept in pursuit of value. It reflects the enterprise's risk management philosophy, and in turn influences the entity's culture and operating style.

Risk appetite is considered in strategy setting, where the desired return from a strategy should be aligned with the entity's risk appetite. Different strategies will expose the entity to different levels of risk, and enterprise risk management, applied in strategy setting, helps management select a strategy consistent with the entity's risk appetite.

Entities consider risk appetite qualitatively, with such categories as high, moderate, or low, or take a quantitative approach, reflecting and balancing goals for growth and return with risk.

Board of Directors

An entity's board of directors is a critical part of the internal environment and significantly influences its elements. The board's independence from management, experience and stature of its members, extent of its involvement and scrutiny of activities, and appropriateness of its actions all play a role. Other factors include the degree to which difficult questions are raised and pursued with management regarding strategy, plans, and performance, and interaction the board or audit committee has with internal and external auditors.

An active and involved board of directors, board of trustees, or comparable body should possess an appropriate degree of management, technical, and other expertise, coupled with the mind-set necessary to perform its oversight responsibilities. This is critical to an effective enterprise risk management environment. And, because the board must be prepared to question and scrutinize management's activities, present alternative views, and act in the face of wrongdoing, the board must include outside directors.

Members of top management may be effective board members, bringing their deep knowledge of the company. But there must be a sufficient number of independent outside directors not only to provide sound advice, counsel, and direction, but also to serve as a necessary check and balance on management. For the internal environment to be effective, the board must have at least a majority of independent outside directors.

Effective boards of directors ensure that management maintains effective risk management. Although an enterprise historically might have not suffered losses and have no obvious significant risk exposure, the board does not succumb to the mythical notion that events with seriously adverse consequences "couldn't happen here." It recognizes that while a company may have a sound strategy, competent employees, sound business processes, and reliable technology, it, like every entity, is vulnerable to risk, and an effectively functioning risk management process is needed.

Integrity and Ethical Values

An entity's strategy and objectives and the way they are implemented are based on preferences, value judgments, and management styles. Management's integrity and commitment to ethical values influence these preferences and judgments, which are translated into standards of behavior. Because an entity's good reputation is so valuable, the standards of behavior must go beyond mere compliance with law. Managers of well-run enterprises increasingly have accepted the view that ethics pays and ethical behavior is good business.

Management integrity is a prerequisite for ethical behavior in all aspects of an entity's activities. The effectiveness of enterprise risk management cannot rise above the integrity and ethical values of the people who create, administer, and monitor entity activities. Integrity and ethical values are essential elements of an entity's internal environment,

affecting the design, administration, and monitoring of other enterprise risk management components.

Establishing ethical values often is difficult because of the need to consider the concerns of several parties. Management values must balance the concerns of the enterprise, employees, suppliers, customers, competitors, and the public. Balancing these concerns can be complex and frustrating because interests are often at odds. For example, providing an essential product (petroleum, lumber, or food) may cause environmental concerns.

Ethical behavior and management integrity are by-products of the corporate culture, which encompasses ethical and behavioral standards and how they are communicated and reinforced. Official policies specify what the board and management want to happen. Corporate culture determines what actually happens, and which rules are obeyed, bent, or ignored. Top management – starting with the CEO – plays a key role in determining the corporate culture. As the dominant personality in an entity, the CEO often sets the ethical tone.

Certain organizational factors also can influence the likelihood of fraudulent and questionable financial reporting practices. Those same factors are likely to influence ethical behavior as well. Individuals may engage in dishonest, illegal, or unethical acts simply because the entity gives them strong incentives or temptations to do so. Undue emphasis on results, particularly in the short term, can foster an inappropriate internal environment. Focusing solely on short-term results can hurt even in the short term. Concentration on the bottom line – sales or profit at any cost – often evokes unsought actions and reactions. High-pressure sales tactics, ruthlessness in negotiations, or implicit offers of kickbacks, for instance, may evoke reactions that can have immediate (as well as lasting) effects.

Other incentives for engaging in fraudulent or questionable reporting practices and, by extension, other forms of unethical behavior may include rewards highly dependent on reported financial and non-financial information, particularly for short-term results.

Removing or reducing inappropriate incentives and temptations goes a long way toward eliminating undesirable behavior. As suggested, this can be achieved by following sound and profitable business practices. For example, performance incentives – accompanied by appropriate controls – can be a useful management technique as long as the performance targets are realistic. Setting realistic targets is a sound motivational practice, reducing counterproductive stress as well as the incentive for fraudulent reporting. Similarly, a well-controlled reporting system can serve as a safeguard against temptation to misstate performance.

Another cause of questionable practices is ignorance. Ethical values must be not only communicated but also accompanied by explicit guidance regarding what is right and wrong.

Formal codes of corporate conduct are important to and the foundation of an effective ethics program. Codes address a variety of behavioral issues, such as integrity and ethics, conflicts of interest, illegal or otherwise improper payments, and anticompetitive arrangements. Upward communications channels where employees feel comfortable bringing relevant information also are important.

Existence of a written code of conduct, documentation that employees received and understand it, and an appropriate communications channel by themselves do not ensure the code is being followed. Also important to compliance are resulting penalties to employees who violate the code, mechanisms that encourage employee reporting of suspected violations, and disciplinary actions against employees who knowingly fail to report violations. But compliance with ethical standards, whether or not embodied in a written code, is equally if not more effectively ensured by top management's actions and the examples they set. Employees are likely to develop the same attitudes about right and wrong – and about risks and controls – as those shown by top management. Messages sent by management's actions quickly become embodied in the corporate culture. And, knowledge that the CEO has "done the right thing" ethically when faced with a tough business decision, sends a powerful message throughout the entity.

Commitment to Competence

Competence reflects the knowledge and skills needed to perform assigned tasks. Management decides how well these tasks need to be accomplished, weighing the entity's strategy and objectives against plans for their implementation and achievement. A trade-off often exists between competence and cost – it is not necessary, for instance, to hire an electrical engineer to change a light bulb.

Management specifies the competency levels for particular jobs and translates those levels into requisite knowledge and skills. The necessary knowledge and skills in turn may depend on individuals' intelligence, training, and experience. Factors considered in developing knowledge and skill levels include the nature and degree of judgment to be applied to a specific job. Often a trade-off can be made between the extent of supervision and the requisite competence level of the individual.

Organizational Structure

An entity's organizational structure provides the framework to plan, execute, control, and monitor its activities. A relevant organizational structure includes defining key areas of authority and responsibility and establishing appropriate lines of reporting. For example, an internal audit function should be structured in a manner that achieves organizational objectivity and permits unrestricted access to top management and the audit committee of the board, and the chief audit executive should report to a level within the organization that allows the internal audit activity to fulfill its responsibilities.

An entity develops an organizational structure suited to its needs. Some are centralized, others decentralized. Some have direct reporting relationships, while others are more of a matrix organization. Some entities are organized by industry or product line, by geographical location or by a particular distribution or marketing network. Other entities, including many state and local governmental units and not-for-profit institutions, are organized by function.

The appropriateness of an entity's organizational structure depends, in part, on its size and the nature of its activities. A highly structured organization with formal reporting lines and responsibilities may be appropriate for a large entity that has numerous operating divisions, including foreign operations. However, such a structure could impede the necessary flow of information in a small company. Whatever the structure, an entity should be organized to enable effective enterprise risk management and to carry out its activities so as to achieve its objectives.

Assignment of Authority and Responsibility

Assignment of authority and responsibility involves the degree to which individuals and teams are authorized and encouraged to use initiative to address issues and solve problems, as well as limits to their authority. It includes establishing reporting relationships and authorization protocols, as well as policies that describe appropriate business practices, knowledge and experience of key personnel, and resources provided for carrying out duties.

Some entities have pushed authority downward to bring decision making closer to front-line personnel. A company may take this tack to become more market-driven or quality-focused – perhaps to eliminate defects, reduce cycle time, or increase customer satisfaction. Alignment of authority and accountability often is designed to encourage individual initiatives, within limits. Delegation of authority means surrendering central control of certain business decisions to lower echelons – to the individuals who are closest to everyday business transactions. This may involve empowerment to sell products at discount prices; negotiate long-term supply contracts, licenses, or patents; or enter alliances or joint ventures.

A critical challenge is to delegate only to the extent required to achieve objectives. This means ensuring that decision making is based on sound practices for risk identification and assessment, including sizing risks and weighing potential losses versus gains in determining which risks to accept and how they are to be managed.

Another challenge is ensuring that all personnel understand the entity's objectives. It is essential that individuals know how their actions are related to one another and contribute to achievement of the objectives.

Increased delegation sometimes is intentionally accompanied by or the result of streamlining or "flattening" the organizational structure. Purposeful structural change to encourage

creativity, taking initiative, and faster response times can enhance competitiveness and customer satisfaction. This increased delegation may carry an implicit requirement for a higher level of employee competence, as well as greater accountability. It also requires effective procedures for management to monitor results so that decisions can be overruled or accepted as necessary. Along with better, market-driven decisions, delegation may increase the number of undesirable or unanticipated decisions. For example, if a district sales manager decides that authorization to sell at 35% off list price justifies a temporary 45% discount to gain market share, management may need to know so that it can overrule or accept such decisions going forward.

The internal environment is greatly influenced by the extent to which individuals recognize that they will be held accountable. This holds true all the way to the chief executive, who, with board oversight, has ultimate responsibility for all activities within an entity.

Additional principles related to roles and responsibilities by parties integral to effective enterprise risk management are set forth in the *Roles and Responsibilities* chapter.

Human Resource Standards

Human resource practices pertaining to hiring, orientation, training, evaluating, counseling, promoting, compensating, and taking remedial actions send messages to employees regarding expected levels of integrity, ethical behavior, and competence. For example, standards for hiring the most qualified individuals, with emphasis on educational background, prior work experience, past accomplishments, and evidence of integrity and ethical behavior, demonstrate an entity's commitment to competent and trustworthy people. The same is true when recruiting practices include formal, in-depth employment interviews and training in the entity's history, culture, and operating style.

Training policies can reinforce expected levels of performance and behavior by communicating prospective roles and responsibilities and by including such practices as training schools and seminars, simulated case studies, and role-playing exercises. Transfers and promotions driven by periodic performance appraisals demonstrate the entity's commitment to advancement of qualified employees. Competitive compensation programs that include bonus incentives serve to motivate and reinforce outstanding performance – although reward systems should be structured, and controls in place, to avoid undue temptation to misrepresent reported results. Disciplinary actions send a message that violations of expected behavior will not be tolerated.

It is essential that employees be equipped to tackle new challenges as issues and risks throughout the entity change and become more complex – driven in part by rapidly changing technologies and increasing competition. Education and training, whether classroom instruction, self-study, or on-the-job training, must help personnel keep pace and deal

effectively with the evolving environment. Hiring competent people and providing one-time training are not enough. The education process is ongoing.

Implications

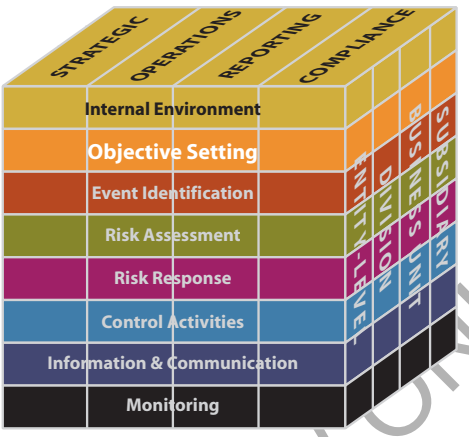
It is difficult to overstate the importance of an entity's internal environment and the impact – positive or negative – it can have on other enterprise risk management components. The impact of an ineffective internal environment can be far-reaching, possibly resulting in financial loss, a tarnished public image, or a business failure.

An energy company generally was thought to have effective enterprise risk management since it had high-powered and respected senior managers, a prestigious board of directors, an innovative strategy, well-designed information systems and control activities, extensive policy manuals prescribing risk and control functions, and comprehensive reconciling and supervisory routines. Its internal environment, however, was significantly flawed. Management participated in highly questionable business practices, and the board turned a "blind-eye." The company was found to have misreported financial results and suffered a loss of shareholder confidence, a liquidity crisis, and destruction of entity value. Ultimately the company went into one of the largest bankruptcies in history.

The attitude and concern of top management for effective enterprise risk management must be definitive and clear, and permeate the organization. It is not sufficient to say the right words. An attitude of "do as I say, not as I do" will only bring about an ineffective environment.

3. OBJECTIVE SETTING

Chapter Summary: Objectives are set at the strategic level, establishing a basis for operations, reporting, and compliance objectives. Every entity faces a variety of risks from external and internal sources, and a precondition to effective event identification, risk assessment, and risk response is establishment of objectives. Objectives are aligned with the entity's risk appetite, which drives risk tolerance levels for the entity.



Objective setting is a precondition to event identification, risk assessment, and risk response. There must first be objectives before management can identify and assess risks to their achievement and take necessary actions to manage the risks.

Strategic Objectives

An entity's mission sets out in broad terms what the entity aspires to achieve. Whatever term is used, such as "mission," "vision," or "purpose," it is important that management – with board oversight – explicitly establish the entity's broad-based reason for being. From this, management sets strategic objectives, formulates strategy, and establishes related operations, compliance, and reporting objectives for the organization. While an entity's mission and strategic objectives are generally stable, its strategy and many related objectives are more dynamic and adjusted for changing internal and external conditions. As they change, strategy and related objectives are realigned with strategic objectives.

Strategic objectives are high-level goals, aligned with and supporting the entity's mission/vision. Strategic objectives reflect management's choice as to how the entity will seek to create value for its stakeholders.

In considering alternative ways to achieve its strategic objectives, management identifies risks associated with a range of strategy choices and considers their implications. Various event identification and risk assessment techniques, discussed below and in later chapters, can be used in the strategy-setting process. In this way, enterprise risk management techniques are used in setting strategy and objectives.

Related Objectives

Establishing the right objectives that support and are aligned with the selected strategy, relative to all entity activities, is critical to success. By focusing first on strategic objectives and strategy, an entity is positioned to develop related objectives at an entity level, achievement of which will create and preserve value. Entity-level objectives are linked to and integrated with more specific objectives that cascade through the organization to sub-objectives established for various activities, such as sales, production, and engineering, and infrastructure functions.

By setting objectives at the entity and activity levels, an entity can identify critical success factors. These are key things that must go right if goals are to be attained. Critical success factors exist for an entity, a business unit, a function, a department, or an individual. By setting objectives, management can identify measurement criteria for performance, with a focus on critical success factors.

Where objectives are consistent with prior practice and performance, the linkage among activities is known. However, where objectives depart from an entity's past practices, management must address the linkages or run increased risks. In such cases, there is an even greater need for business unit objectives or sub-objectives that are consistent with the new direction.

Objectives need to be readily understood and measurable. Enterprise risk management requires that personnel at all levels have a requisite understanding of the entity's objectives as they relate to the individual's sphere of influence. All employees must have a mutual understanding of what is to be accomplished and a means of measuring what is being accomplished.

Categories of Related Objectives

Despite the diversity of objectives across entities, certain broad categories are established:

- *Operations Objectives* – These pertain to the effectiveness and efficiency of the entity's operations, including performance and profitability goals and safeguarding resources against loss. They vary based on management's choices about structure and performance.
- *Reporting Objectives* – These pertain to the reliability of reporting. They include internal and external reporting and may involve financial and non-financial information.
- *Compliance Objectives* – These pertain to adherence to relevant laws and regulations. They are dependent on external factors and tend to be similar across all entities in some cases and across an industry in others.

Certain objectives follow from the business an entity is in. Some companies, for example, submit information to environmental agencies, and publicly traded companies file information with securities regulators. These externally imposed requirements are established by law or regulation, and fall into the reporting or compliance categories or, in these examples, both.

Conversely, operations objectives, as well as those for internal management reporting, are based more on preferences, judgments, and management style. They vary widely among entities simply because informed, competent, and honest people may select different objectives. Regarding product development, for example, one entity chooses to be an early adapter, another a quick follower, and yet another a slow lagger. These choices affect the structure, skills, staffing, and controls of the research and development function. Consequently, no one formulation of objectives is optimal for all entities.

Operations Objectives

Operations objectives relate to the effectiveness and efficiency of the entity's operations. They include related sub-objectives for operations, directed at enhancing operating effectiveness and efficiency in moving the enterprise toward its ultimate goal.

Operations objectives need to reflect the particular business, industry, and economic environments in which the entity functions. The objectives need, for example, to be relevant to competitive pressures for quality, reduced cycle times to bring products to market, or changes in technology. Management must ensure that objectives reflect reality and the demands of the marketplace, and are expressed in terms that allow meaningful performance measurements. A clear set of operations objectives, linked to sub-objectives, is fundamental to success. Operations objectives provide a focal point for directing allocated resources; if an entity's operations objectives are not clear or well conceived, its resources may be misdirected.

Reporting Objectives

Reliable reporting provides management accurate and complete information appropriate for its intended purpose. It supports management's decision making and monitoring of the entity's activities and performance. Examples of such reports include results of marketing programs, daily sales flash reports, production quality, and employee and customer satisfaction results. Reporting also relates to reports prepared for external dissemination, such as financial statements and footnote disclosures, management's discussion and analysis, and reports filed with regulatory agencies.

Compliance Objectives

Entities must conduct their activities, and often must take specific actions, in accordance with relevant laws and regulations. These requirements may relate to markets, pricing, taxes, the environment, employee welfare, and international trade. Applicable laws and regulations establish minimum standards of behavior, which the entity integrates into its compliance

objectives. For example, occupational health and safety regulations cause one company to define its objective as, "Package and label all chemicals in accordance with regulations." In this case, policies and procedures deal with communication programs, site inspections, and training. An entity's compliance record can significantly – either positively or negatively – affect its reputation in the community and marketplace.

Subcategories

The categories of objectives are part of the common language established by this framework, facilitating understanding and communication. An entity may, however, find it useful to discuss a subset of one or more objectives categories, to facilitate communication, internally or externally, on a narrower topic. A company might, for instance, decide to communicate the effectiveness of a part of the reporting category, say, enterprise risk management over external reporting, or perhaps over only external financial reporting. Doing so enables the communication to stay within the context of this enterprise risk management framework, while allowing communications on specific subsets of categories.

Overlap of Objectives

An objective in one category may overlap or support an objective in another. The category in which an objective falls sometimes depends on circumstances. For example, providing reliable information to business unit management to manage and control production activities may serve to achieve both operations and reporting objectives. And, to the extent the information is used for reporting environmental data to the government, it serves compliance objectives.

Some entities use another category of objectives, "safeguarding of resources," sometimes referred to as "safeguarding of assets," which overlaps with the other categories of objectives. Viewed broadly, safeguarding of assets deals with prevention of loss of an entity's assets or resources, whether through theft, waste, inefficiency, or what turns out to be simply bad business decisions – such as selling product at too low a price, failing to retain key employees or prevent patent infringement, or incurring unforeseen liabilities. These are primarily operations objectives, although certain aspects of safeguarding can fall under the other categories. Where legal or regulatory requirements apply, these become compliance objectives. On the other hand, properly reflecting asset losses in the entity's financial statements represents a reporting objective.

When considered in conjunction with public reporting, a narrower definition of safeguarding of assets often is used, dealing with prevention or timely detection of unauthorized acquisition, use, or disposition of an entity's assets. For further discussion of this category of objectives, reference should be made to *Internal Control – Integrated Framework*, including the *Addendum to Reporting to External Parties* module.

Achievement of Objectives

An appropriate process for objective setting is a critical component of enterprise risk management. Although objectives provide the measurable targets toward which the entity moves in conducting its activities, they have differing degrees of importance and priority. Accordingly, while an entity should have reasonable assurance that certain objectives are achieved, that may not be the case for all objectives.

Effective enterprise risk management provides reasonable assurance that an entity's reporting objectives are being achieved. Similarly, there should be reasonable assurance that compliance objectives are being achieved. Achieving reporting and compliance objectives is largely within the entity's control. That is, once the objectives have been determined, the entity has control over its ability to do what is needed to meet them.

But there is a difference when it comes to strategic and operations objectives, because their achievement is not solely within the entity's control. An entity may perform as intended, yet be outperformed by a competitor. It is subject to external events – such as a change in government, poor weather, and the like – where an occurrence is beyond its control. It may even have considered some of these events in its objective-setting process and treated them as having a low likelihood, with a contingency plan in case they occurred. However, such a plan only mitigates the impact of external events. It does not ensure that the objectives will be achieved.

Enterprise risk management over operations focuses primarily on developing consistency of objectives and goals throughout the organization; identifying key success factors and risks; assessing the risks and making informed responses; implementing appropriate risk responses and establishing needed controls; and timely reporting of performance and expectations. For strategic and operations objectives, enterprise risk management can provide reasonable assurance that management and, in its oversight role, the board are made aware, in a timely manner, of the extent to which the entity is moving toward achievement of these objectives.

Selected Objectives

As part of enterprise risk management, management not only selects objectives and considers how they support the entity's mission, but also ensures that they align with the entity's risk appetite. Misalignment could result in not accepting enough risk to achieve the objectives or, conversely, accepting too much risk. Effective enterprise risk management does not dictate which objectives management should choose, but that management has a process that aligns strategic objectives with the entity's mission and that ensures the chosen strategic and related objectives are consistent with the entity's risk appetite.

Risk Appetite

Risk appetite, established by management with oversight of the board of directors, is a guidepost in strategy setting. Companies may express risk appetite as the acceptable balance of growth, risk, and return, or as risk-adjusted shareholder value-added measures. Some entities, such as not-for-profit organizations, express risk appetite as the level of risk they will accept in providing value to their stakeholders.

There is a relationship between an entity's risk appetite and its strategy. Usually any of a number of different strategies can be designed to achieve desired growth and return goals, each having different risks. Enterprise risk management, applied in strategy setting, helps management select a strategy consistent with its risk appetite. If the risk associated with a strategy is inconsistent with the entity's risk appetite, the strategy is revised. This may occur where management initially formulates a strategy that exceeds the entity's risk appetite, or where the strategy does not embrace sufficient risk to allow the entity to achieve its strategic objectives and mission.

The entity's risk appetite is reflected in entity strategy, which in turn guides resource allocation. Management allocates resources across business units, with consideration of the entity's risk appetite and individual business units' strategic plans, to generate a desired return on invested resources. Management looks to align the organization, people, processes, and infrastructure to facilitate successful strategy implementation and enable the entity to stay within its risk appetite.

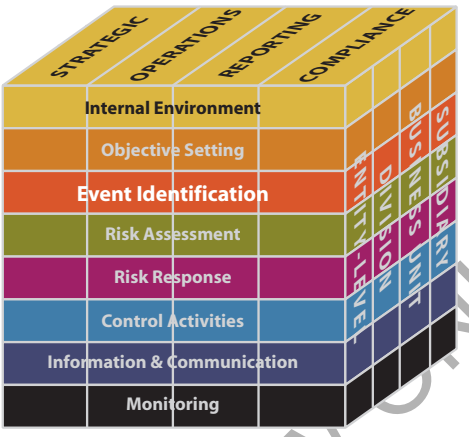
Risk Tolerances

Risk tolerances are the acceptable levels of variation relative to the achievement of objectives. Risk tolerances can be measured, and often are best measured in the same units as the related objectives.

Performance measures are used to help ensure that actual results will be within established risk tolerances. For example, a company targets on-time delivery at 98%, with acceptable variation in the range of 97%–100% of the time; it targets training with a pass rate of 90%, with acceptable performance of at least 75%; and it expects staff to respond to all customer complaints within 24 hours, but accepts that up to 25% of complaints may receive a response within 24–36 hours.

In setting risk tolerances, management considers the relative importance of the related objectives, and aligns risk tolerances with risk appetite. Operating within risk tolerances provides management greater assurance that the entity remains within its risk appetite, which, in turn, provides a higher degree of comfort that the entity will achieve its objectives.

4. EVENT IDENTIFICATION



Chapter Summary: Management identifies potential events that, if they occur, will affect the entity, and determines whether they represent opportunities or whether they might adversely affect the entity's ability to successfully implement strategy and achieve objectives. Events with negative impact represent risks, which require management's assessment and response. Events with positive impact represent opportunities, which management channels back into the strategy and objective-setting processes. When identifying events, management considers a variety of internal and external factors that may give rise to risks and opportunities, in the context of the full scope of the organization.

Events

An event is an incident or occurrence emanating from internal or external sources that affects implementation of strategy or achievement of objectives. Events may have positive or negative impact, or both.

In event identification, management recognizes that uncertainties exist, but does not know whether an event will occur, or when, or its precise impact should it occur. Management initially considers a range of potential events – stemming from both internal and external sources – without necessarily focusing on whether the impact is positive or negative. In this way management identifies not only potential events with negative impact, but also those representing opportunities to be pursued.

Events range from the obvious to the obscure, and the effects from the inconsequential to the highly significant. To avoid overlooking relevant events, identification is best made apart from the assessment of the likelihood of the event occurring and its impact, which is the topic of *Risk Assessment*. However, practical limitations exist, and it is often difficult to know where to draw the line. But even events with a relatively low possibility of occurrence should not be ignored if the impact on achieving an important objective is great.

Influencing Factors

A myriad of external and internal factors drive events that affect strategy implementation and achievement of objectives. As part of enterprise risk management, management recognizes the importance of understanding these external and internal factors and the type of events that can emanate therefrom. External factors, along with examples of related events and their implications, include:

- *Economic* – Related events include price movements, capital availability, or lower barriers to competitive entry, resulting in higher or lower cost of capital and new competitors.
- *Natural environment* – Events include flood, fire, or earthquake, resulting in damage to plant or buildings, restricted access to raw materials, or loss of human capital.
- *Political* – Events include election of government officials with new political agendas, and new laws and regulations, resulting, for example, in newly open or restricted access to foreign markets, or higher or lower taxes.
- *Social* – Events include changing demographics, social mores, family structures, and work/life priorities, and terrorism activity, resulting in changing demand for products and services, new buying venues and human resource issues, and production stoppages.
- *Technological* – Events include new means of electronic commerce, resulting in expanded availability of data, reductions in infrastructure costs, and increased demand for technology-based services.

Events also stem from choices management makes about how it will function. An entity's capability and capacity reflect previous choices, influence future events, and affect management decisions. Internal factors, along with examples of related events and their implications, include:

- *Infrastructure* – Events include increasing capital allocation to preventive maintenance and to call center support, reducing equipment downtime, and improving customer satisfaction.
- *Personnel* – Events include workplace accidents, fraudulent activities, and expiration of labor agreements, resulting in loss of available personnel, monetary or reputational damage, and production stoppages.
- *Process* – Events include process modification without adequate change management protocols, process execution errors, and outsourcing customer delivery with inadequate oversight, resulting in loss of market share, inefficiency, and customer dissatisfaction and loss of repeat business.
- *Technology* – Events include increasing resources to handle volume volatility, security breaches, and potential systems downtime, resulting in backlog reduction, fraudulent transactions, and inability to continue business operations.

Identifying external and internal factors that influence events is useful to effective event identification. Once the major contributing factors are identified, management can consider their significance and focus on events that can affect achievement of objectives.

A manufacturer and importer of footwear, for example, established a vision of being an industry leader in high-quality men's shoes. To achieve this, it set out to manufacture products combining style, comfort, and durability, using the most advanced techniques, together with highly selective import sourcing. The company reviewed its external operating environment and identified social factors and related events such as changing age of its primary consumer market and changing trends in work attire. Events from economic factors included foreign currency fluctuations and interest rate movements. Internal technology factors pointed to an outdated distribution management system, and personnel factors, to inadequate marketing training.

In addition to identifying events at the entity level, events also should be identified at the activity level. This helps focus risk assessment (the subject of the next chapter) on major business units or functions, such as sales, production, marketing, technology development, and research and development.

Event Identification Techniques

An entity's event identification methodology may comprise a combination of techniques, together with supporting tools. For instance, management may use interactive group workshops as part of its event identification methodology, with a facilitator employing any of a variety of technology-based tools to assist participants.

Event identification techniques look to both the past and the future. Techniques that focus on past events and trends consider such matters as payment default histories, changes in commodity prices, and lost-time accidents. Techniques that focus on future exposures consider such matters as shifting demographics, new market conditions, and competitor actions.

Techniques vary widely in level of sophistication. While many of the more sophisticated techniques are industry-specific, most are derived from a common approach. For example, both the financial services and health and safety industries use loss event tracking techniques. These techniques start with a focus on common historical events – where the more basic approaches look at events based on internal staff perceptions, while more advanced techniques are based on factual sources of observable events – and then feed the data into sophisticated projection models. Companies more advanced in enterprise risk management typically employ a combination of techniques that consider both past and potential future events.

Techniques also vary in where they are used within an entity. Some focus on detailed data analysis and create a bottom-up view of events, while others focus top down. Exhibit 4.1 provides examples of event identification techniques.

Exhibit 4.1

- ***Event inventories*** *– These are detailed listings of potential events common to companies within a particular industry, or to a particular process or activity common across industries. Software products can generate relevant lists of generic potential events, which some entities use as a starting point for event identification. For example, a company undertaking a software development project draws on an inventory detailing generic events related to software development projects.*
- ***Internal analysis*** *– This may be done as part of a routine business planning cycle process, typically via a business unit's staff meetings. Internal analysis sometimes utilizes information from other stakeholders (customers, suppliers, other business units) or subject matter expertise outside the unit (internal or external functional experts or internal audit staff). For example, a company considering introduction of a new product utilizes its own historical experience, along with external market research identifying events that have affected the success of competitors' products.*
- ***Escalation or threshold triggers*** *– These triggers alert management to areas of concern by comparing current transactions, or events, with predefined criteria. Once triggered, an event may require further assessment or an immediate response. For example, a company's management monitors sales volume in markets targeted for new marketing or advertising programs and redirects resources based on results. Another company's management tracks competitors' pricing structures and considers changes in its own prices when a specified threshold is met.*
- ***Facilitated workshops and interviews*** *– These techniques identify events by drawing on accumulated knowledge and experience of management, staff, and other stakeholders through structured discussions. The facilitator leads a discussion about events that may affect achievement of entity or unit objectives. For example, a financial controller conducts a workshop with members of the accounting team to identify events that have an impact on the entity's external financial reporting objectives. By combining the knowledge and experience of team members, important events are identified that otherwise might be missed.*
- ***Process flow analysis*** *– This technique considers the combination of inputs, tasks, responsibilities, and outputs that combine to form a process. By considering the internal and external factors that affect inputs to or activities within a process, an entity identifies events that could affect achievement of process objectives. For example, a medical laboratory maps its processes for receipt and testing of blood samples. Using process maps, it considers the range of factors that could affect inputs, tasks, and responsibilities, identifying risks related to sample labeling, handoffs within the process, and personnel shift changes.*

- ***Leading event indicators*** *– By monitoring data correlated to events, entities identify the existence of conditions that could give rise to an event. For example, financial institutions have long recognized the correlation between late loan payments and eventual loan default, and the positive effect of early intervention. Monitoring payment patterns enables the potential for default to be mitigated by timely action.*
- ***Loss event data methodologies*** *– Repositories of data on past individual loss events are a useful source of information for identifying trends and root causes. Once a root cause has been identified, management may find that it is more effective to assess and treat it than to address individual events. For example, a company operating a large fleet of automobiles maintains a database of accident claims and through analysis finds that a disproportionate percentage of accidents, in number and monetary amount, are linked to staff drivers in particular units, geographies, and age bracket. This analysis equips management to identify root causes of events and take action.*

Depth, breadth, timing, and discipline in event identification vary among entities. Management selects techniques that fit its risk management philosophy and ensures that the entity develops needed event identification capabilities and that supporting tools are in place. Overall, event identification needs to be robust, as it forms the basis for the risk assessment and risk response components.

Interdependencies

Events often do not occur in isolation. One event can trigger another, and events can occur concurrently. In event identification, management should understand how events relate to one another. By assessing the relationships, one can determine where risk management efforts are best directed. For example, a change in a central bank interest rate affects foreign exchange rates relevant to a company's currency transaction gains and losses. A decision to curtail capital investment defers an upgrade to distribution management systems, causing additional downtime and increased operating costs. A decision to expand marketing training may improve sales capability and service quality, resulting in an increase in frequency and volume of repeat customer orders. A decision to enter a new line of business, with significant incentives tied to reported performance, can increase risks of error in application of accounting principles and of fraudulent reporting.

Event Categories

It may be useful to group potential events into categories. By aggregating events horizontally across an entity and vertically within operating units, management develops an understanding of relationships between events, gaining enhanced information as a basis for risk assessment. By grouping similar events, management can better determine opportunities and risks.

Event categorization also allows management to consider the completeness of its event identification efforts. For instance, a company may have categorized events related to creditor collections into a single category called creditor defaults. By examining the events in this category, management can gauge whether it has identified all significant potential events related to creditor defaults.

Some companies develop event categories based on categorization of their objectives, using a hierarchy that begins with high-level objectives and then cascades down to objectives relevant to organizational units, functions, or business processes.

Exhibit 4.2 illustrates one approach used in establishing event categories within the context of broad internal and external factors.

Exhibit 4.2

Event Categories	
External Factors	***Internal Factors***
Economic • *Capital availability* • *Credit issuance, default* • *Concentration* • *Liquidity* • *Financial markets* • *Unemployment* • *Competition* • *Mergers/acquisitions* ***Natural Environment*** • *Emissions and waste* • *Energy* • *Natural disaster* • *Sustainable development* ***Political*** • *Governmental changes* • *Legislation* • *Public policy* • *Regulation*	***Infrastructure*** • *Availability of assets* • *Capability of assets* • *Access to capital* • *Complexity* ***Personnel*** • *Employee capability* • *Fraudulent activity* • *Health and safety* ***Process*** • *Capacity* • *Design* • *Execution* • *Suppliers/dependencies* ***Technology*** • *Data integrity* • *Data and system availability* • *System selection* • *Development* • *Deployment* • *Maintenance*

Event Categories	
External Factors	***Internal Factors***
Social • *Demographics* • *Consumer behavior* • *Corporate citizenship* • *Privacy* • *Terrorism* ***Technological*** • *Interruptions* • *Electronic commerce* • *External data* • *Emerging technology*	

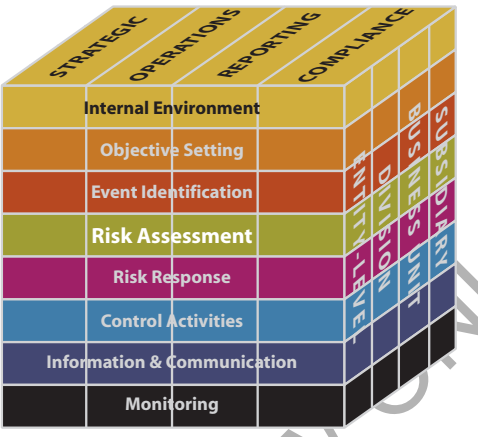
Distinguishing Risks and Opportunities

Events, if they occur, have a negative impact, a positive impact, or both. Events with a negative impact represent risks, which require management's assessment and response. Accordingly, risk is the possibility that an event will occur and adversely affect the achievement of objectives.

Events with a positive impact represent opportunities, or offset the negative impact of risks. Opportunity is the possibility that an event will occur and positively affect the achievement of objectives and creation of value. Events representing opportunities are channeled back to management's strategy or objective-setting processes, so that actions can be formulated to seize the opportunities. Events offsetting the negative impact of risks are considered in management's risk assessment and response.

5. RISK ASSESSMENT

Chapter Summary: Risk assessment allows an entity to consider the extent to which potential events have an impact on achievement of objectives. Management assesses events from two perspectives – likelihood and impact – and normally uses a combination of qualitative and quantitative methods. The positive and negative impacts of potential events should be examined, individually or by category, across the entity. Risks are assessed on both an inherent and a residual basis.



Context for Risk Assessment

External and internal factors influence which events may occur and to what extent the events will affect an entity's objectives. Although some factors are common to companies in an industry, the resulting events often are unique to a particular entity, because of its established objectives and past choices. In risk assessment management considers the mix of potential future events relevant to the entity and its activities in the context of matters that shape the entity's risk profile, such as entity size, complexity of operations, and degree of regulation over its activities.

In assessing risk, management considers expected and unexpected events. Many events are routine and recurring, and are already addressed in management programs and operating budgets, while others are unexpected. Management assesses the risk of unexpected potential events and, if it has not already done so, expected events that can have a significant impact on the entity.

Although the term "risk assessment" sometimes has been used in connection with a one-time activity, in the context of enterprise risk management the risk assessment component is a continuous and iterative interplay of actions that take place throughout the entity.

Inherent and Residual Risk

Management considers both inherent and residual risk. Inherent risk is the risk to an entity in the absence of any actions management might take to alter either the risk's likelihood or impact. Residual risk is the risk that remains after management's response to the risk. Risk assessment is applied first to inherent risks. Once risk responses have been developed, management then considers residual risk.

Estimating Likelihood and Impact

Uncertainty of potential events is evaluated from two perspectives – likelihood and impact. Likelihood represents the possibility that a given event will occur, while impact represents its effect. Likelihood and impact are commonly used terms, although some entities use terms such as probability, and severity, seriousness, or consequence. Sometimes the words take on more specific connotations, with "likelihood" indicating the possibility that a given event will occur in qualitative terms such as high, medium, and low, or other judgmental scales, and with "probability" indicating a quantitative measure such as a percentage, frequency of occurrence, or other numerical metric.

Determining how much attention should be given to assessing the array of risks an entity faces is difficult and challenging. Management recognizes that a risk with a low likelihood of occurrence and little potential impact generally does not warrant further consideration. On the other hand, a risk with high likelihood of occurrence and significant potential impact demands considerable attention. Circumstances in between these extremes usually require difficult judgments. It is important that the analysis be rational and careful.

The time horizon used to assess risks should be consistent with the time horizon of the related strategy and objectives. Because many entities' strategy and objectives focus on short to mid-term time horizons, management naturally focuses on risks associated with those time frames. However, some aspects of strategic direction and objectives extend to the longer term. As a result, management needs to be cognizant of the longer timeframes and not ignore risks that might be further out.

For example, a company operating in California may consider the risk of an earthquake disrupting its business operations. Without a specified risk assessment time horizon, the likelihood of an earthquake exceeding 6.0 on the Richter scale is high, perhaps virtually certain. On the other hand, the likelihood of such an earthquake occurring within two years is substantially lower. By establishing a time horizon, the entity gains greater insight into the relative importance of the risk and an enhanced ability to compare multiple risks.

Management often uses performance measures in determining the extent to which objectives are being achieved and normally uses the same, or congruent, unit of measure when considering the potential impact of a risk on the achievement of a specified objective. A company, for example, with an objective of maintaining a specified level of customer service will have devised a rating or other measure for that objective – such as a customer satisfaction index, number of complaints, or measure of repeat business. When assessing the impact of a risk that might affect customer service – such as the possibility that the company's website might be unavailable for a time period – impact is best determined using the same measures.

Data Sources

Estimates of risk likelihood and impact often are determined using data from past observable events, which provide a more objective basis than entirely subjective estimates. Internally generated data based on an entity's own experience may reflect less subjective personal bias and provide better results than data from external sources. However, even where internally generated data is a primary input, external data can be useful as a checkpoint or to enhance the analysis. For example, a company's management assessing the risk of production stoppages because of equipment failure looks first at frequency and impact of previous failures of its own manufacturing equipment. It then supplements that data with industry benchmarks. This allows a more precise estimate of likelihood and impact of failure, enabling more effective preventive maintenance scheduling. Caution should be exercised when using past events to make predictions about the future, as factors influencing events may change over time.

Perspective

Managers often make subjective judgments about uncertainty, and in doing so they should recognize inherent limitations. Findings in psychology research indicate that decision makers in a variety of capacities, including business managers, are overconfident in their estimation abilities and do not recognize the amount of uncertainty that actually exists. Studies show a marked "overconfidence bias," leading to inappropriately narrow confidence intervals around estimated amounts or likelihoods as applied, for example, in value-at-risk methodologies. This tendency toward overconfidence in estimating uncertainty can be minimized by effective use of internally or externally generated empirical data. In the absence of such data, a keen awareness of the pervasiveness of the bias can help mitigate the effects of overconfidence.

Human tendencies around decision making are exhibited in another way, where it is not uncommon for personnel to make different choices in pursuit of gains versus avoiding losses. By recognizing these human tendencies, managers can frame information to reinforce the risk appetite and behavior throughout the entity. How information is presented or "framed" can significantly affect how the information is interpreted and how the associated risks or opportunities are viewed, as highlighted in Exhibit 5.1.

Exhibit 5.1

Individuals have different responses to potential losses compared with potential gains. How a risk is framed – focusing on the upside (a potential gain) or downside (a potential loss) – often will influence the response. Prospect theory, which explores human decision making, says that individuals are not risk neutral; rather, a response to loss tends to be more extreme than a response to gain. And with this comes a tendency to misinterpret probabilities and best solution reactions. To illustrate, an individual is confronted with two sets of choices:

1. A sure gain of $240, or
a 25% chance to gain $1,000 and a 75% chance to gain nothing.

2. A sure loss of $750, or
a 75% chance to lose $1,000 and a 25% chance to lose nothing.

In the first set of choices, most people select a "sure gain of $240," due to tendencies to be risk averse concerning gain and positively framed questions. In contrast, most people select a "75% chance to lose $1,000," due to a tendency to be risk seeking concerning losses and negatively framed questions. Prospect theory holds that people do not want to put at risk what they already have or think they can have, but they will have higher risk tolerances when they think they can minimize losses.

Assessment Techniques

An entity's risk assessment methodology comprises a combination of qualitative and quantitative techniques. Management often uses qualitative assessment techniques where risks do not lend themselves to quantification or when either sufficient credible data required for quantitative assessments is not practically available or obtaining or analyzing data is not cost-effective. Quantitative techniques typically bring more precision and are used in more complex and sophisticated activities to supplement qualitative techniques.

Quantitative assessment techniques usually require a higher degree of effort and rigor, sometimes using mathematical models. Quantitative techniques are highly dependent on the quality of the supporting data and assumptions, and are most relevant for exposures that have a known history and frequency of variability and allow reliable forecasting. Exhibit 5.2 provides examples of quantitative risk assessment techniques.

Exhibit 5.2

- ***Benchmarking –*** *A collaborative process among a group of entities, benchmarking focuses on specific events or processes, compares measures and results using common metrics, and identifies improvement opportunities. Data on events, processes, and measures are developed to compare performance. Some companies use benchmarking to assess the likelihood and impact of potential events across an industry.*
- ***Probabilistic Models –*** *Probabilistic models associate a range of events and the resulting impact with the likelihood of those events based on certain assumptions. Likelihood and impact are assessed based on historical data or simulated outcomes reflecting assumptions of future behavior. Examples of probabilistic models include value at risk, cash flow at risk, earnings at risk, and development of credit and operational loss distributions. Probabilistic models may be used with different time horizons to estimate such outcomes as the range of values of financial instruments*

over time. Probabilistic models also may be used to assess expected or average outcomes versus extreme or unexpected impacts.

- ***Non-probabilistic Models** – Non-probabilistic models use subjective assumptions in estimating the impact of events without quantifying an associated likelihood. Assessing the impact of events is based on historical or simulated data and assumptions of future behavior. Examples of non-probabilistic models include sensitivity measures, stress tests, and scenario analyses.*

To gain consensus on likelihood and impact using qualitative assessment techniques, entities may employ the same approach they use in identifying events, such as interviews and workshops. A risk self-assessment process captures participants' views on the potential likelihood and impact of future events, using either descriptive or numerical scales.

An entity need not use common assessment techniques across all business units. Rather, the choice of techniques should reflect the need for precision and the culture of the business unit. In one company, for example, in identifying and assessing risk at a process level, one business unit uses self-assessment questionnaires while another uses workshops. The risks are assessed on an inherent and a residual basis, and then organized and grouped by risk categories and objectives for both business units. Although different methods are used, they provide sufficient consistency to facilitate assessment of risks across the entity.

Management is able to derive an entity-wide quantitative impact measure of an event when all of the individual risk assessments for that event are expressed in quantitative terms. For example, the impact on gross margin of a change in energy prices is computed across business units and an entity-wide impact is determined. Where there is a blend of qualitative and quantitative measures, management develops a qualitative assessment across both the qualitative and quantitative measures, with the resulting composite assessment expressed in qualitative terms. Establishing common likelihood and impact terms across an entity and common risk categories for qualitative measures facilitates these composite assessments of risk.

Relationships between Events

Where potential events are not related, management assesses them individually. For example, a company with business units with exposure to different price fluctuations – such as pulp and foreign currency – would assess the risks separately relative to market movements. But where correlation exists between events, or events combine and interact to create significantly different probabilities or impacts, management assesses 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.

For example, a defective valve on a propane tank in a distribution warehouse allows propane to leak; the warehouse doors are kept closed to retain heat in adjoining offices; the driver of an approaching truck activates a remote control device to open the warehouse doors. Together, the presence of propane gas and spark caused by the garage-door motor results in an explosion. These distinct events interact and result in a significant risk. In another example, a company enters a foreign market with new locally hired managers, untested reporting systems, and little basis for central management to judge relative performance, with a resulting significant risk of erroneous or fraudulent reporting.

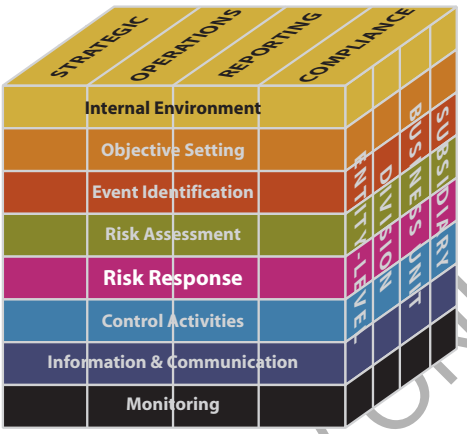
Where risks are likely to affect multiple business units, management may group them into common event categories, and consider them first by unit and then together on an entity-wide basis. For example, a financial services company's business units are subject to risk of a change in government interest rates, and its management assesses the risk not only on each individual business unit but also on a combined, entity-wide basis. A manufacturing company has multiple business units, each with exposure to gold price fluctuations; management aggregates the risk of potential shifts in the price of gold into a single measure showing the net effect of a $1/ounce shift on its total gold inventory.

The nature of events, and whether they are related, may affect assessment techniques used. For example, in assessing the impact of events that could have extreme impact, management may use stress testing, whereas in assessing the effects of multiple events, management might find simulations or scenario analysis more useful.

Looking at interrelationships of risk likelihood and impact is an important management responsibility. Effective enterprise risk management requires that risk assessment be done both with respect to inherent risk and also following risk response, as discussed in the next chapter.

6. RISK RESPONSE

Chapter Summary: Having assessed relevant risks, management determines how it will respond. Responses include risk avoidance, reduction, sharing, and acceptance. In considering its response, management assesses the effect on risk likelihood and impact, as well as costs and benefits, selecting a response that brings residual risk within desired risk tolerances. Management identifies any opportunities that might be available, and takes an entity-wide, or portfolio, view of risk, determining whether overall residual risk is within the entity's risk appetite.



Risk responses fall within the following categories:

- *Avoidance* – Exiting the activities giving rise to risk. Risk avoidance may involve exiting a product line, declining expansion to a new geographical market, or selling a division.
- *Reduction* – Action is taken to reduce risk likelihood or impact, or both. This typically involves any of a myriad of everyday business decisions.
- *Sharing* – Reducing risk likelihood or impact by transferring or otherwise sharing a portion of the risk. Common techniques include purchasing insurance products, engaging in hedging transactions, or outsourcing an activity.
- *Acceptance* – No action is taken to affect risk likelihood or impact.

Exhibit 6.1 provides examples of how these risk responses are applied.

Exhibit 6.1

Avoidance *– A not-for-profit organization identified and assessed risks of providing direct medical services to its members and decided not to accept the associated risks. It decided instead to provide a referral service.*

Reduction *– A stock-clearing corporation identified and assessed the risk of its systems not being available for more than three hours and concluded that it would not accept the impact of such an occurrence. The company invested in technology with enhanced failure self-detecting and back-up systems to reduce the likelihood of system unavailability.*

Sharing – *A university identified and assessed the risk associated with managing its student dormitories and concluded it did not have the requisite in-house capabilities to effectively manage these large residential properties. The university outsourced the dorm management to a property management company better able to reduce the impact and likelihood of property-related risks.*

Acceptance – *A government agency identified and assessed the risks of fire to its infrastructure across diverse geographical regions and assessed the cost of sharing the impact of its risk through insurance coverage. It concluded that the incremental cost of insurance and related deductibles exceeded the likely cost of replacement and decided to accept this risk.*

The avoidance response suggests that no response option was identified that would reduce the impact and likelihood to an acceptable level. Reduction and sharing responses reduce residual risk to a level aligned with desired risk tolerances, while an acceptance response suggests that inherent risk already is within risk tolerances.

For many risks, appropriate response options are obvious and well accepted. For instance, for the risk of losing computing availability, a typical response option is implementation of a business continuity plan. For other risks, available options might not be readily apparent, requiring investigation and analysis. For example, response options relevant to mitigating the effect of competitor activities on brand value might require market research and analysis.

In determining risk response, management should consider such things as:

- Effects of potential responses on risk likelihood and impact – and which response options align with the entity's risk tolerances
- Costs versus benefits of potential responses
- Possible opportunities to achieve entity objectives going beyond dealing with the specific risk

For significant risks, an entity typically considers potential responses from a range of response options. This gives depth to response selection and challenges the "status quo."

Evaluating Possible Responses

Inherent risks are analyzed and responses evaluated with the intent of achieving a residual risk level aligned with the entity's risk tolerances. Often, any of several responses will bring residual risk in line with risk tolerances, and sometimes a combination of responses provides the optimum result. Conversely, sometimes one response will affect multiple risks, in which case management may decide that additional actions to address a particular risk are not needed.

Evaluating Effect on Risk Likelihood and Impact

In evaluating response options, management considers the effect on both risk likelihood and impact, recognizing that a response might affect likelihood and impact differently. For example, a company with a computer center located in a region with heavy storm activity establishes a business continuity plan, which, while having no effect on likelihood of a storm, mitigates the impact of building damage or personnel being unable to get to work. On the other hand, the choice to move the computer center to another region will not reduce the impact of a comparable storm, but does reduce the likelihood of a storm occurring in the first place.

In analyzing responses, management may consider past events and trends, and potential future scenarios. In evaluating alternative responses, management typically determines their potential effect using the same, or congruent, units of measure as those used for the related objective.

Assessing Costs versus Benefits

Resources always have constraints, and entities must consider the relative costs and benefits of alternative risk response options. Cost and benefit measurements for implementing risk responses are made with varying levels of precision. Generally, it is easier to deal with the cost side of the equation, which, in many cases, can be quantified fairly precisely. All direct costs associated with instituting a response, and indirect costs where practically measurable, usually are considered. Some entities also include opportunity costs associated with use of resources.

In some cases, however, it is difficult to quantify costs of risk response. Challenges in quantification arise in estimating time and effort associated with a particular response, as may be the case, for example, in capturing market intelligence on evolving customer preferences, competitors' activities, or other externally generated information.

The benefit side often involves even more subjective valuation. For example, benefits of effective training programs usually are apparent, but difficult to quantify. In many cases, however, the benefit of a risk response can be evaluated in the context of the benefit associated with achievement of the related objective.

When considering cost–benefit relationships, looking at risks as interrelated allows management to pool the entity's risk reduction and risk sharing responses. For instance, when sharing risk via insurance, it may be beneficial to combine risks under one policy since pricing usually is reduced when combined exposures are insured under one financing arrangement.

Opportunities in Response Options

The event identification chapter describes how management identifies potential events affecting achievement of entity objectives, either positively or negatively. Events with positive impacts represent opportunities and are channeled back to the strategy or objective-setting processes.

Similarly, opportunities may be identified when considering risk response. Risk response considerations should not be limited solely to reducing identified risks, but also should include consideration of new opportunities for the entity. Management may identify innovative responses, which, while fitting within the response categories described earlier in this chapter, may be entirely new to the entity or even an industry. Such opportunities may surface when existing risk response options are reaching the limit of effectiveness, and when further refinements likely will provide only marginal changes to a risk impact or likelihood. An example is the creative response by an automobile insurance company to the high number of accidents at certain road intersections – it decided to fund enhancements to traffic signal lights, reducing accident claims and improving margins.

Selected Responses

Once the effects of alternative risk responses have been evaluated, management decides how it intends to manage the risk, selecting a response or combination of responses designed to bring risk likelihood and impact within risk tolerances. The response need not necessarily result in the least amount of residual risk. But where a risk response would result in residual risk exceeding risk tolerance, management revisits and revises the response accordingly or, in certain instances, reconsiders the established risk tolerance. Accordingly, the balancing of risk and risk tolerance may involve an iterative process.

Evaluating alternative responses to inherent risk requires consideration of additional risks that might result from a response. This also may prompt an iterative process whereby before management finalizes a decision, it considers these additional risks, including any that might not be immediately evident.

Once management selects a response, it may need to develop an implementation plan to execute the response. A critical part of an implementation plan is establishing control activities (discussed in the next chapter) to ensure the risk response is carried out.

Management recognizes that some level of residual risk will always exist, not only because resources are limited, but also because of future uncertainty and limitations inherent in all activities.

Portfolio View

Enterprise risk management requires that risk be considered from an entity-wide, or portfolio**,** perspective. Management typically takes an approach in which risk first is considered for each business unit, department, or function, with the responsible manager developing a composite assessment of risks for the unit reflecting the unit's residual risk profile relative to its objectives and risk tolerances.

With a view of risk for individual units, an enterprise's senior management is well positioned to take a portfolio view, to determine whether the entity's residual risk profile is commensurate with its overall risk appetite relative to its objectives. Risks in different units may be within the risk tolerances of the individual units, but, taken together, 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 of risk can be depicted in any of a variety of ways. A portfolio view may be gained by focusing on major risks or event categories across business units, or on risk for the company as a whole, using such metrics as risk-adjusted capital or capital at risk. Such composite measures are particularly useful when measuring risk against objectives stated in terms of earnings, growth, and other performance measures, sometimes relative to allocated or available capital. Such portfolio view measures can provide information useful in reallocating capital across business units and modifying strategic direction.

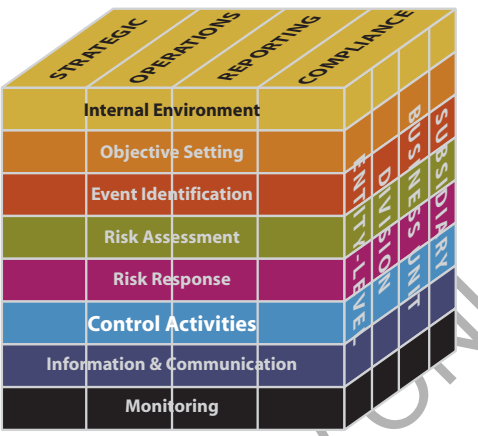
One example is a manufacturing company that takes a portfolio view of risk in the context of its operating earnings objective. Management uses common event categories to capture risks across its business units. It then develops a graph showing, by category and business unit, the risk likelihood in terms 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.

Another example is a financial institution that 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 units' combined risk assessments into a portfolio view of risk for the institution as a whole, enabling management to consider the units' risks, by objective, and determine whether the entity is within its risk appetite.

When looking at risk from a portfolio perspective, management is positioned to consider whether it remains with the established risk appetite. Further, it can reevaluate the nature and type of risk it wishes to take. In cases where the portfolio view shows risks significantly less than the entity's risk appetite, management may decide to motivate individual business unit managers to accept greater risk in targeted areas, striving to enhance the entity's overall growth and return.

7. CONTROL ACTIVITIES

Chapter Summary: Control activities are the policies and procedures that help ensure that management's risk responses are carried out. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities – as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, and segregation of duties.



Control activities are policies and procedures, which are the actions of people to implement the policies, directly or through application of technology, to help ensure that management's risk responses are carried out. Control activities can be categorized based on the nature of the entity's objectives to which they relate: strategic, operations, reporting, and compliance.

Although some control activities relate solely to one category, there often is overlap. Depending on circumstances, a particular control activity could help satisfy entity objectives in more than one of the categories. For example, certain operations controls also can help ensure reliable reporting, reporting control activities can serve to effect compliance, and so on.

Integration with Risk Response

Having selected risk responses, management identifies control activities needed to help ensure that the risk responses are carried out properly and in a timely manner.

Linkage of objectives, risk responses, and control activities is illustrated in the following example: A company sets an objective to meet or exceed sales targets, identifying as a risk failing to have sufficient knowledge of external factors such as current and potential customers' needs. To reduce the likelihood of occurrence and impact of the risk, management establishes buying histories of existing customers and undertakes new market research initiatives. These risk responses serve as focal points for the establishment of control activities, including tracking progress of development of customer buying histories against established timetables, and taking steps to ensure the accuracy of reported data. In this sense, control activities are built directly into the management process.

In selecting control activities, management considers how control activities are related to one another. In some instances, a single control activity addresses multiple risk responses. In other instances, multiple control activities are needed for one risk response. In still others,

management might find that existing control activities are sufficient to ensure that new risk responses are executed effectively.

While control activities generally are established to ensure risk responses are appropriately carried out, with respect to certain objectives, control activities themselves are the risk response. For instance, for an objective to ensure specified transactions are properly authorized, the response will likely be control activities such as segregation of duties and approvals by supervisory personnel.

Just as selection of risk responses considers their appropriateness and remaining, or residual, risk, selection or review of control activities should include consideration of their relevance and appropriateness to the risk response and related objective. This may be accomplished by separate consideration of the propriety of the control activities, or by considering residual risk in the context of both the risk response and related control activities.

Control activities are an important part of the process by which an enterprise strives to achieve its business objectives. Control activities are not performed simply for their own sake or because it seems to be the "right or proper" thing to do. In the example above, management needs to take steps to ensure that sales targets are met. Control activities serve as mechanisms for managing the achievement of that objective.

Types of Control Activities

Many different descriptions of types of control activities have been put forth, including preventive, detective, manual, computer, and management controls. Control activities also can be typed by specified control objectives, such as ensuring completeness and accuracy of data processing.

Exhibit 7.1 describes commonly used control activities. These are just a few among many procedures commonly performed by personnel at various organizational levels that serve to enforce adherence to established action plans and to keep entities on track toward achieving their objectives. They are presented to illustrate the range and variety of control activities, not to suggest any particular categorization.

Exhibit 7.1

- ***Top-level reviews*** *– Senior management reviews actual performance versus budgets, forecasts, prior periods, and competitors. Major initiatives are tracked – such as marketing thrusts, improved production processes, and cost containment or reduction programs – to measure the extent to which targets are being reached. Implementation of plans is monitored for new product development, joint ventures, or financing.*
- ***Direct functional or activity management*** *– Managers running functions or activities review performance reports. A manager responsible for a bank's consumer loans*

reviews reports by branch, region, and loan (collateral) type, checking summarizations and identifying trends, and relating results to economic statistics and targets. In turn, branch managers receive data on new business by loan-officer and local-customer segment. Branch managers also focus on compliance issues, reviewing reports required by regulators on new deposits over specified amounts. Reconciliations are made of daily cash flows, with net positions reported centrally for overnight transfer and investment.

- ***Information processing*** *– A variety of controls are performed to check accuracy, completeness, and authorization of transactions. Data entered are subject to on-line edit checks or matching to approved control files. A customer's order, for example, is accepted only after reference to an approved customer file and credit limit. Numerical sequences of transactions are accounted for, with exceptions followed up and reported to supervisors. Development of new systems and changes to existing ones are controlled, as is access to data, files, and programs.*
- ***Physical controls*** *– Equipment, inventories, securities, cash, and other assets are physically secured and periodically counted and compared with amounts shown on control records.*
- ***Performance indicators*** *– Relating different sets of data – operating or financial – to one another, together with analyses of the relationships and investigative and corrective actions, serves as a control activity. Performance indicators include, for example, staff turnover rates by unit. By investigating unexpected results or unusual trends, management identifies circumstances where an insufficient capacity to complete key processes may mean that objectives have a lower likelihood of being achieved. How managers use this information – for operating decisions only, or also to follow up on unexpected results in reporting systems – determines whether analysis of performance indicators serves operational purposes alone or reporting control purposes as well.*
- ***Segregation of duties*** *– Duties are divided, or segregated, among different people to reduce the risk of error or fraud. For instance, responsibilities for authorizing transactions, recording them, and handling the related asset are divided. A manager authorizing credit sales would not be responsible for maintaining accounts receivable records or handling cash receipts. Similarly, salespersons would not have the ability to modify product price files or commission rates.*

Often, a combination of controls is implemented to deal with related risk responses. For example, a company's management sets transaction limits to manage risks related to an investment portfolio, and establishes control activities designed to help ensure the trading limits are not exceeded. Control activities include preventive controls to stop certain transactions before execution, and detective controls to identify other transactions on a timely basis. The control activities combine computer and manual controls, including automated

controls to ensure all information is correctly captured, and routing procedures enabling responsible individuals to authorize or approve investment decisions.

Policies and Procedures

Control activities usually involve two elements: a policy establishing what should be done and procedures to effect the policy. For example, a policy might call for review of customer trading activities by a securities dealer's retail branch manager. The procedure is the review itself, performed in a timely manner and with attention to factors set forth in the policy, such as the nature and volume of securities traded and their relation to customer net worth and age.

Many times, policies are communicated orally. Unwritten policies can be effective where the policy is a long-standing and well-understood practice, and in smaller organizations where communications channels involve few management layers and close interaction with and supervision of personnel. But regardless whether it's written, a policy must be implemented thoughtfully, conscientiously, and consistently. A procedure will not be useful if performed mechanically and without a sharp, continuing focus on conditions to which the policy is directed. Further, it is essential that conditions identified as a result of the procedure be investigated and appropriate corrective actions taken. Follow-up actions might vary depending on the size and organizational structure of an enterprise. They could range from formal reporting processes in a large company – where business units state why targets were not met and what actions are being taken to prevent recurrence – to an owner-manager of a small business walking down the hall to speak with the plant manager about what went wrong and what needs to be done.

Controls over Information Systems

With widespread reliance on information systems to operate an enterprise and meet reporting and compliance objectives, controls are needed over significant systems. Two broad groupings of information systems control activities can be used. The first is general controls, which apply to many if not all application systems and help ensure their continued, proper operation. The second is application controls, which include computerized steps within application software to control the processing. General and application controls, combined with manual process controls where necessary, work together to ensure completeness, accuracy, and validity of information.

General Controls

General controls include controls over information technology management, information technology infrastructure, security management, and software acquisition, development, and maintenance. They apply to all systems – from mainframe to client/server to desktop and portable computer environments. Exhibit 7.2 provides examples of common controls within these categories.

Exhibit 7.2

- ***Information technology management*** *– A steering committee provides oversight, monitoring, and reporting of information technology activities and improvement initiatives.*
- ***Information technology infrastructure*** *– Controls apply to system definition, acquisition, installation, configuration, integration, and maintenance. Controls may include service-level agreements that establish and reinforce system performance, business continuity planning that maintains system availability, tracking network performance for operational failures, and scheduling computer operations. The system software component of information technology infrastructure may include such controls as management or steering committee review and approval of significant new acquisitions, restricting access to system configuration and operating system software, automated reconciliations of data accessed through middleware software, and parity bit detection for communications errors. System software controls also include incident tracking, system logging, and review of reports detailing usage of data-altering utilities.*
- ***Security management*** *– Logical access controls such as secure passwords restrict access at the network, database, and application levels. User accounts and related access privilege controls help restrict authorized users to only applications or application functions needed to do their jobs. Internet firewalls and virtual private networks protect data from unauthorized external access.*
- ***Software acquisition, development, and maintenance*** *– Controls over software acquisition and implementation are incorporated into an established process for managing change, including documentation requirements, user acceptance testing, stress testing, and project risk assessments. Access to source codes is controlled via code library. Software developers work only in segregated development/test environments and do not have access to the production environment. Controls over system changes include required authorization of change requests, review of the changes, approvals, documentation, testing, implications of changes for other information technology components, stress testing results, and implementation protocols.*

Application Controls

Application controls focus directly on completeness, accuracy, authorization, and validity of data capture and processing. They help ensure data are captured or generated when needed, supporting applications are available, and interface errors are detected quickly.

An important objective of application controls is to prevent errors from entering the system, as well as to detect and correct errors once they are present. To do this, application controls often involve computerized edit checks consisting of format, existence, reasonableness, and

other data checks built into applications during development. When properly designed, they can provide control over data entering the system.

Exhibit 7.3 provides examples of application controls. These are just a few among a myriad of controls performed every day, through calculation and comparison, that serve to prevent and detect inaccurate, incomplete, inconsistent, or improper data capture and processing.

Exhibit 7.3

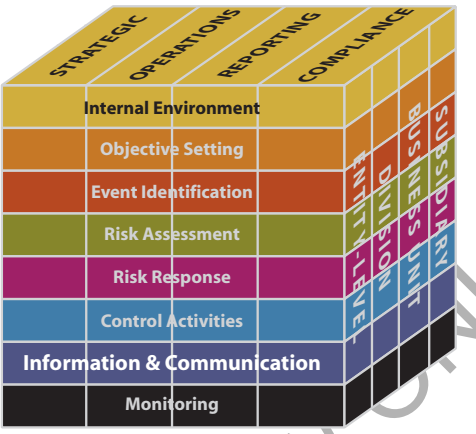
- ***Balancing control activities*** *– Detect data capture errors by reconciling amounts entered, either manually or automatically, to a control total. A company automatically balances the total number of transactions processed and passed from its on-line order entry system to the number of transactions received in its billing system.*
- ***Check digits*** *– Validate data by calculations. A company's part numbers contain a check digit to detect and correct inaccurate ordering from its suppliers.*
- ***Predefined data listings*** *– Provide the user with predefined lists of acceptable data. A company's intranet site includes drop-down lists of products available for purchase.*
- ***Data reasonableness tests*** *– Compare data captured with a present or learned pattern of reasonableness. An order to a supplier by a home renovation retail store for an unusually large number of board feet of lumber triggers a review.*
- ***Logic tests*** *– Include use of range limits or value or alphanumeric tests. A government agency detects potential errors in social security numbers by checking whether all entered numbers contain nine digits.*

Entity Specific

Because each entity has its own set of objectives and implementation approaches, there will be differences in risk responses and related control activities. Even if two entities had identical objectives and made similar decisions on how they should be achieved, the control activities likely would be different. Each entity is managed by different people who use individual judgments in effecting control. Moreover, controls reflect the environment and industry in which an entity operates, as well as the size and complexity of its organization, nature and scope of its activities, its history, and its culture.

Large, complex organizations with diverse activities may face more difficult control issues than small, simple organizations with less varied activities. An entity with decentralized operations, and an emphasis on local autonomy and innovation, presents different control circumstances than a highly centralized one. Other factors that influence an entity's complexity, and therefore the nature of its controls, include location and geographical dispersion, extensiveness and sophistication of operations, and information processing methods.

8. INFORMATION AND COMMUNICATION



Chapter Summary: Pertinent information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Information systems use internally generated data, and information from external sources, providing information for managing risks and making informed decisions relative to objectives. Effective communication also occurs, flowing down, across, and up the organization. All personnel receive a clear message from top management that enterprise risk management responsibilities must be taken seriously. They understand their own role in enterprise risk management, as well as how individual activities relate to the work of others. They must have a means of communicating significant information upstream. There is also effective communication with external parties, such as customers, suppliers, regulators, and shareholders.

Every enterprise identifies and captures a wide range of information, relating to external as well as internal events and activities, relevant to managing the entity. This information is delivered to personnel in a form and timeframe that enable them to carry out their enterprise risk management and other responsibilities.

Information

Information is needed at all levels of an organization to identify, assess, and respond to risks, and to otherwise run the entity and achieve its objectives. An array of information is used, relevant to one or more objectives categories.

Operating information from internal and external sources, both financial and non-financial, is relevant to multiple business objectives. Financial information, for instance, is used in developing financial statements for reporting purposes, and also for operating decisions, such as monitoring performance and allocating resources. Reliable financial information is fundamental to planning, budgeting, pricing, evaluating vendor performance, assessing joint ventures and alliances, and a range of other management activities.

Similarly, operating information is essential for developing financial and other reports. This includes the routine – purchases, sales, and other transactions – as well as information on competitors' product releases or economic conditions, which can affect inventory and receivables valuations. And information needed for compliance purposes, such as information on airborne particle emissions or personnel data, also may serve financial reporting objectives.

Information comes from many sources – internal and external, and in quantitative and qualitative forms – and facilitates responses to changing conditions. A challenge for management is to process and refine large volumes of data into actionable information. This challenge is met by establishing an information systems infrastructure to source, capture, process, analyze, and report relevant information. These information systems – usually computerized but also involving manual inputs or interfaces – often are viewed in the context of processing internally generated data. But information systems have a much broader application. They also deal with information about external events, for example, market- or industry-specific economic data that signals changes in demand for a company's products or services, data on goods and services for production processes, market intelligence on evolving customer preferences or demands, information on competitors' product development activities, and legislative or regulatory initiatives.

Information systems can be formal or informal. Conversations with customers, suppliers, regulators, and entity personnel often provide critical information needed to identify risks and opportunities. Similarly, attendance at professional or industry seminars and memberships in trade and other associations can provide valuable information.

Keeping information consistent with needs is particularly important when an entity faces fundamental industry changes, highly innovative and quick-moving competitors, or significant customer demand shifts. Information systems change as needed to support new objectives. They identify and capture needed financial and non-financial information, and also process and report this information in a timeframe and way that are useful in controlling the entity's activities.

Strategic and Integrated Systems

As enterprises have become more collaborative and integrated with customers, suppliers, and business partners, the division between an entity's information systems architecture and that of external parties is increasingly blurred. As a result, data processing and data management often become a shared responsibility of multiple entities. In such cases, an organization's information systems architecture must be sufficiently flexible and agile to effectively integrate with affiliated external parties.

The design of an information systems architecture and acquisition of technology are important aspects of entity strategy, and choices regarding technology can be critical to achieving objectives. Decisions about technology selection and implementation depend on many factors, including organizational goals, marketplace needs, and competitive requirements. While information systems are fundamental to effective enterprise risk management, risk management techniques can assist in making technology decisions.

Information systems have long been designed and used to support business strategy. This role becomes critical as business needs change and technology creates new opportunities for

strategic advantage. In some cases, changes in technology have reduced the advantage gained in initial deployment, driving new strategic direction. For instance, airline reservation systems that gave travel agents easy access to flight information later moved to customer-facing Internet reservation systems, significantly reducing or eliminating involvement of the traditional travel agent.

Integration with Operations

Information systems often are fully integrated into most aspects of operations. Web and web-based systems are common, with many companies having enterprise-wide information systems such as enterprise resource planning. These applications facilitate access to information previously trapped in functional or departmental silos, making it available for widespread management use. Transactions are recorded and tracked in real time, enabling managers to immediately access financial and operating information more effectively to control business activities. For example, a construction company dealing in multiple large-scale projects uses an integrated, extranet-based system to meet marketplace and efficiency expectations. The system provides information that helps managers track customer-supplied inventory and parts, identify over- or short-supply material at multiple job sites, obtain cost savings with suppliers of common materials or combine with similar organizations to obtain volume discounts, and oversee the subcontractors' activities. It also allows employees to seamlessly share current drawings with architects and engineers, customers, subcontractors, and regulators, while maintaining drawing version control. Additionally, the system encompasses knowledge management capabilities that allow company employees to share innovative solutions throughout the organization.

To support effective enterprise risk management, an entity captures and uses historical and present data. Historical data allows the entity to track actual performance against targets, plans, and expectations. They provide insights into how the entity performed under varying conditions, allowing management to identify correlations and trends, and to forecast future performance. Historical data also can provide early warning of potential events that warrant management attention.

Present or current-state data allows an entity to determine whether it is remaining within established risk tolerances. Such data allows management to take a real-time view of existing risks within a process, function, or unit, and to identify variations from expectations.

Developments in information systems have improved the ability of many organizations to measure and monitor performance and present analytical information at an enterprise level. System complexity and integration continue, with organizations utilizing new technology capabilities as they emerge. However, the growing reliance on information systems at the strategic and operational level brings about new risks – such as information security breaches or cyber-crimes – that must be integrated into the entity's enterprise risk management.

Depth and Timeliness of Information

The information infrastructure sources and captures data in a timeframe and at a depth consistent with an entity's need to identify, assess, and respond to risk, and remain within its risk tolerances. Timeliness of information flow needs to be consistent with the rate of change in the entity's internal and external environments.

The importance of depth of data is illustrated by looking at different events affecting a brokerage firm located in a city susceptible to floods. For business continuity planning, management maintains a general awareness of potential flood conditions and is positioned to advise personnel when to move to back-up facilities. Information captured at this high level is sufficient to allow the firm to adequately manage the risk. In contrast, as a broker, the firm sources and continuously captures changes in stock, bond, and commodity prices to several decimal points. This level of data timeliness and detail is consistent with the firm's need to respond immediately to price changes that may precipitate risks, such as an overexposure to a particular market sector or security inconsistent with the firm's risk appetite.

The information infrastructure converts raw data into relevant information that assists personnel in carrying out their enterprise risk management and other responsibilities. Information is provided in a form and timeframe that are actionable, readily usable, and linked to defined accountabilities.

Advances in data collection, processing, and storage have resulted in exponential growth in data volume. With more data available – often in real time – to more people in an organization, the challenge is to avoid "information overload" by ensuring flow of the right information, in the right form, at the right level of detail, to the right people, at the right time. In developing the knowledge and information infrastructure, consideration should be given to the distinct information requirements of individual users and departments, and to summary-level information needed by different levels of management.

Information Quality

With increasing dependence on sophisticated information systems and data-driven automated decision systems and processes, data reliability is critical. Inaccurate data can result in unidentified risks or poor assessments and bad management decisions.

The quality of information includes ascertaining whether:

- Content is appropriate – Is it at the right level of detail?
- Information is timely – Is it there when required?
- Information is current – Is it the latest available?
- Information is accurate – Is the data correct?
- Information is accessible – Is it easy to obtain by those who need it?

To drive data quality, entities establish enterprise-wide data management programs, encompassing acquisition, maintenance, and distribution of relevant information. Without such programs, information systems might not provide the information that management and other personnel require.

Challenges are many: Conflicting functional needs, system constraints, and non-integrated processes can inhibit data acquisition and its effective use. To meet these challenges, management establishes a strategic plan with clear accountability and responsibilities for data integrity, and performs regular data quality assessments.

Having the right information, on time and at the right place, is essential to effecting enterprise risk management. That is why information systems, while a component of enterprise risk management, also must be controlled.

Communication

Communication is inherent in information systems. As discussed above, information systems must provide information to appropriate personnel so that they can carry out their operating, reporting, and compliance responsibilities. But communication also must take place in a broader sense, dealing with expectations, responsibilities of individuals and groups, and other important matters.

Internal

Management provides specific and directed communication that addresses behavioral expectations and the responsibilities of personnel. This includes a clear statement of the entity's risk management philosophy and approach and a clear delegation of authority. Communication about processes and procedures should align with, and underpin, the desired culture.

Communication should effectively convey:

- The importance and relevance of effective enterprise risk management
- The entity's objectives
- The entity's risk appetite and risk tolerances
- A common risk language
- The roles and responsibilities of personnel in effecting and supporting the components of enterprise risk management

All personnel, particularly those with important operating or financial management responsibilities, need to receive a clear message from top management that enterprise risk management must be taken seriously. Both the clarity of the message and effectiveness with which it is communicated are important.

Personnel also need to know how their activities relate to the work of others. This knowledge is necessary to recognize a problem or determine its cause and corrective action. And, they need to know what is deemed acceptable and unacceptable behavior. There have been well-publicized instances of fraudulent reporting in which managers, under pressure to meet budgets, misrepresented operating results. In a number of these instances, no one had told these individuals that such misreporting could be illegal or otherwise improper. This underscores the critical nature of how messages are communicated within an organization. A manager who instructs subordinates, "Meet the budget – I don't care how you do it, just do it," unwittingly can send the wrong message.

Front-line employees who deal with critical operating issues every day are often in the best position to recognize problems as they arise, and communications channels should ensure personnel can communicate risk-based information across business units, processes, or functional silos, as well as upstream. For example, sales representatives or account managers may learn of important customer product design needs, production personnel may become aware of costly process deficiencies, and purchasing personnel may be confronted with improper incentives from suppliers. Communication breakdowns can occur when individuals or units are discouraged from providing information important to others or do not have a vehicle to provide it. Personnel may be aware of significant risks, but unwilling or unable to report them.

For such information to be reported, there must be open channels of communication and a clear-cut willingness to listen. Personnel must believe their superiors truly want to know about problems and will deal with them effectively. Most managers recognize intellectually that they should avoid "shooting the messenger." But when caught up in everyday pressures, they can be unreceptive to people bringing them legitimate problems. Personnel are quick to pick up on spoken or unspoken signals that a superior doesn't have the time or interest to deal with problems they have uncovered. Compounding such problems, the unreceptive manager is the last to know that the communications channel has been effectively shut down.

In most cases, normal reporting lines in an organization are the appropriate channels of communication. In some circumstances, however, separate lines of communication are needed to serve as a fail-safe mechanism in case normal channels are inoperative. Many companies provide, and make employees aware of, a channel directly to the chief internal auditor or legal counsel or other senior officer having access to the board of directors, along with board or audit committee oversight, and laws and regulations increasingly call on companies to establish these mechanisms. Because of its importance, effective enterprise risk management requires such an alternative communications channel. Without both open communications channels and a willingness to listen, the upward flow of information might be blocked.

It is important that personnel understand that there will be no reprisals for reporting relevant information. A clear message is sent by the existence of mechanisms that encourage employees to report suspected violations of an entity's code of conduct and by the treatment of reporting personnel.

A relevant and comprehensive code of conduct, coupled with employee training sessions, and ongoing corporate communications and feedback mechanisms, along with the right example set by the actions of senior management, can reinforce these important messages.

Among the most critical communications channels is that between top management and the board of directors. Management must keep the board up-to-date on performance, risk, and the functioning of enterprise risk management, and other relevant events or issues. The better the communications, the more effective a board will be in carrying out its oversight responsibilities – acting as a sounding board for management on critical issues, monitoring its activities, and providing advice, counsel, and direction. By the same token, the board should communicate its information needs to management and provide feedback and direction.

External

There needs to be appropriate communication not only within the entity, but with the outside as well. With open external communications channels, customers and suppliers can provide highly significant input on the design or quality of products or services, enabling a company to address evolving customer demands or preferences. For example, customer or supplier complaints or inquiries about shipments, receipts, billings, or other activities often point to operating problems, and possibly to fraudulent or other improper practices. Management should be ready to recognize implications of such circumstances and investigate and take necessary corrective actions, focusing on the impact on financial reporting and compliance as well as operations objectives.

Open communication about the entity's risk appetite and risk tolerances is important, particularly for entities linked with others in supply chains or e-business enterprises. In such instances, management considers how its risk appetite and risk tolerances align with those of its business partners, ensuring it does not inadvertently accept too much risk through its partners.

Communication to stakeholders, regulators, financial analysts, and other external parties provides information relevant to their needs, so they can understand readily the circumstances and risks the entity faces. Such communication should be meaningful, pertinent, and timely, and conform to legal and regulatory requirements.

Management's commitment to communication with external parties – whether open and forthcoming and serious in follow-up, or otherwise – also sends messages throughout the organization.

Means of Communication

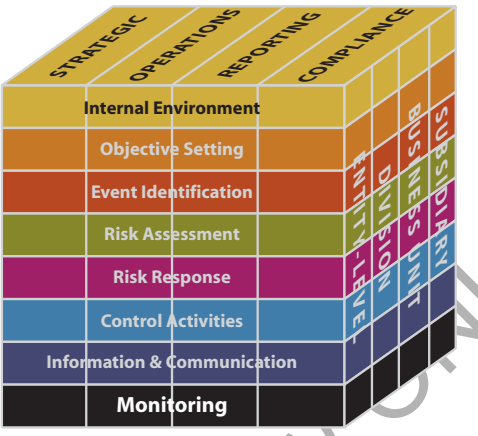
Communication can take such forms as policy manuals, memoranda, e-mails, bulletin board notices, webcasts, and videotaped messages. Where messages are transmitted orally – in large groups, smaller meetings, or one-on-one sessions – tone of voice and body language emphasize what is being said.

The way management deals with personnel can communicate a powerful message. Managers should remember that actions speak louder than words. Their actions are, in turn, influenced by the entity's history and culture, drawing on past observations of how their mentors dealt with similar situations.

An entity with a history of operating with integrity, and whose culture is well understood by people throughout the organization, will likely find little difficulty communicating its message. An entity without such a tradition will need to put more effort into the way messages are communicated.

9. MONITORING

Chapter Summary: Enterprise risk management is monitored – assessing the presence and functioning of its components over time. This is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two. Ongoing monitoring occurs in the normal course of management activities. The scope and frequency of separate evaluations will depend primarily on an assessment of risks and the effectiveness of ongoing monitoring procedures. Enterprise risk management deficiencies are reported upstream, with serious matters reported to top management and the board.



An entity's enterprise risk management changes over time. Risk responses that were once effective may become irrelevant; control activities may become less effective, or no longer be performed; or entity objectives may change. This can be due to the arrival of new personnel, changes in entity structure or direction, or the introduction of new processes. In the face of such changes, management needs to determine whether the functioning of enterprise risk management continues to be effective.

Monitoring can be done in two ways: through ongoing activities or separate evaluations. Enterprise risk management mechanisms usually are structured to monitor themselves on an ongoing basis, at least to some degree. The greater the degree and effectiveness of ongoing monitoring, the less need for separate evaluations. The frequency of separate evaluations necessary for management to have reasonable assurance about the effectiveness of enterprise risk management is a matter of management's judgment. In making that determination, consideration is given to the nature and degree of changes occurring and their associated risks, the competence and experience of the personnel implementing risk responses and related controls, and the results of ongoing monitoring. Usually, some combination of ongoing monitoring and separate evaluations will ensure that enterprise risk management maintains its effectiveness over time.

Ongoing monitoring is built into the normal, recurring operating activities of an entity. Ongoing monitoring is performed on a real-time basis, reacts dynamically to changing conditions, and is ingrained in the entity. As a result, it is more effective than separate evaluations. Since separate evaluations take place after the fact, problems often will be identified more quickly by ongoing monitoring routines. Many entities with sound ongoing monitoring activities nonetheless conduct separate evaluations of enterprise risk management

periodically. An entity that perceives a need for frequent separate evaluations should focus on enhancing ongoing monitoring activities.

Ongoing Monitoring Activities

Many activities serve to monitor the effectiveness of enterprise risk management in the ordinary course of running the business. These stem from regular management activities, which might involve variance analysis, comparisons of information from disparate sources, and dealing with unexpected occurrences.

Ongoing monitoring activities generally are performed by line operating or functional support managers, giving thoughtful consideration to implications of information they receive. By focusing on relationships, inconsistencies, or other relevant implications, they raise issues and follow up with other personnel as necessary to determine whether corrective or other action is called for. Ongoing monitoring activities are differentiated from activities performed as required by policy in business processes. For example, approvals of transactions, reconciliations of account balances, and verifying the accuracy of changes to master files, performed as required steps in information systems or accounting processes, are best defined as control activities.

Exhibit 9.1 includes examples of ongoing monitoring activities.

Exhibit 9.1

- *Managers reviewing operating reports, used to manage operations on an ongoing basis, may spot inaccuracies or exceptions to anticipated results. For example, managers of sales, purchasing, and production at divisional, subsidiary, and corporate levels who are in touch with operations can question reports that differ significantly from their knowledge of operations. Timely and complete reporting and resolution of these exceptions enhance effectiveness of the process.*
- *Changes in information reported in value-at-risk models used to evaluate the impacts of potential market movements on an entity's financial position are related to reported financial transactions, focusing on expected relationships.*
- *Communications from external parties corroborate internally generated information or indicate problems. Customers implicitly corroborate billing data by paying their invoices. Conversely, customer complaints about billings could indicate system deficiencies in the processing of sales transactions. Similarly, reports from investment managers on securities gains, losses, and income can corroborate or signal problems with the entity's (or the manager's) records. An insurance company's review of safety policies and practices provides information on operational safety and compliance performance.*

- *Regulators communicate with management on compliance or other matters that reflect on the functioning of enterprise risk management.*
- *Internal and external auditors and advisors regularly provide recommendations to strengthen enterprise risk management. Auditors may focus considerable attention on key risks and related responses and design of control activities. Potential weaknesses may be identified, and alternative actions recommended to management, accompanied by information useful in making cost-benefit determinations. Internal auditors or personnel performing similar review functions can be particularly effective in monitoring an entity's activities.*
- *Training seminars, planning sessions, and other meetings provide important feedback to management on whether enterprise risk management is effective. In addition to particular problems that may indicate risk issues, participants' risk and control consciousness often becomes apparent.*
- *Managers in the normal course of running the business discuss with personnel such matters as their understanding of the entity's code of conduct, how they identify risks, and issues arising in connection with the operation of control activities. These discussions confirm proper functioning of elements of enterprise risk management or surface matters needing attention.*

Separate Evaluations

While ongoing monitoring procedures usually provide important feedback on the effectiveness of other enterprise risk management components, it may be useful to take a fresh look from time to time, focusing directly on enterprise risk management effectiveness. This also provides an opportunity to consider the continued effectiveness of the ongoing monitoring procedures.

Scope and Frequency

Evaluations of enterprise risk management vary in scope and frequency, depending on the significance of risks and importance of the risk responses and related controls in managing the risks. Higher-priority risk areas and responses tend to be evaluated more often. Evaluation of the entirety of enterprise risk management – which generally will be needed less frequently than the assessment of specific parts – may be prompted by a number of reasons: major strategy or management change, acquisitions or dispositions, changes in economic or political conditions, or changes in operations or methods of processing information. When a decision is made to undertake a comprehensive evaluation of an entity's enterprise risk management, attention should be directed to addressing its application in strategy setting as well as with respect to significant activities. The evaluation scope also will depend on which objectives categories – strategic, operations, reporting, and compliance – are to be addressed.

Who Evaluates

Often, evaluations take the form of self-assessments, where persons responsible for a particular unit or function determine the effectiveness of enterprise risk management for their activities. For example, the chief executive of a division directs the evaluation of its enterprise risk management activities. He or she personally assesses the risk management activities associated with strategic choices and high-level objectives as well as the internal environment component, and individuals in charge of the division's various operating activities assess the effectiveness of enterprise risk management components relative to their spheres of responsibility. Line managers focus on operations and compliance objectives, and the divisional controller focuses on reporting objectives. The division's assessments are then considered by senior management, along with evaluations of the company's other divisions.

Internal auditors normally perform evaluations as part of their regular duties, or at the specific request of senior management, the board, or subsidiary or divisional executives. Similarly, management may utilize input from external auditors in considering the effectiveness of enterprise risk management. A combination of efforts may be used in conducting whatever evaluative procedures management deems necessary.

The Evaluation Process

Evaluating enterprise risk management is a process in itself. While approaches or techniques vary, a discipline should be brought to the process, with certain basics inherent in it.

The evaluator must understand each of the entity's activities and each of the components of enterprise risk management being addressed. It may be useful to focus first on how enterprise risk management purportedly functions – sometimes referred to as the system or process design.

The evaluator must determine how the system actually works. Procedures designed to operate in a particular way may be modified over time to operate differently or may no longer be performed. Sometimes new procedures are established but are not known to those who described the process and are not included in available documentation. A determination as to actual functioning can be accomplished by holding discussions with personnel who perform or are affected by enterprise risk management, by examining records on performance, or a combination of procedures.

The evaluator analyzes the enterprise risk management process design and the results of tests performed. The analysis is conducted against the backdrop of management's established standards for each component, with the ultimate goal of determining whether the process provides reasonable assurance with respect to the stated objectives.

Methodology

A variety of evaluation methodologies and tools are available, including checklists, questionnaires, and flowcharting techniques. As part of their evaluation methodology, some companies compare or benchmark their enterprise risk management process against those of other entities. An entity may, for example, measure its enterprise risk management against those companies with reputations for having particularly good enterprise risk management. Comparisons might be done directly with another company or under the auspices of trade or industry associations. Other organizations may provide comparative information, and peer review functions in some industries can help a company evaluate its enterprise risk management against its peers. A word of caution is needed. When conducting comparisons, consideration must be given to differences that always exist in objectives, facts, and circumstances. And all eight enterprise risk management components, as well as the inherent limitations of enterprise risk management, need to be kept in mind.

Documentation

The extent of documentation of an entity's enterprise risk management varies with the entity's size, complexity, and similar factors. Larger organizations usually have written policy manuals, formal organization charts, written job descriptions, operating instructions, information system flowcharts, and so forth. Smaller entities typically have considerably less documentation. Many aspects of enterprise risk management are informal and undocumented, yet are regularly performed and highly effective. These activities may be tested in the same ways as documented activities. The fact that elements of enterprise risk management are not documented does not mean that they are not effective or that they cannot be evaluated. However, an appropriate level of documentation usually makes evaluations more effective and efficient.

The evaluator may decide to document the evaluation process itself. He or she usually will draw on existing documentation of the entity's enterprise risk management. Typically, this will be supplemented with additional documentation, along with descriptions of the tests and analyses performed in the evaluation.

Where management intends to make a statement to external parties regarding enterprise risk management effectiveness, it should consider developing and retaining documentation to support the statement. Such documentation may be useful if the statement subsequently is challenged.

Reporting Deficiencies

Deficiencies in an entity's enterprise risk management may surface from many sources, including the entity's ongoing monitoring procedures, separate evaluations, and external parties. A deficiency is a condition within enterprise risk management worthy of attention that may represent a perceived, potential, or real shortcoming, or an opportunity to strengthen

enterprise risk management to increase the likelihood that the entity's objectives will be achieved.

Sources of Information

One of the best sources of information on enterprise risk management deficiencies is enterprise risk management itself. Ongoing monitoring activities of an enterprise, including managerial activities and everyday supervision of employees, generate insights from those who are directly involved in the entity's activities. These insights are gained in real time and can provide quick identification of deficiencies. Other sources of deficiencies are the separate evaluations of enterprise risk management. Evaluations performed by management, internal auditors, or other functions can highlight areas in need of improvement.

External parties frequently provide important information on the functioning of an entity's enterprise risk management. These include customers, vendors and others doing business with the entity, external auditors, and regulators. Reports from external sources should be carefully considered for their implications for enterprise risk management, and appropriate corrective actions should be taken.

What Is Reported

What should be reported? Although a universal answer is not possible, certain parameters can be drawn.

All identified enterprise risk management deficiencies that affect an entity's ability to develop and implement its strategy and to set and achieve its objectives should be reported to those positioned to take necessary action. The nature of matters to be communicated will vary depending on individuals' authority to deal with circumstances that arise and on the oversight activities of superiors. In considering what needs to be communicated, it is necessary to look at the implications of findings. It is essential not only that a particular transaction or event be reported, but also that related potentially faulty procedures be reevaluated.

It can be argued that no problem is so insignificant as to make investigation of its implications unwarranted. An employee taking a few dollars from a petty cash fund for personal use, for example, would not be significant in terms of that particular event, and probably not in terms of the amount of the entire petty cash fund. Thus, investigating it might not be worthwhile. However, such apparent condoning of personal use of the entity's money might send the wrong message to employees.

In addition to deficiencies, identified opportunities to increase the likelihood that the entity's objectives will be achieved also should be reported.

To Whom to Report

Information generated in the course of operating activities usually is reported through normal channels to immediate superiors. They in turn may communicate upstream or laterally in the organization, so that the information ends up with personnel who can and should act on it. Alternative communications channels also should exist for reporting sensitive information such as illegal or improper acts. Findings of enterprise risk management deficiencies usually should be reported not only to the individual responsible for the function or activity involved, but also to at least one level of management above that person. This higher level of management provides needed support or oversight for taking corrective action and is positioned to communicate with others in the organization whose activities may be affected. Where findings cut across organizational boundaries, the reporting should cross over as well and be directed to a sufficiently high level to ensure appropriate action.

Reporting Directives

Providing needed information on enterprise risk management deficiencies to the right party is critical. Protocols should be established to identify what information is needed at a particular level for effective decision making.

Such protocols reflect the general rule that a manager should receive information that affects actions or behavior of personnel within his or her responsibility, as well as information needed to achieve specific objectives. A chief executive normally would want to be apprised, for example, of serious infractions of policies and procedures. He or she also would want supporting information on matters that could have significant financial impacts or strategic implications or that could affect the entity's reputation.

Senior managers should be apprised of risk management and control deficiencies affecting their units. Examples include circumstances where assets with a specified monetary value are not adequately protected, where the competence of employees is lacking, or where important financial reconciliations are not performed correctly. Managers should be informed of deficiencies in their units in increasing levels of detail, as one moves down the organizational structure.

Supervisors define reporting protocols for subordinates. The degree of specificity will vary, usually increasing at lower levels in the organization. While reporting protocols can inhibit effective reporting if too narrowly defined, they can enhance reporting if sufficient flexibility is provided.

Parties to whom deficiencies are to be communicated sometimes provide specific directives regarding what should be reported. A board of directors or audit committee, for example, may ask management or internal or external auditors to communicate only those deficiencies meeting a specified threshold of seriousness or importance.

10. ROLES AND RESPONSIBILITIES

Chapter Summary: Everyone in an entity has some responsibility for enterprise risk management. The chief executive officer is ultimately responsible and should assume "ownership." Other managers support the risk management philosophy, promote compliance with the risk appetite, and manage risks within their spheres of responsibility consistent with risk tolerances. Other personnel are responsible for executing enterprise risk management in accordance with established directives and protocols. The board of directors provides important oversight to enterprise risk management. A number of external parties often provide information useful in effecting enterprise risk management, but they are not responsible for the effectiveness of the entity's enterprise risk management.

Enterprise risk management is effected by a number of parties, each with important responsibilities. The board of directors (directly or through its committees), management, internal auditors, and other personnel all make important contributions to risk management. Other parties, such as external auditors and regulatory bodies, are sometimes associated with risk assessments and internal control. However, a distinction exists between those who are part of an entity's enterprise risk management process and those who are not, but whose actions nonetheless can affect the process or otherwise help the entity achieve its objectives. Directly or indirectly helping an entity achieve its objectives, however, does not make an external party a part of or responsible for the entity's enterprise risk management.

Entity Personnel

The board of directors, management, risk officers, financial officers, internal auditors, and indeed every individual within an entity contribute to effective enterprise risk management.

Board of Directors

Management is accountable to the board of directors or trustees, which provides monitoring, guidance, and direction. By selecting management, the board has a major role in defining what it expects in integrity and ethical values, and through its oversight activities can determine whether its expectations are being met. Similarly, by reserving authority in certain key decisions, the board plays a role in setting strategy, formulating high-level objectives, and broad-based resource allocation.

The board provides oversight with regard to enterprise risk management by:

- Knowing the extent to which management has established effective enterprise risk management in the organization
- Being aware of and concurring with the entity's risk appetite
- Reviewing the entity's portfolio view of risk and considering it against the entity's risk appetite

- Being apprised of the most significant risks and whether management is responding appropriately

The board is part of the internal environment component and must have the requisite composition and focus for enterprise risk management to be effective.

Effective board members are objective, capable, and inquisitive. They have a working knowledge of the entity's activities and environment and commit the time necessary to fulfill their board responsibilities. They utilize resources as needed to conduct special investigations and have open and unrestricted communications with internal auditors, external auditors, and legal counsel.

Boards of directors may use board committees in carrying out certain of their duties. The use and focus of committees vary from one entity to another, although common committees are nominating/governance, compensation, and audit committees, with each focusing attention on elements of enterprise risk management. The nominating committee, for example, identifies and considers qualifications of prospective board members, and the compensation committee considers the appropriateness of reward systems, balancing healthy motivational programs with the need to avoid unnecessary temptation to manipulate compensation drivers. The audit committee has a direct role in the reliability of external reporting, and must recognize key risks relative to reliable financial reporting. As such, the board and its committees are an important part of enterprise risk management.

Management

Management is directly responsible for all activities of an entity, including enterprise risk management. Naturally, management at different levels has different enterprise risk management responsibilities. These vary, often considerably, depending on the entity's characteristics.

In any entity, the chief executive officer has ultimate ownership responsibility for enterprise risk management. One of the most important aspects of this responsibility is ensuring the presence of a positive internal environment. More than any other individual or function, the CEO sets the tone at the top that influences internal environmental factors and other components of enterprise risk management. A CEO also can influence the board of directors, through whatever influence he or she has on identifying new members, and in setting an example and serving to attract, or deter, candidates for the board. Increasingly, candidates for board seats look closely at top management's integrity and ethical values in determining whether to accept a nomination. Potential directors also focus on whether the entity's enterprise risk management has the necessary critical underpinnings of integrity and ethical values to enable its effectiveness.

The chief executive's responsibilities include seeing that all components of enterprise risk management are in place. The CEO generally fulfills this duty by:

- Providing leadership and direction to senior managers. Together with them, the CEO shapes the values, principles, and major operating policies that form the foundation of the entity's enterprise risk management. The CEO and key senior managers set strategic objectives, strategy, and related high-level objectives. They also set broad-based policies and develop the entity's risk management philosophy, risk appetite, and culture. They take actions concerning the entity's organizational structure, content and communication of key policies, and the type of planning and reporting systems the entity will use.
- Meeting periodically with senior managers responsible for major functional areas – sales, marketing, production, procurement, finance, human resources – to review their responsibilities, including how they manage risk. The CEO gains knowledge of risks inherent in operations, risk responses, and control improvements required, and the status of efforts under way. To discharge this responsibility, the CEO must clearly define the information he or she needs.

With this knowledge, the CEO is positioned to monitor activities and risks in relation to the entity's risk appetite. Where evolving circumstances, emerging risks, strategy implementation, or anticipated actions indicate potential misalignment with risk appetite, the CEO will take necessary action to reestablish alignment, or discuss with the board of directors further action to be taken or whether the entity's risk appetite should be adjusted.

Senior managers in charge of organizational units have responsibility for managing risks related to their units' objectives. They convert strategy into operations, identify events and assess risks, and effect risk responses. Managers guide application of enterprise risk management components within their spheres of responsibility, ensuring application is consistent with risk tolerances. In this sense, a cascading responsibility exists, where each executive is effectively a CEO for his or her sphere of responsibility.

Senior managers usually assign responsibility for specific enterprise risk management procedures to managers in specific processes, functions, or departments. Accordingly, these managers usually play a more hands-on role in devising and executing particular risk procedures that address unit objectives, such as techniques for event identification and risk assessment, and in determining responses, such as developing protocols for purchasing raw materials or accepting new customers. They also make recommendations on related control activities, monitor their application, and meet with upper-level managers to report on the control activities' functioning.

This may involve investigating external events or conditions, data entry errors, or transactions appearing on exception reports, looking into reasons for departmental expense budget variances and following up on customer back orders or product inventory positions. Significant matters, whether pertaining to a particular transaction or an indication of a larger concern, are communicated upward in the organization.

Staff functions, such as human resources, compliance, or legal, also have important supporting roles in designing or shaping effective enterprise risk management components. The human resources function may design and help implement training programs on the entity's code of conduct and other broad policy issues, often rolled out with business unit leadership. The legal function provides information to line managers on new laws and regulations that affect operating policies, and it or compliance officers provide critical information on whether planned transactions or protocols conform to legal and ethical requirements.

Managers' responsibilities should entail both authority and accountability. Each manager should be accountable to the next higher level for his or her portion of enterprise risk management, with the CEO ultimately accountable to the board. Although different management levels have distinct enterprise risk responsibilities and functions, their actions should coalesce in the entity's enterprise risk management.

Risk Officer

Some companies have established a centralized coordinating point to facilitate enterprise risk management. A risk officer – referred to in some organizations as the chief risk officer or risk manager – works with other managers in establishing effective risk management in their areas of responsibility. Established by and under direct auspices of the chief executive, the risk officer has the resources to help effect enterprise risk management across subsidiaries, businesses, departments, functions, and activities. The risk officer may have responsibility for monitoring progress and for assisting other managers in reporting relevant risk information up, down, and across the entity. The risk officer also may serve as a supplementary reporting channel.

Some companies assign this role to another senior officer, such as chief financial officer, general counsel, chief audit executive, or chief compliance officer; others have found that the importance and breadth of scope of this function require separate assignment and resources.

Companies have found this role most successful when set up with clarity around its responsibility as a staff function – providing support and facilitation to line management. For enterprise risk management to be effective, line managers must assume primary responsibility and have accountability for managing risk within their respective areas.

Responsibilities of a risk officer may include:

- Establishing enterprise risk management policies, including defining roles and responsibilities and participating in setting goals for implementation
- Framing authority and accountability for enterprise risk management in business units
- Promoting an enterprise risk management competence throughout the entity, including facilitating development of technical enterprise risk management expertise and helping managers align risk responses with the entity's risk tolerances and developing appropriate controls
- Guiding integration of enterprise risk management with other business planning and management activities
- Establishing a common risk management language that includes common measures around likelihood and impact, and common risk categories
- Facilitating managers' developing of reporting protocols, including quantitative and qualitative thresholds, and monitoring the reporting process
- Reporting to the chief executive on progress and outliers and recommending action as needed

Financial Executives

Of particular significance to enterprise risk management activities are finance and controllership executives and their staffs, whose activities cut across, up, and down all operating and business units. These financial executives often are involved in developing entity-wide budgets and plans, and they track and analyze performance, often from an operations, compliance, and reporting perspective. These activities are usually part of an entity's central or "corporate" organization, but commonly they also have "dotted line" responsibility for monitoring division, subsidiary, or other unit activities. As such, the chief financial officer, chief accounting officer, controller, and others in the financial function are central to the way management exercises enterprise risk management. They play an important role in preventing and detecting fraudulent reporting, and as a member of top management, the chief financial officer helps set the tone of the organization's ethical conduct; has a major responsibility for the financial statements, and influences the design, implementation, and monitoring of the company's reporting systems.

When looking at the components of enterprise risk management, it is clear that the chief financial officer and his or her staff play critical roles. This person is a key player when objectives are established, strategies decided, risks analyzed, and decisions made on how changes affecting the entity will be managed. He or she provides valuable input and direction and is positioned to focus on monitoring and following up on the actions decided.

As such, the chief financial officer should come to the table an equal partner with the other functional heads. Any attempt by management to have him or her more narrowly focused – limited to principally areas of financial reporting and treasury, for example – could severely limit the entity's ability to succeed.

Internal Auditors

Internal auditors play a key role in evaluating the effectiveness of – and recommending improvements to – enterprise risk management. Standards established by the Institute of Internal Auditors specify that the scope of internal auditing should encompass risk management and control systems. This includes evaluating the reliability of reporting, effectiveness and efficiency of operations, and compliance with laws and regulations. In carrying out their responsibilities, internal auditors assist management and the board of directors or audit committee by examining, evaluating, reporting on, and recommending improvements to the adequacy and effectiveness of the entity's enterprise risk management.

The Institute of Internal Auditors standards also address what roles are appropriate for internal audit, making clear that internal auditors should be objective with regard to the activities they audit. This objectivity should be reflected by their position and authority within the entity and appropriate internal auditor staff assignments. Organizational position and authority involve such matters as a reporting line to an individual who has sufficient authority to ensure appropriate audit coverage, consideration, and response; selection and dismissal of the chief audit executive only with concurrence of the board of directors or audit committee; access to the board or audit committee; and authority to follow up on findings and recommendations.

Other Entity Personnel

Enterprise risk management is, to some degree, the responsibility of everyone in an entity and therefore should be an explicit or implicit part of everyone's job description. This is true from two perspectives:

- Virtually all personnel play some role in effecting risk management. They may produce information used in identifying or assessing risks, or take other actions needed to effect enterprise risk management. The care with which those activities are performed directly affects the effectiveness of an entity's enterprise risk management.
- All personnel are responsible for supporting information and communication flows inherent in enterprise risk management. This includes communicating to a higher organizational level any problems in operations, non-compliance with the code of conduct, or other violations of policy or illegal actions. Enterprise risk management relies on checks and balances, including segregation of duties, and on personnel not "looking the other way." Personnel should understand the need to resist pressure from superiors to participate in improper activities, and channels outside of normal reporting lines should be available to permit reporting of such circumstances.

Enterprise risk management is everyone's business, and roles and responsibilities of all personnel should be well defined and effectively communicated.

External Parties

A number of external parties can contribute to achievement of an entity's objectives, sometimes by actions that parallel those taken within the entity. In other cases, external parties may provide information useful to the entity in its enterprise risk management activities.

External Auditors

External auditors provide management and the board of directors a unique, independent, and objective view that can contribute to an entity's achievement of its external financial reporting objectives, as well as other objectives.

In a financial statement audit, the auditor expresses an opinion on the fairness of the financial statements in conformity with generally accepted accounting principles, thereby contributing to the entity's external financial reporting objectives. The auditor conducting a financial statement audit may contribute further to those objectives, by providing information useful to management in carrying out its risk management-related responsibilities. Such information includes:

- Audit findings, analytical information, and recommendations for actions necessary to achieve established objectives
- Findings regarding deficiencies in risk management and control that come to the auditor's attention, and recommendations for improvement

This information frequently will relate not only to reporting but to strategic, operations, and compliance activities as well, and can make important contributions to an entity's achievement of its objectives in each of these areas. The information is reported to management and, depending on its significance, to the board of directors or audit committee.

It is important to recognize that a financial statement audit, by itself, normally does not include a significant focus on enterprise risk management, and in any event does not result in the auditor forming an opinion on the entity's enterprise risk management. Where, however, law or regulation requires the auditor to evaluate a company's assertions related to internal control over financial reporting and the supporting basis for those assertions, the scope of the work directed at those areas will be extensive, and additional information and assurance will be gained.

Legislators and Regulators

Legislators and regulators affect the enterprise risk management of many entities, either through requirements to establish risk management mechanisms or internal controls or through examinations of particular entities. Many of the relevant laws and regulations deal primarily with financial reporting risks and controls. Some, however – particularly those that apply to government organizations – also can deal with operations and compliance objectives. Many entities have long been subject to legal requirements for internal control. For example, U.S. public companies have been required to establish and maintain internal accounting control systems that satisfy specified objectives. More-recent legislation requires that senior executives of publicly listed companies certify to the effectiveness of the companies' internal control over financial reporting, together with auditor attestation.

Several regulatory agencies directly examine entities for which they have oversight responsibility. For example, federal and state bank examiners conduct examinations of banks and often focus on aspects of the banks' risk management and internal control systems. These agencies make recommendations and take enforcement action.

Therefore, legislators and regulators affect entities' enterprise risk management in two ways: They establish rules that provide the impetus for management to ensure that risk management and control systems meet minimum statutory and regulatory requirements. And, pursuant to examination of a particular entity, they provide information useful to the entity in applying enterprise risk management, and recommendations and sometimes directives to management regarding needed improvements.

Parties Interacting with the Entity

Customers, vendors, business partners, and others who conduct business with an entity are an important source of information used in enterprise risk management activities. Information can be as varied as emerging demand for new product or service, shipment or billing discrepancies, quality issues, or actions by personnel outside integrity and ethical boundaries. This input can be extremely important to the entity in achieving its strategic, operations, reporting, and compliance objectives. The entity must have mechanisms in place to receive such information and to take appropriate action. Needed action includes not only addressing the particular situation reported, but also investigating the underlying source of the problem and fixing it.

In addition to customers and vendors, other parties, such as creditors, can provide oversight regarding achievement of an entity's objectives. A bank, for example, may request reports on an entity's compliance with certain debt covenants. It also may recommend performance indicators or other desired targets or controls.

Outsource Service Providers

Many organizations outsource business functions, delegating their day-to-day management to outside providers. Administrative, finance, and internal operations sometimes are outsourced, with the objective of obtaining access to enhanced capabilities and lower cost of services. A financial institution may outsource its loan review process to a third party; a technology company may outsource the operation and maintenance of its information technology processing; and a retail company may outsource its internal audit function. While these external parties execute activities for or on behalf of the entity, management cannot abdicate its responsibility to manage the associated risks and should implement a program to monitor those activities.

Financial Analysts, Bond Rating Agencies, News Media

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 on 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 sometimes is 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.

11. LIMITATIONS OF ENTERPRISE RISK MANAGEMENT

Chapter Summary: Effective enterprise risk management, no matter how well designed and operated, provides only reasonable assurance to management and the board of directors regarding achievement of an entity's objectives. Achievement of objectives is affected by limitations inherent in all management processes. These include the realities that human judgment in decision making can be faulty and that breakdowns can occur because of such human failures as simple error or mistake. Additionally, controls can be circumvented by the collusion of two or more people, and management has the ability to override the enterprise risk management process, including risk response decisions and control activities. Another limiting factor is the need to consider the relative costs and benefits of risk responses.

To some observers, enterprise risk management, with embedded internal control, ensures that an entity will not fail – that is, the entity will always achieve its objectives. This view is misguided.

In considering limitations of enterprise risk management, three distinct concepts must be recognized:

- First, risk relates to the future, which is inherently uncertain.
- Second, enterprise risk management – even effective enterprise risk management – operates at different levels with respect to different objectives. For strategic and operations objectives, enterprise risk management can help ensure that management, and the board in its oversight role, is aware, in a timely manner, only of the extent to which the entity is moving toward achievement of these objectives. But it cannot provide even reasonable assurance that the objectives themselves will be achieved.
- Third, enterprise risk management cannot provide absolute assurance with respect to any of the objective categories.

The first limitation acknowledges that no one can predict the future with certainty. The second acknowledges that certain events are simply outside management's control. The third has to do with the reality that no process will always do what it is intended to do.

Reasonable assurance does not imply that enterprise risk management frequently will fail. Many factors, individually and collectively, reinforce the concept of reasonable assurance. 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. Furthermore, the normal everyday operating activities and responsibilities of people functioning at various levels of an organization are directed at achieving the entity's objectives. Indeed, among a cross-section of well-controlled entities, it is likely that most will be apprised regularly of movement toward their strategic and operations objectives, will

achieve compliance objectives regularly, and consistently will produce – period after period, year after year – reliable reports. 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.

Judgment

The effectiveness of enterprise risk management is limited by the realities of human frailty in making business decisions. Decisions must be made with human judgment in the time available, based on information at hand, and under the pressures of the conduct of business. With the clairvoyance of hindsight, some decisions later may be found to produce less than desirable results and may need to be changed.

Breakdowns

Well-designed enterprise risk management can break down. Personnel may misunderstand instructions. They may make judgment mistakes. Or, they may commit errors due to carelessness, distraction, or fatigue. An accounting department supervisor responsible for investigating exceptions simply might forget to follow up or fail to pursue the investigation far enough to be able to make appropriate corrections. Temporary personnel executing control duties for vacationing or sick employees might not perform correctly. System changes may be implemented before personnel have been trained to react appropriately to signs of incorrect functioning.

Collusion

The collusive activities of two or more individuals can result in enterprise risk management failures. Individuals acting collectively to perpetrate and conceal an action from detection often can alter financial data or other management information in a manner that cannot be identified by the enterprise risk management process. For example, there may be collusion between an employee performing an important control function and a customer, a supplier, or another employee. On a different level, several layers of sales or divisional management might collude in circumventing controls so that reported results meet budgets or incentive targets.

Costs versus Benefits

As discussed in the *Risk Assessment* chapter, there are always resource constraints, and entities must consider the relative costs and benefits of decisions, including those related to risk response and control activities.

In determining whether a particular action should be taken or control established, the risk of failure and the potential effect on the entity are considered along with the related costs. For example, it may not pay for a company to install sophisticated inventory controls to monitor

levels of raw material if the cost of the raw material used in a production process is low, the material is not perishable, ready supply sources exist, and storage space is readily available.

Costs and benefits of implementing event identification and risk assessment capabilities and related response and control activities are measured with different levels of precision, often varying depending on the nature of the entity. The challenge is to find the right balance. Just as limited resources should not be allocated to less than significant risks, excessive control is costly and counterproductive. Customers placing telephone orders will not tolerate order acceptance procedures that are too cumbersome or time-consuming. A bank that makes creditworthy potential borrowers "jump through hoops" will not book many new loans. Too little control, on the other hand, presents undue risk of bad debts. An appropriate balance is needed in a highly competitive environment. And, despite the difficulties, cost-benefit decisions will continue to be made.

Management Override

Enterprise risk management can be only as effective as the people who are responsible for its functioning. Even in effectively managed and controlled entities – those with generally high levels of integrity and risk and control consciousness, alternative communications channels, and an active and informed board with an appropriate governance process – a manager still might be able to override enterprise risk management. No management or control system is infallible, and those with criminal intent will seek to break systems. However, effective enterprise risk management will improve the entity's capacity to prevent and detect override activities.

The term "management override" is used here to mean overruling prescribed policies or procedures for illegitimate purposes – such as personal gain or an enhanced presentation of an entity's financial condition or compliance status. A manager of a division or unit, or a member of top management, might override enterprise risk management for many reasons: to increase reported revenue to cover an unanticipated decrease in market share; to enhance reported earnings to meet unrealistic budgets; to boost the market value of the entity prior to a public offering or sale; to meet sales or earnings projections to bolster bonus pay-outs tied to performance or value of stock options; to appear to cover violations of debt covenant agreements; or to hide lack of compliance with legal requirements. Override practices include deliberate misrepresentations to bankers, lawyers, auditors, and vendors, and intentionally issuing false documents such as purchase orders and sales invoices.

Management override should not be confused with management intervention, which represents management's actions to depart from prescribed policies or procedures for legitimate purposes. Management intervention is necessary to deal with non-recurring and non-standard transactions or events that otherwise might be handled inappropriately. Provision for management intervention is necessary because no process can be designed to

anticipate every risk and every condition. Management's actions to intervene are generally overt and commonly documented or otherwise disclosed to appropriate personnel. Actions to override usually are not documented or disclosed, with an intent to cover up the actions.

12. WHAT TO DO

Actions that might be taken as a result of this report depend on the position and role of the parties involved.

- *Board Members* – Members of the board of directors should discuss with senior management the state of the entity's enterprise risk management and provide oversight as needed. The board also should ensure that the entity's enterprise risk management mechanisms provide it with an assessment of the most significant risks relative to strategy and objectives, including what actions management is taking and how it is engaged in monitoring enterprise risk management. The board should seek input from the internal auditors, external auditors, and advisors.
- *Senior Management* – This study suggests that the chief executive should assess the entity's enterprise risk management capabilities. Using this framework, a CEO, together with key operating and financial executives, can focus attention where needed. Under one approach, the chief executive brings together business unit heads and key functional staff to discuss an initial assessment of enterprise risk management capabilities and effectiveness. Whatever its form, an initial assessment should determine whether there is a need for, and how to proceed with, a broader, more in-depth evaluation. It also should ensure that ongoing monitoring processes are in place. Time spent in evaluating enterprise risk management represents an investment, but one capable of providing a high return.
- *Other Entity Personnel* – Managers and other personnel should consider how their enterprise risk management responsibilities are being conducted in light of this framework and discuss with more senior personnel ideas for strengthening enterprise risk management. Internal auditors should consider the breadth of their focus on enterprise risk management.
- *Regulators* – Expectations for enterprise risk management vary widely with regard to what it can accomplish, and about what the "reasonable assurance" concept means and how it should be applied. This framework can promote a shared view of enterprise risk management, including what it can do and its limitations. Regulators may refer to this framework in establishing expectations, whether by rule or guidance, or in conducting examinations, for entities they oversee.
- *Professional Organizations* – Rule-making and other professional organizations providing guidance on financial management, auditing, and related topics should consider their standards and guidance in light of this framework. To the extent diversity in concept and terminology is eliminated, all parties will benefit.
- *Educators* – This framework should be the subject of academic research and analysis, to see where future enhancements can be made. With the presumption that this report becomes accepted as a common ground for understanding, its concepts and terms should find their way into university curricula.

We believe this report offers a number of benefits. With this foundation for mutual understanding, all parties will be able to speak a common language and communicate more effectively. Business executives will be positioned to assess enterprise risk management processes against a standard, and strengthen the process and move their enterprises toward established goals. Future research can be leveraged off an established base. Legislators and regulators will be able to gain an increased understanding of enterprise risk management, its benefits, and its limitations. With all parties utilizing a common enterprise risk management framework, these collective and reinforcing benefits will be realized.

A. OBJECTIVES AND METHODOLOGY

In Fall 2001, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) initiated a study designed to help organizations manage risk. Despite an abundance of literature on the subject, COSO concluded there was a need for this study to design and build a framework and related application techniques. PricewaterhouseCoopers was engaged to conduct this project, resulting in this report, *Enterprise Risk Management – Integrated Framework*.

The *Framework* volume defines risk and enterprise risk management, and provides foundational definitions, concepts, objectives categories, components, and principles of a comprehensive enterprise risk management framework. It provides direction for companies and other organizations in determining how to enhance their enterprise risk management, providing context for and facilitating application in the real world. This document also is designed to provide a basis for entities' use in determining whether their enterprise risk management is effective and, if not, what is needed to make it so.

The *Application Techniques* volume links directly to the *Framework*. It provides illustrations of risk management techniques that can be applied by companies and other organizations at various levels – enterprise, line of business, and individual process or function – and in support of incremental or transformational enhancement.

Because of readers' diverse needs, input was obtained from corporate executives of organizations of varying sizes, including public and private companies in different industries, and government organizations. The executives included corporate chief executives, chief financial officers, chief risk officers, controllers, internal auditors, legislators, regulators, lawyers, external auditors, consultants, academicians, and others.

Throughout the project, the project team received advice and counsel from an Advisory Council to the COSO Board. The Advisory Council, composed of individuals in senior financial management, internal and external audit, and academia, met periodically with the project team and members of the COSO Board to review the project plan, progress, and drafts of the framework, and to take up related matters. At important project milestones, the Advisory Council and the project team communicated with the COSO Board.

The methodology employed in this study was designed to produce a report meeting the stated objectives. The project consisted of five phases:

I. Assessment

The project team assessed the current state of risk management models through literature review, survey, and workshops, for the purpose of capturing relevant information across the full spectrum of risk management. This phase encompassed analyzing the information, comparing and contrasting conceptual and practical risk

management philosophies and protocols, understanding user needs, and identifying critical issues and concerns.

II. Envisioning

The team created a working enterprise risk management framework conceptual model and developed a preliminary inventory of tools as a basis for the application techniques. Using customized input solicitation techniques, the team tested the concepts with key user and stakeholder groups and, based on feedback, refined the conceptual model.

III. Building and Designing

Using the refined conceptual model as a blueprint, the team developed the framework, including definitions, objectives categories, components, principles, infrastructure, and management context, along with related discussion. This phase also encompassed designing the organization and approach to developing the application techniques. Both the draft framework and application techniques design were reviewed with key user and stakeholder groups, and reactions and suggestions for enhancement obtained.

IV. Preparation for Public Exposure

In this phase the team refined the framework and further developed the application techniques, and reviewed them with executives from several companies who provided feedback on their value and utility.

V. Finalization

This phase encompassed issuing the *Framework* volume for public exposure for a 90-day comment period and field testing the framework with select companies. Upon receipt of comments, the project team reviewed and analyzed them, and identified needed modifications. The team finalized the *Framework* and *Application Techniques* volumes and provided the final manuscripts to the COSO Advisory Council and COSO Board for review and acceptance.

As part of this process, the project team gave careful consideration to all information received, including other frameworks already in existence. A listing of some of the published sources referenced is included in *Appendix D – Selected Bibliography*. As one might expect, many different and sometimes contradictory opinions were expressed on fundamental issues – within a project phase and between phases. The project team, with COSO Advisory Council and Board oversight, carefully considered the merits of the positions put forth, both individually and in the context of related issues, embracing those that facilitated development of a relevant, logical, and internally consistent framework. The Advisory Council and COSO Board are entirely supportive of, and have approved, the framework resulting from this process.

B. SUMMARY OF KEY PRINCIPLES

The following highlights key principles inherent in the eight enterprise risk management components. This appendix purports neither to precisely or fully describe the principles set forth in the *Framework*, nor to represent a complete list of principles.

Internal Environment

Risk Management Philosophy

- The entity's risk management philosophy represents the shared beliefs and attitudes characterizing how the entity considers risk in all activities
- It reflects the entity's values, influencing its culture and operating style
- It affects how enterprise risk management components are applied, including how events are identified, the kinds of risks accepted, and how they are managed
- It is well developed, understood, and embraced by the entity's personnel
- It is captured in policy statements, oral and written communications, and decision making
- Management reinforces the philosophy not only with words but also with everyday actions

Risk Appetite

- The entity's risk appetite reflects the entity's risk management philosophy and influences the culture and operating style
- It is considered in strategy setting, with strategy aligned with risk appetite

Board of Directors

- The board is active and possesses an appropriate degree of management, technical, and other expertise, coupled with the mind-set necessary to perform its oversight responsibilities
- It is prepared to question and scrutinize management's activities, present alternative views, and act in the face of wrongdoing
- It has at least a majority of independent outside directors
- It provides oversight to enterprise risk management and is aware of and concurs with the entity's risk appetite

Integrity and Ethical Values

- The entity's standards of behavior reflect integrity and ethical values
- Ethical values not only are communicated but also accompanied by explicit guidance regarding what is right and wrong
- Integrity and ethical values are communicated through a formal code of conduct
- Upward communications channels exist where employees feel comfortable bringing relevant information

- Penalties are applied to employees who violate the code, mechanisms encourage employee reporting of suspected violations, and disciplinary actions are taken against employees who knowingly fail to report violations
- Integrity and ethical values are communicated through management actions and the examples they set

Commitment to Competence

- Competence of the entity's people reflects the knowledge and skills needed to perform assigned tasks
- Management aligns competence and cost

Organizational Structure

- The organizational structure defines key areas of responsibility and accountability
- It establishes lines of reporting
- It is developed in consideration of the entity's size and nature of activities
- It enables effective enterprise risk management

Assignment of Authority and Responsibility

- Assignment of authority and responsibility establishes the degree to which individuals and teams are authorized and encouraged to use initiative to address issues and solve problems, and provides limits to authority
- The assignments establish reporting relationships and authorization protocols
- Policies describe appropriate business practices, knowledge and experience of key personnel, and associated resources
- Individuals know how their actions interrelate and contribute to achievement of objectives

Human Resource Standards

- Standards address hiring, orientation, training, evaluating, counseling, promoting, compensation, and remedial actions, driving expected levels of integrity, ethical behavior, and competence
- Disciplinary actions send the message that violations of expected behavior will not be tolerated

Objective Setting

Strategic Objectives

- The entity's strategic objectives establish high-level goals that align with and support its mission/vision
- They reflect management's strategic choices as to how the entity will seek to create value for its stakeholders

- Management identifies risks associated with strategy choices and considers their implications

Related Objectives

- Related objectives support and are aligned with selected strategy, relative to all entity activities
- Each level of objectives is linked to more specific objectives that cascade through the organization
- The objectives are readily understood and measurable
- They align with risk appetite

Selected Objectives

- Management has a process that aligns strategic objectives with the entity's mission and ensures the strategic and related objectives are consistent with the entity's risk appetite

Risk Appetite

- The entity's risk appetite is a guidepost in strategy setting
- It guides resource allocation
- It aligns organization, people, processes, and infrastructure

Risk Tolerances

- Risk tolerances are measurable, preferably in the same units as the related objectives
- They align with risk appetite

Event Identification

Events

- Management identifies potential events affecting strategy implementation or achievement of objectives – those that may have positive or negative impacts, or both
- Even events with a relatively low possibility of occurrence are considered if the impact on achieving an important objective is great

Influencing Factors

- Management recognizes the importance of understanding external and internal factors and the type of events that can emanate therefrom
- Events are identified both at the entity and activity levels

Event Identification Techniques

- Techniques used look to both the past and future
- Management selects techniques that fit its risk management philosophy and ensures the entity develops needed event identification capabilities

- Event identification is robust, forming a basis for risk assessment and risk response components

Interdependencies

- Management understands how events relate to one another

Distinguishing Risks and Opportunities

- Events with negative impact represent risks, which management assesses and responds to
- Events representing opportunities are channeled back to management's strategy or objective-setting processes

Risk Assessment

- In assessing risk, management considers expected and unexpected events

Inherent and Residual Risk

- Management assesses inherent risks
- Once risk responses have been developed, management considers residual risk

Estimating Likelihood and Impact

- Potential events are evaluated from two perspectives – likelihood and impact
- In assessing impact, management normally uses the same, or congruent, unit of measure as used for the objective
- The time horizon used to assess risks should be consistent with the time horizon of the related strategy and objectives

Assessment Techniques

- Management uses a combination of qualitative and quantitative techniques
- The techniques support development of a composite assessment of risk

Relationships between Events

- Where correlation exists between events, or events combine and interact, management assesses them together

Risk Response

- In responding to risk, management considers among risk avoidance, reduction, sharing, and acceptance

Evaluating Possible Responses

- Responses are evaluated with the intent of achieving residual risk aligned with the entity's risk tolerances

- In evaluating risk responses, management considers their effects on likelihood and impact
- Management considers their costs versus benefits, as well as new opportunities

Selected Responses

- Responses chosen by management are designed to bring anticipated risk likelihood and impact within risk tolerances
- Management considers additional risks that might result from a response

Portfolio View

- Management considers risk from an entity-wide, or portfolio, perspective
- Management determines whether the entity's residual risk profile is commensurate with its overall risk appetite

Control Activities

Integration with Risk Response

- Management identifies control activities needed to help ensure that risk responses are carried out properly and in a timely manner
- Selection or review of control activities includes consideration of their relevance and appropriateness to the risk response and related objective
- In selecting control activities, management considers how control activities interrelate

Types of Control Activities

- Management selects from a variety of types of control activities, including preventive, detective, manual, computer, and management controls

Policies and Procedures

- Policies are implemented thoughtfully, conscientiously, and consistently
- Procedures are carried out with sharp, continuing focus on conditions to which the policy is directed
- Conditions identified as a result of the procedure are investigated and appropriate corrective actions taken

Controls over Information Systems

- Appropriate general and application controls are implemented

Information and Communication

Information

- Relevant information is obtained from internal and external sources
- The entity captures and uses historical and present data as needed to support effective enterprise risk management
- The information infrastructure converts raw data into relevant information that assists personnel in carrying out their enterprise risk management and other responsibilities; information is provided at a depth and in a form and timeframe that are actionable, readily usable, and linked to defined accountabilities – including the need to identify, assess, and respond to risk
- Source data and information are reliable, and provided on time at the right place to enable effective decision making
- Timeliness of information flow is consistent with the rate of change in the entity's internal and external environments
- Information systems change as needed to support new objectives

Communication

- Management provides specific and directed communication addressing behavioral expectations and responsibilities of personnel, including a clear statement of the entity's risk management philosophy and approach and clear delegation of authority
- Communication about processes and procedures aligns with, and underpins, the desired culture
- All personnel receive a clear message from top management that enterprise risk management must be taken seriously
- Personnel know how their activities relate to the work of others, enabling them to recognize problems, determine cause, and take corrective action
- Personnel know what is deemed acceptable and unacceptable behavior
- There are open channels of communication and a willingness to listen, and personnel believe their superiors truly want to know about problems and will deal with them effectively
- Communications channels outside normal reporting lines exist, and personnel understand there will be no reprisals for reporting relevant information
- An open communications channel exists between top management and the board of directors, with appropriate information communicated on a timely basis
- Open external communications channels exist, where customers and suppliers can provide significant input
- The entity communicates relevant information to regulators, financial analysts, and other external parties

Monitoring

- Management determines, through ongoing monitoring activities or separate evaluations, or a combination, whether the functioning of enterprise risk management continues to be effective

Ongoing Monitoring Activities

- Monitoring activities are built into the entity's normal, recurring operations, performed in the ordinary course of running the business
- They are performed on a real-time basis and react dynamically to changing conditions

Separate Evaluations

- Separate evaluations focus directly on enterprise risk management effectiveness and provide an opportunity to consider the continued effectiveness of the ongoing monitoring activities
- The evaluator understands each of the entity activities and each enterprise risk management component being addressed
- The evaluator analyzes enterprise risk management design and the results of tests performed, against the backdrop of management's established standards, determining whether enterprise risk management provides reasonable assurance with respect to the stated objectives

Reporting Deficiencies

- Deficiencies reported from both internal and external sources are carefully considered for their implications for enterprise risk management, and appropriate corrective actions are taken
- All identified deficiencies that affect the entity's ability to develop and implement its strategy and to achieve its established objectives are reported to those positioned to take necessary action
- Not only are reported transactions or events investigated and corrected, but potentially faulty underlying procedures also are reevaluated
- Protocols are established to identify what information is needed at a particular level for effective decision making

Roles and Responsibilities

Board of Directors

- The board knows the extent to which management has established effective risk management in the organization
- It is aware of and concurs with the entity's risk appetite
- It reviews the portfolio view of risk and considers it against the risk appetite
- Is apprised of the most significant risks and whether management is responding appropriately

Management

- The chief executive has ultimate responsibility for enterprise risk management
- He/she ensures the presence of a positive internal environment, and that all enterprise risk management components are in place
- Senior managers in charge of organizational units have responsibility for managing risks related to their unit's objectives
- They guide application of enterprise risk management, ensuring application is consistent with risk tolerances
- Each manager is accountable to the next higher level, for his/her portion of enterprise risk management, with the CEO ultimately accountable to the board

Other Entity Personnel

- Enterprise risk management is an explicit or implicit part of everyone's job description
- Personnel understand the need to resist pressure from superiors to participate in improper activities, and channels outside normal reporting lines are available to permit reporting such circumstances
- The enterprise risk management roles and responsibilities of all personnel are well defined and effectively communicated

Parties Interacting with the Entity

- Mechanisms are in place to receive relevant information from parties interacting with the entity and take appropriate action
- Action includes not only addressing the particular situation reported, but also investigating the underlying source of the problem and fixing it
- For outsourced activities, management has implemented a program to monitor those activities
- Management considers the observations and insights of financial analysts, bond rating agencies and the news media that may enhance enterprise risk management

C. RELATIONSHIP BETWEEN *ENTERPRISE RISK MANAGEMENT – INTEGRATED FRAMEWORK* AND *INTERNAL CONTROL – INTEGRATED FRAMEWORK*

In 1992, the Committee of Sponsoring Organizations of the Treadway Commission issued *Internal Control – Integrated Framework*, which establishes a framework for internal control and provides evaluation tools that business and other entities can use to evaluate their control systems. The framework identifies and describes five interrelated components necessary for effective internal control.

Internal Control – Integrated Framework defines internal control as a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

This appendix outlines the relationship between the internal control framework and the enterprise risk management framework.

Broader than Internal Control

Internal control is encompassed within and an integral part of enterprise risk management. Enterprise risk management is broader than internal control, expanding and elaborating on internal control to form a more robust conceptualization focusing more fully on risk. *Internal Control – Integrated Framework* remains in place for entities and others looking at internal control by itself.

Categories of Objectives

Internal Control – Integrated Framework specifies three categories of objectives – operations, financial reporting, and compliance. Enterprise risk management specifies three similar objectives categories – operations, reporting, and compliance. The reporting category in the internal control framework is defined as relating to the reliability of published financial statements. In the enterprise risk management framework, the reporting category is significantly expanded, to cover all reports developed by an entity, disseminated both internally and externally. These include reports used internally by management and those issued to external parties, including regulatory filings and reports to other stakeholders. And, the scope expands from financial statements to cover not just financial information more broadly, but non-financial information as well.

Enterprise Risk Management – Integrated Framework adds another category of objectives, namely, strategic objectives, which operate at a higher level than the others. Strategic objectives flow from an entity's mission or vision, and the operations, reporting, and compliance objectives should be aligned with them. Enterprise risk management is applied in strategy setting, as well as in working toward achievement of objectives in the other three categories.

The enterprise risk management framework introduces the concepts of risk appetite and risk tolerance. Risk appetite is the broad-based amount of risk an entity is willing to accept in pursuit of its mission/vision. It serves as a guidepost in strategy setting and selection of related objectives. Risk tolerances are the acceptable levels of variation relative to achievement of objectives. In setting risk tolerances, management considers the relative importance of the related objectives and aligns risk tolerances with risk appetite. Operating within risk tolerances provides management greater assurance that the entity remains within its risk appetite, which, in turn, provides a higher degree of comfort that the entity will achieve its objectives.

Portfolio View

A concept not contemplated in the internal control framework is a portfolio view of risk. In addition to focusing on risk in considering achievement of entity objectives on an individual basis, it is necessary to consider composite risks from a "portfolio" perspective.

Components

With the enhanced focus on risk, the enterprise risk management framework expands the internal control framework's risk assessment component, creating four components – objective setting (which is a prerequisite to internal control), event identification, risk assessment, and risk response.

Internal Environment

In discussing the environment component, the enterprise risk management framework discusses an entity's risk management philosophy, which is the set of shared beliefs and attitudes characterizing how an entity considers risks, reflecting its values and influencing its culture and operating style. As described above, the framework encompasses the concept of an entity's risk appetite, which is supported by more specific risk tolerances.

Because of the critical importance of the board of directors and its composition, the enterprise risk management framework expands on the internal control framework's call for at least a critical mass of independent directors – that is, normally at least two independent directors – stating that for enterprise risk management to be effective, the board must have at least a majority of independent outside directors.

Event Identification

The enterprise risk management and internal control frameworks both acknowledge that risks occur at every level of the entity and result from a variety of internal and external factors. And, both frameworks consider risk identification in the context of the potential impact on the achievement of objectives.

The enterprise risk management framework discusses the concept of potential events, defining an event as an incident or occurrence emanating from internal or external sources that affect strategy implementation or achievement of objectives. Potential events with positive impact represent opportunities, while those with negative impact represent risks. Enterprise risk management involves identifying potential events using a combination of techniques that consider both past as well as emerging trends, and what triggers the events.

Risk Assessment

While both the internal control and enterprise risk management frameworks call for assessment of risk in terms of the likelihood that a given risk will occur and its potential impact, the enterprise risk management framework suggests viewing risk assessment through a sharper lens. Risks are considered on an inherent and a residual basis, preferably expressed in the same unit of measure established for the objectives to which the risks relate. Time horizons should be consistent with an entity's strategies and objectives, and, where possible, observable data. The enterprise risk management framework also calls attention to interrelated risks, describing how a single event may create multiple risks.

As noted, enterprise risk management encompasses the need for management to develop an entity-level portfolio view. With managers responsible for business unit, function, process, or other activities having developed a composite assessment of risk for individual units, entity-level management considers risk from a "portfolio" perspective.

Risk Response

The enterprise risk management framework identifies four categories of risk response – avoid, reduce, share, and accept. As part of enterprise risk management, management considers potential responses from these categories and considers these responses with the intent of achieving a residual risk level aligned with the entity's risk tolerances. Having considered responses to risk on an individual or a group basis, management considers the aggregate effect of its risk responses across the entity.

Control Activities

Both frameworks present control activities as helping ensure that management's risk responses are carried out. The enterprise risk management framework explicitly makes the point that in some instances control activities themselves serve as a risk response.

Information and Communication

The enterprise risk management framework expands on the information and communication component of internal control, highlighting consideration of data derived from past, present, and potential future events. Historical data allows the entity to track actual performance against targets, plans, and expectations, and provides insights into how the entity performed in past periods under varying conditions. Present or current-state data provides important additional information, and data on potential future events and underlying factors completes the information analysis. The information infrastructure sources and captures data in a timeframe and at a depth of detail consistent with the entity's need to identify events and assess and respond to risks and remain within its risk appetite.

The discussion around existence of an alternative communications channel, outside normal reporting lines, in the internal control framework has greater emphasis in the enterprise risk management framework, which states that effective risk management requires such a channel.

Roles and Responsibilities

Both frameworks focus attention on the roles and responsibilities of various parties that are a part of, or provide important information to, internal control and enterprise risk management. The enterprise risk management framework describes the role and responsibilities of risk officers and expands on the role of an entity's board of directors.

D. SELECTED BIBLIOGRAPHY

American Institute of Certified Public Accountants and The Canadian Institute of Chartered Accountants. *Managing Risk in the New Economy*. New York. AICPA. 2000.

Banham, Russ. *A High Level of Intolerance*. CFO, The Magazine for Senior Financial Executives. April 2000.

Barton ,Thomas L., William G. Shenkir, and Paul L.Walker. *Making Enterprise Risk Management Pay Off*: *How Leading Companies Implement Risk Management.* Financial Executive. 2001.

Bazerman, Max H. *Judgment in Managerial Decision Making*. New York. John Wiley & Sons. 2001.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). *Internal Control – Integrated Framework*. New York. AICPA. 1992.

Crouhy, Michael, Dan Galai, and Robert Mark. *Risk Management*. New York. McGraw-Hill. 2001.

Davidson, Clive. *Lofty Ambitions for Measuring Global Risk*. Securities Industry News. June 5, 2000.

DeLoach, James W. *Enterprise-Wide Risk Management: Strategies for Linking Risk and Opportunity*. London. Financial Times Prentice Hall. 2000.

DiPiazza, Samuel A., Jr. and Robert G. Eccles. *Building Public Trust: The Future of Corporate Reporting*. New York. John Wiley & Sons. 2002.

Everson, Miles. *Creating an Operational Risk-Sensitive Culture*. The RMA Journal. March 1, 2002.

Economist Intelligence Unit in cooperation with Arthur Andersen & Co. *Managing Business Risk – An Integrated Approach*. The Economist Intelligence Unit. 1995.

Economist Intelligence Unit in cooperation with MCC Enterprise Risk. *Enterprise Risk Management – Implementing New Solutions*. The Economist Intelligence Unit. 2001.

FEI Research Foundation in cooperation with Andersen. *Risk Management: An Enterprise Perspective*. Financial Executive. 2002.

Haubenstock, Michael and John Gontero. *Operational Risk Management: The Next Frontier*. New York. RMA. 2001.

Institute of Chartered Accountants in England and Wales. *Internal Control Guidance for Directors on the Combined Code*. London. ICAEW. 1999.

Institute of Directors in Southern Africa. *King Report on Corporate Governance for South Africa 2001*. The Institute of Directors in Southern Africa. 2001.

International Organization for Standardization. *ISO/IEC Guide 73*. 2002.

Lam, James. *The CRO Is Here to Stay*. Risk Management. April 2001.

National Commission on Fraudulent Financial Reporting. *Report of the National Commission on Fraudulent Financial Reporting*. 1987.

Nottingham, Lucy. *A Conceptual Framework for Integrated Risk Management*. Ottawa. Conference Board of Canada. 1997.

Risk Management Group of the Basel Committee on Banking Supervision. *Sound Practices for the Management and Supervision of Operational Risk*. 2001.

Root, Stephen J. *Beyond COSO Internal Control to Enhance Corporate Governance*. New York. John Wiley & Sons. 1998.

Standards Australia and Standards New Zealand. *Australian/New Zealand Standard 4360:1999: Risk Management*. Standards Australia and Standards New Zealand, 1999.

Steinberg, Richard M. *The CEO and the Board: Enhancing the Relationship*. G100 Insights. April 2003.

Steinberg, Richard M. and Catherine L. Bromilow. *Corporate Governance and the Board – What Works Best*. The Institute of Internal Auditors Research Foundation. 2001.

The Institute of Risk Management (IRM), The Association of Insurance and Risk Managers (AIRMIC), and ALARM The National Forum for Risk Management in the Public Sector. *A Risk Management Standard*. AIRMIC, ALARM, and IRM. 2002.

Thiessen, Karen. *A Composite Sketch of Chief Risk Officer*. Ottawa. Conference Board of Canada. 2001.

Thiessen, Karen. *Don't Gamble with Goodwill – The Value of Effectively Communicating Risks*. Ottawa. Conference Board of Canada. 2000.

Tillinghast–Towers Perrin. *Enterprise Risk Management: Trends and Emerging Practices*. New York. Tillinghast–Towers Perrin, 2001.

Walker, Paul L., William G. Shenkir, and Thomas L. Barton. *Enterprise Risk Management: Pulling It All Together*. The Institute of Internal Auditors Research Foundation. 2002.

E. CONSIDERATION OF COMMENT LETTERS

As noted in *Appendix A*, a draft of this Framework document was exposed for public comment. The 78 response letters received contain hundreds of individual comments on a wide variety of matters. Each comment was considered in formulating revisions to the final document. This appendix summarizes the more significant issues and resulting modifications reflected in this final report. It also provides perspective on why certain views were accepted over others.

Definition of Enterprise Risk Management

Realizing Value for Stakeholders

The exposure draft described how enterprise risk management enables an organization to realize value for its stakeholders, although the concept of value was not explicitly reflected in the definition of enterprise risk management. Some respondents suggested the definition should make such explicit reference.

It was concluded that the definition as presented should be retained. The definition explicitly states that enterprise risk management involves providing assurance regarding achievement of entity objectives, which inherently provides value. Further, the text surrounding the definition describes how enterprise risk management provides value for stakeholders. Because of this existing linkage to and description around value, and to avoid an unreasonably long definition (as suggested by other respondents), the definition has been retained.

Opportunities

The exposure draft described how enterprise risk management involves identifying and addressing potential events that have negative impact on an entity, called risks, and events with positive impact, referred to as opportunities. Some respondents said because of the importance of identifying opportunities, the definition of risk should be broadened to include that concept. Some argued that not including opportunities in the definition of risk can lead a reader not to see opportunities as part of enterprise risk management, thereby undermining the framework's relevance. On the other hand, some respondents suggested that all reference to opportunities be eliminated from the final report.

It was concluded that because of the importance of identifying and seizing opportunities, the framework's discussion of opportunities should be retained and enhanced, and the final report expands the discussion on identifying and reacting to opportunities as an integral part of enterprise risk management. Discussions in the component chapters of the final report further describe the process by which management considers both the negative and positive – or opportunity side – effects of potential events in managing risk. As to the definition of risk, it was concluded that adding the concept of opportunity would cloud the concepts and make communication more difficult. Maintaining the distinction between a negative event and a positive one brings clarity to the enterprise risk management language.

A Process

The exposure draft defined enterprise risk management as a process and set forth components that can be viewed as elements of a process. Some respondents said the term "process" inappropriately implies carrying out predefined, sequential steps or tasks.

The report has been revised to reinforce the concept that enterprise risk management is not necessarily conducted sequentially, but rather is a continuous and iterative interplay of actions conducted throughout an entity.

Applied in Strategy Setting

The exposure draft described how objectives must be set and clearly communicated before risks to their achievement can be identified and addressed. It also stated that enterprise risk management techniques are applied in strategy setting to assist management in evaluating and selecting the entity's strategy, and linking to related objectives. Some respondents commented that risk management is secondary to management's development of entity strategy, and that the framework places undue focus on risk rather than objective setting.

It was concluded that it is not necessary, or useful, to portray one concept, strategy setting, as necessarily more important than another, managing risk. Both are important and inherent in enterprise risk management. The final document does, however, contain enhanced discussion of the strategy and objective-setting process in effecting enterprise risk management.

Risk Appetite and Tolerance

The exposure draft discussed the concepts of risk appetite and risk tolerance. Some respondents suggested that additional information should be provided, including guidance on how to express and measure risk appetite. Others stated there is little difference in these two concepts and that they should be combined.

The final report retains the distinction between risk appetite and risk tolerance, where risk appetite pertains at a high level to the entity as a whole, while risk tolerance relates to specific objectives. The *Application Techniques* volume illustrates application of these concepts.

Provides Reasonable Assurance

Some respondents suggested the concept of reasonable assurance should be more precisely defined.

It was concluded that the discussion surrounding the term "reasonable assurance" is appropriate, and further precision in its definition is beyond the scope of this project.

Categories of Objectives

Some respondents said that setting forth categories of entity objectives is not helpful and unnecessarily complicates the framework.

The final document retains the categories of entity objectives, on the basis that the categorization allows a focus on separate aspects of enterprise risk management, facilitates distinguishing between what can be expected from each category of objectives, and supports use of a common language for enterprise risk management.

Achievement of Objectives

Some respondents questioned why reasonable assurance applies only to the extent to which strategic and operations objectives are being achieved, rather than to their actual achievement.

It was concluded that the distinction between what can be expected of enterprise risk management regarding achievement of strategic and operations objectives, relative to reporting and compliance objectives, continues to be appropriate for the reasons set forth in the document, centered on whether achievement is within or outside an entity's control.

Effectiveness

Several respondents stated that enterprise risk management effectiveness should be defined relative to results attained, measured in terms of outcomes the process is intended to achieve, rather than as a subjective judgment of whether the eight components are present and functioning properly.

The criteria for effectiveness – the presence and effective functioning of each component – remain in the final document. It was concluded that the principle developed in the internal control framework, and carried forward to the enterprise risk management framework, is logical and best serves users' needs – that when the eight components are deemed present and functioning effectively (and no material weaknesses exist), the result or outcome is that management and the board gain reasonable assurance regarding achievement of the stated objectives. The final document retains that principle, and also highlights that bringing risk within the entity's risk appetite is a necessary element of effective enterprise risk management. The concept of a subjective judgment as to the presence and functioning of the eight components has been removed, on the grounds that the judgment can be objective, based on the principles in this framework.

Encompasses Internal Control

The exposure draft contained some but not all of the text of *Internal Control – Integrated Framework*, stating that the entirety of the internal control document was incorporated by reference in the enterprise risk management framework. The exposure draft included an appendix comparing and contrasting the two frameworks.

Some respondents suggested that the final report should identify more prominently those portions carried forward from *Internal Control – Integrated Framework*. Some recommended that the entirety of *Internal Control – Integrated Framework* be included as an attachment, with a detailed reconciliation of differences between the two documents, while others suggested that the document describe in detail in what way *Internal Control – Integrated Framework* is expanded on in the enterprise risk management framework. And some respondents suggested that the document highlight and clarify the intended audience and purpose of each framework.

It was concluded that the description of differences between the frameworks is at the appropriate level. *Appendix C* highlights the key differences and identifies which concepts in the enterprise risk management framework are incorporated directly from *Internal Control – Integrated Framework*, which concepts taken from the internal control framework are expanded on, and which are new. It was deemed unnecessary to include the internal control framework as an attachment, as it is readily available to users. And, the purpose and intended audiences of each of the frameworks already are described in sufficient depth.

Enterprise Risk Management and the Management Process

Some respondents suggested that the exhibit comparing management activities with enterprise risk management activities provided little useful information and could cause confusion to readers. Some said setting forth management activities as distinct from enterprise risk management activities could reduce – rather than reinforce – the notion of embedding risk management within business and management activities.

The exhibit in the exposure draft has not been carried forward to the final report; instead, relevant messages are presented in the text.

Information and Communication

Some respondents commented on the importance of a communications channel outside normal reporting lines, suggesting that such a channel is a necessary element of enterprise risk management.

The final report reflects this view, stating that for enterprise risk management to be effective, an entity is required to maintain such a communications channel.

Roles and Responsibilities

Some respondents suggested that there is need for greater clarity regarding the different accountabilities for enterprise risk management of the board of directors, management, other entity personnel, and external parties.

The final report expands the discussion and clarifies the respective roles and responsibilities of these parties.

Other Considerations

Form and Presentation

Some respondents commented on the length, format, and style of the exposure draft, and expressed a variety of views on how the report could be reorganized and streamlined.

It was concluded that the report should be reorganized and streamlined to enhance readability and clarity and reduce redundancy. The exposure draft's "Executive Summary" has been replaced by a shorter summary. Chapter 1 of the exposure draft, "Relevance of Enterprise Risk Management," has been eliminated, with the more important concepts incorporated into the final report's "Definition" chapter. Redundancies have been reduced, less important discussions deleted or shortened, and the report wording streamlined.

Relationship between* Enterprise Risk Management – Integrated Framework *and Other Reports and Legislation

Some respondents said it would be useful to have a discussion of relationships between the enterprise risk management framework and the Sarbanes-Oxley Act of 2002, the Basel Committee on Banking Supervision's New Basel Capital Accord, and risk management legislation in Australia, Canada, Germany, Japan, the United Kingdom, and other countries. Some respondents recommended that the document state clearly that *Internal Control – Integrated Framework* continues to be an acceptable framework for compliance with Section 404 the Sarbanes-Oxley Act of 2002 and that issuance of *Enterprise Risk Management – Integrated Framework* does not require companies to use it for purposes of Section 404 compliance.

It was concluded that reconciling *Enterprise Risk Management – Integrated Framework* with other documents is beyond the scope of this project. With regard to complying with Sarbanes-Oxley Section 404 requirements, COSO is communicating, via the *Foreword* to this report, that *Internal Control – Integrated Framework* remains in place and is appropriately looked to as a basis for reporting under certain legislative requirements such as the Sarbanes-Oxley Act of 2002.

Application Guidance

Some respondents recommended inclusion of specified content for the application guidance volume. Some suggested that one or more comprehensive case studies be included in order to help organizations of various sizes implement the framework. Others suggested that the *Framework* document and application guidance contain cross-reference linkages.

It was concluded that the application guidance volume should contain certain suggested content, including illustrations of how entities may apply specific concepts described in the *Framework* document. The final report contains that information, although it was decided that it is not practicable to identify or develop one case study illustrating application of all of the framework's concepts, and doing so is beyond the scope of this project. With the sharpened focus of the content of this volume, it was decided that a more appropriate title is *Application Techniques*, and the name has been revised accordingly. Also, directional linkages from the *Application Techniques* to the *Framework* document have been included.

F. GLOSSARY

Application Controls – Programmed procedures in application software, and related manual procedures, designed to help ensure the completeness and accuracy of information processing. Examples include computerized edit checks of input data, numerical sequence checks, and manual procedures to follow up on items listed in exception reports.

Compliance – Used with "objectives": having to do with conforming with laws and regulations applicable to an entity.

Component – There are eight enterprise risk management components: the entity's internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, and monitoring.

Control – 1. A noun, denoting an item, e.g., existence of a control – a policy or procedure that is part of internal control. A control can exist within any of the eight components. 2. A noun, denoting a state or condition, e.g., to effect control – the result of policies and procedures designed to control; this result may or may not be effective internal control. 3. A verb, e.g., to control – to regulate; to establish or implement a policy that effects control.

Criteria – A set of standards against which enterprise risk management can be measured in determining effectiveness. The eight enterprise risk management components, taken in the context of inherent limitations of enterprise risk management, represent criteria for enterprise risk management effectiveness for each of the four objectives categories.

Deficiency – A condition within enterprise risk management worthy of attention that may represent a perceived, potential, or real shortcoming, or an opportunity to strengthen enterprise risk management to provide a greater likelihood that the entity's objectives will be achieved.

Design – 1. Intent. As used in the definition, enterprise risk management is intended to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance as to achievement of objectives. 2. Plan; the way a process is supposed to work, contrasted with how it actually works.

Effected – Used with enterprise risk management: devised and maintained.

Enterprise Risk Management Process – A synonym for enterprise risk management applied in an entity.

Entity – An organization of any size established for a particular purpose. An entity, for example, may be a business enterprise, not-for-profit organization, government body, or academic institution. Terms used as synonyms include organization and enterprise.

Event – An incident or occurrence, from sources internal or external to an entity, that affects achievement of objectives.

General Controls – Policies and procedures that help ensure the continued, proper operation of computer information systems. They include controls over information technology management, information technology infrastructure, security management, and software acquisition, development, and maintenance. General controls support the functioning of programmed application controls. Other terms sometimes used to describe general controls are general computer controls and information technology controls.

Impact – Result or effect of an event. There may be a range of possible impacts associated with an event. The impact of an event can be positive or negative relative to the entity's related objectives.

Inherent Limitations – Those limitations of enterprise risk management. The limitations relate to the limits of human judgment; resource constraints, and the need to consider the cost of controls in relation to expected benefits; the reality that breakdowns can occur; and the possibility of management override and collusion.

Inherent Risk – The risk to an entity in the absence of any actions management might take to alter either the risk's likelihood or impact.

Integrity – The quality or state of being of sound moral principle; uprightness, honesty, and sincerity; the desire to do the right thing, to profess and live up to a set of values and expectations.

Internal Control – A process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations.

Internal Control System – A synonym for internal control applied in an entity.

Likelihood – The possibility that a given event will occur. Terms sometimes take on more specific connotations, with "likelihood" indicating the possibility that a given event will occur in qualitative terms such as high, medium, and low, or other judgmental scales, and "probability" indicating a quantitative measure such as a percentage, frequency of occurrence, or other numerical metric.

Management Intervention – Management's actions to overrule prescribed policies or procedures for legitimate purposes; management intervention is usually necessary to deal with non-recurring and non-standard transactions or events that otherwise might be handled inappropriately by the system (contrast this term with Management Override).

Management Override – Management's overruling of prescribed policies or procedures for illegitimate purposes with the intent of personal gain or an improperly enhanced presentation of an entity's financial condition or compliance status (contrast this term with Management Intervention).

Management Process – The series of actions taken by management to run an entity. Enterprise risk management is a part of and integrated with the management process.

Manual Controls – Controls performed manually, not by computer.

Objectives Category – One of four categories of entity objectives – strategic, effectiveness and efficiency of operations, reliability of reporting, and compliance with applicable laws and regulations. The categories overlap, so that a particular objective might fall into more than one category.

Operations – Used with "objectives": having to do with the effectiveness and efficiency of an entity's activities, including performance and profitability goals, and safeguarding resources against loss.

Opportunity – The possibility that an event will occur and positively affect the achievement of objectives.

Policy – Management's dictate of what should be done to effect control. A policy serves as the basis for procedures for its implementation.

Procedure – An action that implements a policy.

Reasonable Assurance – The concept that enterprise risk management, no matter how well designed and operated, cannot provide a guarantee regarding achievement of an entity's objectives. This is because of Inherent Limitations in enterprise risk management.

Reporting – Used with "objectives": having to do with the reliability of the entity's reporting, including both internal and external reporting of financial and non-financial information.

Residual Risk – The remaining risk after management has taken action to alter the risk's likelihood or impact.

Risk – The possibility that an event will occur and adversely affect the achievement of objectives.

Risk Appetite – The broad-based amount of risk a company or other entity is willing to accept in pursuit of its mission (or vision).

Risk Tolerance – The acceptable variation relative to the achievement of an objective.

Stakeholders – Parties that are affected by the entity, such as shareholders, the communities in which the entity operates, employees, customers, and suppliers.

Strategic – Used with "objectives": having to do with high-level goals that are aligned with and support the entity's mission (or vision).

Uncertainty – Inability to know in advance the exact likelihood or impact of future events.

G. ACKNOWLEDGMENTS

The COSO Board, Advisory Council, and PricewaterhouseCoopers LLP gratefully acknowledge the many executives, legislators, regulators, auditors, academics, and others who gave their time and energy to participating in and contributing to various aspects of the study. Also recognized are the considerable efforts of the COSO organizations and their members who responded to surveys, participated in workshops and meetings, and provided comments and feedback throughout the development of this framework.

The following PricewaterhouseCoopers partners provided important input to this framework: Dick Anderson, Jeffrey Boyle, Glenn Brady, Michael Bridge, John Bromfield, Gary Chamblee, Nicholas Chipman, John Copley, Michael de Crespigny, Stephen Delvecchio, Scott Dillman, P. Gregory Garrison, Bruno Gasser, Susan Kenney, Brian Kinman, Robert Lamoureux, James LaTorre, Mike Maali, Jorge Manoel, Cathy McKeon, Juan Pujadas, Richard Reynolds, Mark Stephen, Robert Sullivan, Jeffrey Thompson, and Shyam Venkat.

The following individuals also contributed to this study: Michael Haubenstock, Director, Enterprise Risk Management, Capital One Finance Corporation; Adrienne Willich, Manager of Operational Risk, Capital One Finance Corporation; and Daniel Mudge, President and Chief Operating Officer, OpVantage. Richard A. Scott, William G. Shenkir, and Paul L. Walker from the University of Virginia conducted preliminary research leading to this study. Thanks also go to Myra Cleary for her editorial guidance.

Special acknowledgment goes to Robert G. Eccles, President, Advisory Capital Partners, Inc. and former Harvard Business School Professor, for his extensive contributions to this framework.

Finally, we pay tribute to William H. Bishop, III, President of the Institute of Internal Auditors, who until his passing worked tirelessly to enhance the role and stature of the auditing profession. Bill's participation in this project, and indeed in COSO's internal control framework project, helped make those reports better. As a colleague and friend, he will be sorely missed.