COSO Enterprise Risk Management

Understanding the New Integrated ERM Framework

Robert R. Moeller

John Wiley & Sons, Inc.

COSO Enterprise Risk Management

COSO Enterprise Risk Management

Understanding the New Integrated ERM Framework

Robert R. Moeller

John Wiley & Sons, Inc.

This book is printed on acid-free paper.

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.

Published simultaneously in Canada.

Wiley Bicentennial Logo: Richard J. Pacifico

For general information on our other products and services, or technical support, please contact our Customer Care Department within the United States at 800-762-2974, outside the United States at 317-572-3993 or fax 317-572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

For more information about Wiley products, visit our Web site at http://www.wiley.com.

Library of Congress Cataloging-in-Publication Data:

Moeller, Robert R.
COSO enterprise risk management : understanding the new integrated ERM framework / Robert R. Moeller.
p. cm.
Includes index.
ISBN 978-0-471-74115-2 (cloth : alk. paper)
1. Risk management. I. Title.
HD61.M57 2007
658.15'5--dc22

2006102245

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

To my very best friend and wife,
Lois Moeller

CONTENTS

PREFACE

Risk management is one of those concepts wherein almost everyone will agree that, "Yes, we need a good risk management program!" but those same professionals will then have difficulty, when pressed for a better definition, explaining what they mean by the term *risk management.* The lack of a consistent understanding of risk management has until recently been similar to the earlier lack of a general understanding of the term *internal control.* Going as far back as the 1950s in the United States, auditors and general managers talked about the importance of good internal controls, but there was no one widely accepted, consistent definition of what was meant by that expression. It was not until the early 1990s with the release of the Committee of Sponsoring Organizations (COSO) internal control framework that we have had a consistent and widely recognized definition of internal controls for all organizations.

Risk management has had a similar history of inconsistent and not always clearly understood definitions. Insurance organizations had their own definitions of risk management, while others, such as credit management, have had a whole different set of definitions and understandings. Project managers had been frequently asked to rate a proposed new effort as having a high, medium, or low risk without fully understanding the meaning of such a risk-level rating. Until recently, all organizations, including for-profit entities, not-for-profits, and governmental agencies, have not had a consistent definition of the meaning of risk management as well as what actions were necessary to establish an effective risk management structure or framework. To help with this definition problem, the COSO standards-setting entity launched a new risk management definition or framework definition called COSO enterprise risk management (COSO ERM). This new risk management framework, officially released in late 2004, proposed a structure and set of definitions to

allow organizations of all types and sizes to understand and better manage their risk environments. As a new set of corporate guidance directives, COSO ERM does not receive that much enterprise-wide attention today but will, almost certainly, only become more important in upcoming years.

The major objective of this book is to help business professionals, at all levels, from staff internal auditors to corporate board members, to understand risk management in general and make more effective use of the new COSO ERM risk management framework. This book is designed to help professionals to better understand the COSO ERM framework and to make better use of this tool in understanding, using, and evaluating the risks associated with their business decisions. Using the COSO ERM framework's model and terminology, we will discuss the importance of understanding the various risks facing many aspects of business operations and how to use something called "one's appetite for risk" to help make appropriate decisions in many areas of business operations.

COSO ERM concepts are important for all levels of the organization. In addition to its applicability for more senior managers, this book will explain how all professionals in an organization can make better decisions through use of the COSO ERM framework. This framework provides a new way of looking at all aspects of risk in today's organization. Just as it took some years for the COSO internal controls framework to reach its current level of acceptance and criticality in organizations worldwide, the importance of COSO ERM will only grow with time. This book is designed to help professionals to develop and follow an effective risk culture for many of their business and operating decisions. Many of the chapters in this book will reference an example company, Global Computer Products, Inc., to help the reader understand the use and practical application of COSO ERM. This hypothetical example company will be described in more detail in the chapters following.

Among other topics, we will discuss the roles and responsibilities of an ERM function in today's enterprise. Similar but different from traditional internal audit functions, this new professional function would review areas of potential risk and report their findings and recommendations through the new vehicle of a risk assessment report, as discussed in Chapter 5.

The Sarbanes-Oxley Act (SOx) has had a major impact on how organizations should use and adapt COSO ERM. Legislated in the United States in 2002 after a series of major corporate failures and accounting scandals, SOx has established strong requirements on organizational internal controls and governance.

Chapter by chapter, this book covers the following aspects and elements of COSO ERM:

- **Chapter 1, Importance of Enterprise Risk Management Today.** This chapter discusses some of the events that led to COSO ERM, including ongoing industry and public concerns about the lack of a consistent definition of internal controls and an uncertainty of the meaning and concept of risk on an overall enterprise level. That path took us from the 1980s Treadway Report to the COSO internal control framework and external auditing's internal control standards. ERM did not have such a step-by-step path, but COSO ERM represents an important framework going forward.
- **Chapter 2, Risk Management Fundamentals.** The key concepts and terminology used in risk assessments are introduced here. These include some of the basic graphical and probability tools that have been used by risk managers over time as well as the terminology of risk assessments. This concept will be helpful in understanding risks in both a quantitative and qualitative sense and in using and understanding COSO ERM. As part of its discussion, the chapter will introduce some basic concepts of probability and how they are used to measure and assess risks.
- **Chapter 3, Components of COSO ERM.** A three-dimensional model or framework for understanding enterprise risk, COSO ERM consists of eight vertical components or layers as part of one model dimension with a second dimension of four vertical columns covering key risk objectives and a third dimension describing the organizational units that are part of the risk framework. This chapter describes the COSO ERM components, from the importance of the internal environment to the need for risk monitoring. An understanding of these framework components sets the stage for using or applying COSO ERM.
- **Chapter 4, COSO ERM Organizational Objectives.** Risk management must be understood in terms of its strategic, operational, reporting, and compliance objectives, as well as how it should be implemented throughout the organization, from an individual unit to the entire enterprise. These are the other two dimensions of COSO ERM. The chapter discusses their elements and how they all relate together. The idea is to think of ERM as an overall structure that will allow managers to understand and manage risks throughout an organization.

- **Chapter 5. Implementing an Effective ERM Program.** Every organization has high-level objectives that often include the need for growth and innovation, the desire for efficient allocation of capital, and the always important requirement to control costs. In order to achieve these objectives, an organization needs both an effective strategy and the capability to assess and manage any risks that can serve as impediments. Using our Global Computer Products model company as an example, this chapter will consider how the COSO ERM framework approach can help an organization to better manage risks and to achieve key objectives. This chapter will also outline the suggested approach for completing risk assessment reviews.
- **Chapter 6, Integrating ERM with COSO Internal Controls.** When COSO ERM was first released, some professionals incorrectly viewed this new risk-based framework as just an update of the COSO Internal Control framework of about ten years earlier. This would be an easy mistake to make. Both frameworks sort of look alike with their three-dimensional model concepts and with some common terminology; in addition, both are the responsibility of the COSO group. While other chapters describe the unique characteristics of COSO ERM, this chapter will revisit COSO internal controls and how that separate framework works with ERM. Both are important to an organization on several levels.
- **Chapter 7, Sarbanes-Oxley and COSO ERM.** Enacted in 2002, SOx has had a major impact on public corporations in the United States and worldwide. This chapter will explore how an effective risk management program, following COSO ERM, will help an organization to better comply with SOx and its Section 404 internal control assessment requirements. An effective risk management program will help senior management and the board of directors to better understand and comply with the requirements of this important legislation.
- **Chapter 8, Importance of ERM in the Corporate Board Room.** The board of directors and its audit committee has a very important responsibility in understanding and accepting all levels of organizational risk. This chapter will include guidance to help board members to better understand COSO ERM and how it relates to other corporate governance requirements. The chapter will also introduce the board of directors risk committee, an evolving new element of

corporate governance. An effective ERM program at this very senior board level of the organization is essential for the total achievement of governance and success objectives.

- **Chapter 9, Role of Internal Audit in ERM.** Internal audit plays an important role in monitoring ERM in the organization, although they do not have the primary responsibility for its implementation and maintenance. This chapter looks at important roles for internal audit in reviewing critical control systems and processes as well as techniques for building a risk-based approach to the overall internal audit process. Internal auditors have always considered risks in planning and performing their audits, but COSO ERM as well as newer Institute of Internal Auditors (IIA) standards suggest a greater need for internal audit emphasis on ERM.
- **Chapter 10, Understanding Project Management Risks.** Many organizational efforts are organized as projects—limited-duration activities that are managed as separate efforts within normal organization boundaries. Better-organized projects follow the Project Management Institute's de facto standard called PMBOK (Project Management Book of Knowledge), with its own risk management component. This chapter will discuss how to integrate PMBOK risks with the overall ERM framework to better manage and control project risks.
- **Chapter 11, Information Technology and ERM.** Because of the complexity in building and maintaining computer systems and applications, risk management has been very important to information technology (IT) processes. This chapter will look at three important IT areas and how COSO ERM should help an organization to better understand those IT risks:
  1. *Application systems risks.* An enterprise often faces significant risks when they purchase or develop new applications, implement them to a production status, and then maintain them as production systems. There are risks associated with each of these areas, and COSO ERM can help in their management.
  2. *Effective continuity planning.* Once more commonly called disaster recovery planning, computer systems and operations can be subject to unexpected interruptions in their services. COSO ERM provides an enhanced framework to understand and manage those risks.

3. *Worms, viruses, and systems network access risks.* There are many risks and threats in our world of interconnected systems and resources. COSO ERM provides guidance to assist an organization in deciding where it should allocate resources. This chapter also discusses the more significant of these potential risks.

- **Chapter 12, Establishing an Effective Risk Culture.** Effective risk management needs to go beyond implementing COSO ERM as an initiative with one or another organization functions. It should be an overall philosophy that is understood and used throughout the organization. This chapter discusses how to establish an ERM function, with an emphasis on the larger organization, as well as the roles and responsibilities of the chief risk officer (CRO), who would lead such a function. While such an organization-wide ERM function is almost expected to be appropriate for the larger organization, smaller organizations also need to consider establishing structures to introduce a risk management culture throughout their organizations.
- **Chapter 13, ERM Worldwide.** While COSO ERM is a U.S.-based standard, there are other risk management standards that have been released throughout the world. This chapter will look at these various international standards, including the British Standard BS-6079-3:2000 and how they relate to COSO ERM. There will also be an emphasis on the draft ISO international risk management standard on risk management, and why it may become very important to today's organization.
- **Chapter 14, COSO ERM Going Forward.** It took five to ten years after its initial publication for the COSO internal control framework to become recognized as a worldwide de facto standard for measuring and assessing internal controls. This chapter predicts a similar future for COSO ERM. Whether or not that is the case, the ERM concepts here will be important for managers, at all levels, moving into the future.

1

IMPORTANCE OF ENTERPRISE RISK MANAGEMENT TODAY

Well-recognized or mandated standards are important for any organization. Compliance with them allows an enterprise to demonstrate they are following best practices or are in compliance with regulatory rules. For example, an organization's financial statements are prepared to be consistent with generally accepted accounting principles (GAAP)—a common standard—and are audited by an external audit firm in accordance with generally accepted auditing standards (GAAS). This financial audit process applies to virtually all organizations worldwide, no matter their size or organization structure. Investors and lenders want an external party—an independent auditor—to examine financial records and attest whether they are fairly stated. As part of this financial statement audit process, that same external auditor has to determine that there are good supporting internal controls surrounding all significant financial transactions.

Internal controls cover many areas in organization operations. An example of an internal control is a separation of duties control where a person who prepares a check for

issue to an outside party should not be the same person who approves the check. This is a common and well-recognized internal control, and many others relate to similar situations where one person or process has been designated to check the work of another party. While this is a simple example of an internal control, there have been many differing approaches to what is meant by internal controls.

COSO RISK MANAGEMENT: HOW DID WE GET HERE?

With practices almost the same as can be found in the information systems, the world of auditing, accounting, and corporate management are filled with product and process names that are quickly turned into acronyms. We quickly forget these names, words, or even the concepts that created the acronym and continue just using the several letter acronyms. For example, International Business Machines Corporation (IBM) many years ago launched a custom software product for just one customer called the Customer Information Control System (CICS) back in the old legacy system days of the early 1970s when it needed a software tool to access files on an on-line basis. Competitors at that time had on-line, real-time software but IBM did not. This IBM product was enhanced and generalized over the years. It is still around today for legacy systems and is still called CICS. Today's users call it "kicks," and the meaning of the acronym has been essentially lost and forgotten.

The internal control standards organization goes by its acronym of COSO (Committee of Sponsoring Organizations). Of course, that explanation does not offer much help—who is this committee and what are they sponsoring? To understand how this internal control standard came about, it is necessary to go back to the late 1970s and early 1980s, a period when there were many major organizational failures in the United States due to conditions including very high inflation, the resultant high interest rates, and some aggressive corporate accounting and financial reporting approaches. The scope of these corporation failures seems minor today when contrasted with the likes of the more recent Enron or WorldCom financial frauds, but they raised major concerns at that earlier time. In the 1970s, concern was that several major corporations suffered a financial

collapse shortly after the release of their financial reports, signed by their external auditors, that showed both adequate earnings and financial health. Some of these failures were caused by fraudulent financial reporting, but many others turned out to be victims of the high inflation and high interest rates during that period. It was not uncommon for companies that failed to have issued fairly positive annual reports just in advance of the bad news about to come. This also was a period of high regulatory activity in the United States, and some members of Congress drafted legislation to ''correct'' these business or audit failures. Congressional hearings were held, but no legislation was ever passed. Rather, a private professional group, the National Commission on Fraudulent Financial Reporting, was formed to study the issue. Five U.S. professional financial organizations sponsored this Commission: the American Institute of Certified Public Accountants (AICPA), the Institute of Internal Auditors (IIA), the Financial Executives Institute (FEI), the American Accounting Association (AAA), and the Institute of Management Accountants (IMA). Named after its chair, Securities and Exchange Commission (SEC) Commissioner James C. Treadway, the authority had as its official name The Committee of Sponsoring Organizations of the Treadway Commission. Today, that group has become known by its acronym name, COSO.

The original focus of COSO was not on risk but on the reasons behind the internal control problems that had contributed to those financial reporting failures. COSO's first report, released in 1987,[1] called for management to report on the effectiveness of their internal control systems. Called the Treadway Commission Report, it emphasized the key elements of an effective system of internal controls, including a strong control environment, a code of conduct, a competent and involved audit committee, and a strong management function. Enterprise risk management (ERM) was not a key topic at that time. The Treadway Report emphasized the need for a consistent definition of internal control and subsequently published what is now known as the COSO definition of internal control, now the generally recognized worldwide internal accounting control standard or framework.

That final COSO report on internal controls was released in 1992 with the official title *Internal Control–Integrated Framework.*[2] Throughout this book, that 1992 report is referred to as the COSO internal control report or framework to differentiate it from the COSO enterprise risk management (COSO ERM framework), our main topic. The COSO internal control report proposed a common framework for the definition of internal control, as well as procedures to evaluate those controls.[3] For virtually all persons

involved in modern business today, an understanding of that COSO definition of internal controls is essential.

COSO INTERNAL CONTROL FRAMEWORK

The term *internal control* has been part of the vocabulary of business for many years, but it historically never has had a precise, consistent definition. The COSO internal control report developed a now almost universally accepted definition or description of internal control, as follows:

> Internal control is a process, affected 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[4]

This COSO definition of internal control should be familiar to many managers, auditors, and others as it forms the basis for Sarbanes-Oxley Act (SOx) Section 404 internal control assessments[5] that are very important to virtually all organizations worldwide and will be discussed in Chapter 7.

Using this general definition of internal control, COSO uses a three-dimensional model to describe an internal control system in an organization. The model, as shown in Exhibit 1.1, consists of five horizontal levels or layers, three vertical components, and multiple sectors spanning its third dimension. This model might be viewed in terms of its $5 \times 3 \times 3$ or 45 individual components. However, these are not individual components but are all interconnected, with the internal controls in each depending on the others. While each level and component of the COSO internal control framework is important for understanding internal controls in an organization, we will focus here on two horizontal levels: the control environment foundation level and the risk environment level. These are particularly important components for understanding how the COSO internal control framework relates to the COSO ERM model introduced later in Chapters 3 and 4.

COSO Internal Control Elements

The Control Environment. Just as any building needs a strong foundation, the COSO internal control framework has its foundation in what COSO calls the *internal control environment*, the starting basis for all internal controls in an entity. This control environment level of the internal control model has a

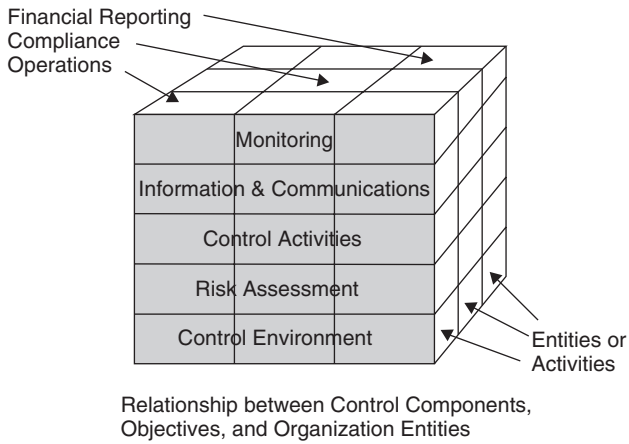

EXHIBIT 1.1 AN ORGANIZATION'S COSO INTERNAL CONTROL MODEL

Source: Robert Moeller, *Brink's Modern Internal Auditing,* 6th ed. Copyright © 2005, John Wiley and Sons. Reprinted with permission of John Wiley & Sons, Inc.

pervasive influence on how business activities are structured and risks are assessed in an organization. It serves as a foundation for all other components of internal control and has an influence on each of the three internal control objectives and all activities. The control environment reflects the overall attitude, awareness, and actions by the board of directors, management, and others regarding the importance of internal controls in the organization.

An organization's history and culture often play a major role in forming this control environment. When an organization has historically placed a strong management emphasis on producing error-free products, when senior management continues to emphasize this importance, and if this message has been communicated to all levels, this becomes a major control environment factor for the organization. The words of senior management, the chief executive officer (CEO) and others, communicate a strong message to employees, customers, and other stakeholders. This very important set of messages is known as the *tone at the top*. However, if senior management has a reputation for "looking the other way" at policy violations and other matters, this "management doesn't really care" message will be quickly communicated to others in the enterprise as well. A positive "tone at the top" set of messages by senior management will establish this theme in the control environment for the entire organization.

The COSO control environment component has major elements that managers and auditors should always understand and keep in mind when implementing organization changes or performing reviews of activities or

units. These form the foundations or basis for good internal controls. Managers should try to develop a general awareness of these control environment factors covering their overall organization and should consider them essential components of the internal control framework. The control environment, as well as other elements of the COSO internal control model, is further divided into multiple control factors. Definitions of this standard can be confusing, with the internal control framework having a control environment component consisting of multiple control factors. Although space does not allow a discussion of the entire COSO internal control framework, the following are the identified control factors for the framework's control environment. These should also help to provide an understanding of how the overall COSO internal control framework is defined.

Control Environment Factors

Integrity and Ethical Values

The collective integrity and ethical values of an organization are essential elements of its control environment and are often defined and broadcast through the ''tone at the top'' messages communicated by senior management. If an enterprise has developed a strong code of business conduct that emphasizes integrity and ethical values, and if all stakeholders appear to follow that code, these are strong messages that the organization has a good set of ethical values. A code of conduct today is an important component of organizational governance. However, even though an organization may have a strong code of conduct, its principles can be violated through just ignorance of that code rather than by deliberate employee malfeasance. In many instances, employees may not know that they are doing something wrong or may erroneously believe that their actions are in the organization's best interests. This ignorance is often caused by poor moral guidance by senior management rather than by any overall employee intentions to deceive. Often embedded in that code of conduct, an organization's policies and values must be communicated to all levels of the organization. While there may always be ''bad apples'' in any organization, a strong policy and demonstrated appropriate actions will encourage everyone to act correctly. Going back to our check issuance separation of duties control example, the ethical values of the organization should be strong enough that the approving party is obligated to review the check request rather than just "rubber stamping" a signature with no scrutiny or review. When performing an independent review in a given area, an auditor or manager should always determine if appropriate messages or signals have been transmitted throughout the organization.

All managers—as well as other stakeholders—should have a good understanding of their organization's code of conduct and how it is applied and communicated. If the code is out of date, does not appear to address important ethical issues facing an organization, or is not communicated to all stakeholders on a recurring basis, failure to broadcast this message may represent a significant internal control deficiency to the organization. What types of issues are included in a code of conduct? The issues covered may vary, but Exhibit 1.2 is an example of such a code of conduct table of contents.

While a code of conduct describes the rules for ethical behavior in an organization, and while senior members of management may regularly transmit a proper ethical message, other incentives and temptations can erode this overall internal control environment. Individuals in the enterprise may be tempted to engage in dishonest, illegal, or unethical acts if their organization gives them strong incentives or temptations to do so. For example, an enterprise may establish very high, unrealistic performance targets for sales or production quotas. If there are strong rewards for the achievement of these performance goals—or worse, strong threats for missed targets—employees may be encouraged to engage in fraudulent or questionable practices or to record fictitious account transactions to achieve those goals. The kinds of temptations that encourage stakeholders to engage in improper accounting or similar acts include:

- Nonexistent or ineffective controls, such as poor segregation of duties in sensitive areas, that offer temptations to steal or to conceal poor performance
- High decentralization that leaves top management unaware of actions taken at lower organization levels and thereby reduces the chances of getting caught
- A weak management function that has neither the ability nor the authority to detect and report improper behavior
- Penalties for improper behavior that are insignificant or unpublicized and thus lose their value as deterrents

There is a strong message here both for responsible managers and for the enterprise in total. First, a manager should always consider these control environment factors when assessing organization performance, and should be skeptical and perform appropriate tests when reviewing various areas of operations. Whenever things look ''too good,'' a manager might want to look a bit harder. This more detailed look at operational types of assessments

The following topics are found in a typical organization code of conduct.

I. Introduction.

A. Purpose of this Code of Conduct: A general statement about the background of this Code of Conduct.

B. Our Commitment to Strong Ethical Standards: A restatement of the Mission Statement and printed letter from the CEO.

C. Where to Seek Guidance: A description of the ethics hotline process.

D. Reporting Noncompliance: Guidance for whistleblowers—how to report.

E. Your Responsibility to Acknowledge the Code: A description of the code acknowledgment process.

II. Fair Dealing.

A. Our Selling Practices: Guidance for dealing with customers.

B. Our Buying Practices: Guidance and policies for dealing with vendors.

III. Conduct in the Workplace.

A. Equal Employment Opportunity Standards: A strong commitment statement.

B. Workplace and Sexual Harassment: An equally strong commitment statement.

C. Alcohol and Substance Abuse: A policy statement in this area.

IV. Conflicts of Interest.

A. Outside Employment: Limitations on accepting employment from competitors.

B. Personal Investments: Rules regarding using company data to make personal investment decisions.

C. Gifts and Other Benefits: Rules regarding receiving bribes and improper gifts.

D. Former Employees: Rules prohibiting giving favors to ex-employees in business.

E. Family Members: Rules about giving business to family members, creating potential conflicts of interest.

V. Company Property and Records.

A. Company Assets: A strong statement on employees' responsibility to protect assets.

B. Computer Systems Resources: An expansion of the company assets statement to reflect all aspects of computer systems resources.

EXHIBIT 1.2 CODE OF CONDUCT TOPICS EXAMPLE

C. Use of the Company's Name: A rule that the company name should be used only for normal business dealings.

D. Company Records: A rule regarding employee responsibility for records integrity.

E. Confidential Information: Rules on the importance of keeping all company information confidential and not disclosing it to outsiders.

F. Employee Privacy: A strong statement on the importance of keeping employee personal information confidential to outsiders and even other employees.

G. Company Benefits: Employees must not take company benefits where they are not entitled.

VI. Complying with the Law.

A. Inside Information and Insider Trading: A strong rule prohibiting insider trading or otherwise benefiting from inside information.

B. Political Contributions and Activities: A strong statement on political activity rules.

C. Bribery and Kickbacks: A firm rule of using bribes or accepting kickbacks.

D. Foreign Business Dealings: Rules regarding dealing with foreign agents in line with the Foreign Corrupt Practices Act.

E. Workplace Safety: A statement on the company policy to comply with OSHA rules.

F. Product Safety: A statement on the company commitment to product safety.

G. Environmental Protection: A rule regarding the company's commitment to comply with applicable environmental laws.

EXHIBIT 1.2 CODE OF CONDUCT TOPICS EXAMPLE *(CONTINUED)*

Source: Robert R. Moeller, *Sarbanes-Oxley and the New Internal Auditing Rules,* Copyright © 2004, John Wiley and Sons. Reprinted with permission of John Wiley & Sons, Inc.

should not be to just find something wrong in the reported "too-good-to-be-true" numbers but also to assess whether deficiencies in the control environment may lead to possible fraudulent activities. This internal control environment factor of integrity and ethical values should always be a major component of the COSO control environment. In order for an organization to have good internal controls, it must have strong integrity standards and high overall ethical values.

Commitment to Competence

An organization's control environment can be seriously eroded if a significant number of positions are filled with persons lacking required job skills. Managers will encounter the situation from time to time when a person has been assigned to a particular job but does not seem to have the appropriate skills, training, or intelligence to perform that job. Because all humans have different levels of skills and abilities, adequate supervision and training should be available to help employees until proper skills are acquired.

An organization needs to specify the required competence levels for its various job tasks and to translate those requirements into necessary levels of knowledge and skill. By placing the proper people in appropriate jobs and giving adequate training when required, an enterprise is making a *commitment to competence*, an important element in the organization's overall control environment. Managers often find it valuable to assess whether adequate position descriptions have been created, whether procedures are in operation to place appropriate people in those positions, and whether training and supervision are adequate.

Although an important portion of the control environment, assessments of staff competence can be difficult. While many human resources functions often have elaborate grading and evaluation schemes, these too often become exercises where everyone at all levels is rated "above average". In a high-level subjective manner, management should assess whether their staff at all levels is ''competent'' with regard to assigned work duties and with their efforts to satisfy overall organization objectives. If a manager visits a remote subsidiary operation and finds that no one in the accounting department there seems to have any knowledge of how to record and report financial transactions, and also that no training program exists to help these ''accountants,'' control environment issues can be raised for this operating unit as well as for larger units. This is the type of issue to be discussed with first-line managers for that unit as well as with more senior management and the human resources function.

A special case of the importance of a commitment to competence occurs when a CEO appoints a son or daughter to a high-level executive position while there is no evidence that the progeny has the experience or skill to handle the job. These arrangements usually work only when the child has previously spent some time "in the trenches" before appointment to a more senior position. The grooming or training of the son or daughter says much about the organization's commitment to competence.

Board of Directors and Audit Committee

The control environment is very much influenced by the actions of an organization's board of directors and its audit committee. In past years, and certainly prior to SOx, boards and their audit committees often were dominated by senior management, with only limited, minority representation from outside shareholders. This created situations wherein the boards were not totally independent of management. Company officers sat on the board and were, in effect, managing themselves, often with less concern for the outside shareholders than for their own business or personal interests. As discussed in Chapter 7, SOx has changed all of that. Boards today now have a more important corporate governance role, and their audit committees are required to consist of independent, outside directors.

In addition to now being a SOx legal requirement, an active and independent board is an essential component of an organization's control environment. Board members should ask appropriate questions to top management and give all aspects of the organization detailed scrutiny. By setting high-level policies and by reviewing overall conduct, the board and its audit committee have the ultimate responsibility for setting this ''tone at the top.''

Management's Philosophy and Operating Style

These senior management factors have a considerable influence over an organization's control environment. As discussed in Chapter 5 on implementing an effective risk management program, some top-level managers frequently take significant organization risks in their new business or product ventures, while others are very cautious and conservative. Some persons seem to operate by the "seat of the pants" while others insist that everything must be properly approved and documented. As an example, a given manager may take a very aggressive approach in the interpretation of tax and financial-reporting rules, while another may prefer to go by the book. These comments do not necessarily mean that one approach is always good and the other consistently bad or incorrect. A small, entrepreneurial organization may be forced to take certain business risks to remain competitive while one in a highly regulated industry would be more risk averse.

These management philosophy and operational style considerations are all part of the control environment for an organization. Managers and others responsible for assessing internal controls should understand these factors and take them into consideration when installing and establishing an effective system of internal controls for the overall enterprise. While no one set of styles and philosophies is the best for all, these factors are important

when considering the other components of internal control in an organization. While discussed as part of the internal control environment here, the need to better understand these risk-related control environment factors is one of the reasons for COSO ERM.

Organization Structure

The organization structure component provides a framework for planning, executing, controlling, and monitoring activities for achieving overall objectives. This is an aspect of the control environment that relates to the way various functions are managed and organized, following the classic organization chart. Some organizations are highly centralized, while others are decentralized by product or geography. Still others are organized in a matrix manner with no single direct lines of reporting. This structure is a very important aspect of the organization's control environment. No one structure provides a preferred environment for internal controls.

There are many ways in which the various components of an organization can be assembled. Organizational control is part of a larger control process. The term *organization* is often used interchangeably with the term *organizing* and means about the same thing to many people. *Organization* sometimes refers to hierarchical relationships among people but is also used broadly to include all of the problems of management. This book and other sources generally use the term *organization* to refer to the organizational entity, such as a corporation, a not-for-profit association, or any organized group. We sometimes use *enterprise* as an synonym for *organization.* This section considers the organization as the set of *arrangements* developed as a result of the organizing process.

An organization can be described as the way individual work efforts are both assigned and subsequently integrated for the achievement of overall goals. While in a sense this concept could be applied to the manner in which a single individual organizes his or her efforts, it is more applicable when a number of people are involved in a group effort. For a large modern corporation, a strong plan of organizational control is an important component of the system of internal control. Individuals and subgroups must have an understanding of the total goals and objectives of the group or entity of which they are a part. Without such an understanding, there can be significant control weaknesses.

Every organization—whether a business, government, philanthropic, or some other unit—needs an effective plan of organization. A manager responsible for any function or unit needs to have a good understanding of this organizational structure and the resultant reporting relationships,

whether a functional, decentralized, or matrix organization structure. Often, a weakness in organizational controls can have a pervasive effect throughout the total control environment. Despite clear lines of authority, organizations have built-in inefficiencies that become greater as the size of the organization expands. These inefficiencies can often cause control procedures to break down, and management should be aware of them when evaluating the organizational control environment in the organization.

Complex or not-well-understood organizational structures can cause some major challenges here. In today's economy, there are many situations wherein a division or unit is spun off as an independent corporation by its former parent company. While the employees of this new spun-off corporation would have followed the systems and procedures of the previous parent, they now have the responsibility to establish their own organizational structure controls. Organizational structure lines of authority can become confusing for stakeholders in the environment of corporate mergers, joint ventures, and acquisitions. All too often the internal control structure is ignored while the free-standing business is built and financial structure details are established.

Assignment of Authority and Responsibility

This COSO-defined area of the control environment is similar to the organization structure factors previously discussed. An organization's structure defines the assignment and integration of the total work effort. The assignment of authority is essentially the way responsibilities are defined in terms of job descriptions and structured in terms of organization charts. Although job assignments can never fully escape some overlapping or joint responsibilities, the more precisely these responsibilities can be stated, the better. The decision of how responsibilities will be assigned will often avoid confusion and conflict between individual and group work efforts.

Many organizations of all types and sizes today have streamlined their operations and pushed their decision-making authority downward and closer to the front-line personnel. The idea is that these front-line employees should have the knowledge and power to make important decisions in their own area of operations rather than be required to pass the request for a decision up through organization channels. The critical challenge that goes with this delegation or empowerment is that although it can delegate some authority in order to achieve some organizational objectives, senior management is ultimately responsible for any decisions made by those subordinates. An organization can place itself at risk if too many decisions involving higher-level

objectives are assigned at inappropriately lower levels without adequate management review. In addition, each person in the enterprise must have a good understanding of that organization's overall objectives as well as how an individual's actions interrelate to achieve those objectives. The framework section of the actual COSO Internal Controls report[6] describes this very important area of the control environment as follows:

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

Human Resources Policies and Practices

Human resource practices cover such areas as hiring, orientation, training, evaluating, counseling, promoting, compensating, and taking appropriate remedial actions. While the human resources function should have adequately published policies in these areas, their actual practice areas send strong messages to employees regarding their expected levels of ethical behavior and competence. The higher-level employee who openly abuses a human resources policy, such as ignoring a plant smoking ban, quickly sends a message to others in the organization. That message grows even louder when a lower-level employee is disciplined for the same unauthorized cigarette while everyone looks the other way at the higher-level violator.

Areas where these human resources policies and practices are particularly important include:

- *Recruitment and hiring.* The organization should take steps to hire the best, most qualified candidates. Potential employee backgrounds should be checked to verify their education credentials and prior work experiences. Interviews should be well organized and in-depth. They should also transmit a message to the prospective candidate about the organization's values, culture, and operating style.
- *New employee orientation.* A clear signal should be given to new employees regarding the organization's value system and the consequences of not complying with those values. This often occurs when new employees are introduced to the code of conduct and asked to formally acknowledge their acceptance of that code. Without these messages, new employees may join the organization lacking an appropriate understanding of its values.
- *Evaluation, promotion, and compensation.* There should be a fair performance evaluation program in place that is not subject to an

excessive amount of managerial discretion. Because issues such as evaluation and compensation can violate employee confidentiality, the overall system should be established in a manner that appears to be fair to all members of the organization. Bonus incentive programs are often useful tools to motivate and reinforce outstanding performance by all employees, but there must be a perception that these bonuses are awarded in a fair and equitable manner.

- *Disciplinary actions.* Consistent and well-understood policies for disciplinary actions should be in place. All employees should know that if they violate certain rules, they will be subject to a progression of disciplinary actions leading up to dismissal. The organization should take care to ensure that no double standard exists for disciplinary actions—or, if any such double standard does exist, that higher-level employees are subject to even more severe disciplinary actions.

Effective human resource policies and procedures are a critical component in this overall control environment. Messages from the top of strong organization structures will accomplish little if the organization does not have strong human resource policies and procedures in place. Management should always consider this element of the control environment when performing reviews of other elements of the internal control framework.

Exhibit 1.1 showed the components of the COSO internal control framework as a cube, with the control environment as the lowest or foundation component. This concept of showing the control environment acting as the foundation is very appropriate. The COSO internal control environment and the seven just-discussed control environment factors provide the foundation for the other components of this COSO internal control framework. An organization that is building a strong internal control structure should give special attention to placing solid foundation bricks in their control environment structure.

Risk Assessment. With reference again to Exhibit 1.1, the next level or layer above the control foundation is risk assessment. An organization's ability to achieve its objectives can be at risk due to a variety of internal and external factors. As part of its overall internal control structure, an organization should have a process in place to evaluate the potential risks that may impact attainment of its various internal control objectives. While this type of risk assessment process can be either a formal quantitative risk assessment process or less formal approaches, as will be introduced in

Chapter 2, there should be at least a minimal understanding of the risk assessment process. An organization that has an informal objective of ''no changes'' in its marketing plans may want to assess the risk of not achieving that objective due to the entry of new competitors that may place pressures on the objective of doing the same as in the prior year. Risk assessment should be a forward-looking process. That is, many organizations have found that the best time and place to assess their various levels of risks is during an annual or periodic planning process. This risk assessment process should be performed at all levels and for virtually all activities within the organization. The COSO internal control framework describes risk assessment as a three-step process:

1. Estimate the significance of the risk.
2. Assess the likelihood or frequency of the risk occurring.
3. Consider how the risk should be managed and assess what actions must be taken.

The COSO ERM framework, as discussed starting in Chapter 3, retains these same factors but treats this concept in a much more thorough and almost elegant fashion. The COSO internal control risk assessment process puts the responsibility on management to go through the steps to assess whether a risk is significant and then, if so, to take appropriate actions. COSO ERM leads to a far more comprehensive, integrated approach to understanding an organization's risks as part of their internal control environment.

The COSO internal control framework—released over ten years before COSO ERM—emphasized that risk analysis is not a theoretical process, but often can be critical to an entity's overall success. As part of its overall assessment of internal control, management should take steps to assess the risks that may impact the overall organization as well as the risks over various organization activities or entities. A variety of risks, caused by either internal or external sources, may affect the overall organization. COSO ERM has defined some essential components, suggested a common language, and outlined an approach to allow an organization to better manage its enterprise-level risks.

Other Components and Activities

The control environment as well as risk assessment represent only two components of the overall COSO internal control framework. While these two set the stage both for COSO internal controls and ERM, the other

internal elements of control activities, information and communications, and monitoring are also very important for understanding the overall COSO internal control framework. An understanding of the COSO internal control framework is essential for today's manager in all levels and components of an organization. If for no other reason, that understanding was a requirement for an organization to achieve SOx Section 404 internal control compliance, as summarized in Chapter 7. However, the objective of this book is not to provide a detailed description of the entire COSO internal control framework but rather to introduce it as perhaps a precursor to ERM.

Internal controls and enterprise risk management each take a different perspective to understanding and evaluating activities in an organization. While internal controls are more focused on established aspects of an organization's daily activities, ERM focuses on activities that an organization and its managers may or may not do. A manager is interested, for example, in the controls necessary to accumulate accounting transactions, to summarize them in a well-controlled manner, and to publish them as the financial results of the organization. However, that same manager may be concerned about the financial impact on the organization due to the launch of a new product, the reaction and actions of competitors, and overall market conditions for that new product launch. All of these do not involve the here and now of an internal control framework, but they do involve risk.

COSO INTERNAL CONTROL FRAMEWORK AS A RECOGNIZED STANDARD

The COSO internal control framework was released in 1992 as a three-volume publication describing this approach or standard. Although there initially was limited mention or recognition of this new suggested standard beyond comments in some AICPA and IIA publications, the major public accounting firms at that time and others began to see its value. Over the next several years, it began to be referenced in various professional books and as an offering in public seminars.

Public accounting auditing standards were once the responsibility of the AICPA's Auditing Standards Board (ASB), who released their standards in the form of numbered documents called Statements on Auditing Standards (SASs). These auditing standards were released when there was a need for improved audit clarification or standards in some area. The COSO internal control framework got its official stamp of approval with the release of SAS 78[7] an auditing standard that mandated the use of the COSO Internal

Control report. Although it generally followed COSO, SAS 78 emphasizes the reliability of the financial reporting objective by placing it first, ahead of COSO's effectiveness and efficiency of operations, and compliance with applicable laws and regulations. SAS 78 was issued as an amendment to the previous internal control auditing standard, SAS 55, and legitimatized and mandated the use of COSO internal control standards for audits of U.S. corporations after its 1996 effective date.

The responsibility of the AICPA's ASB to set auditing standards changed with SOx in 2002. A new entity called the Public Company Accounting Oversight Board (PCAOB) has been established to supervise all independent auditing firms, working under SOx reporting requirements, and to take responsibility for the release of auditing standards. As part of its start-up as a new regulatory function, the PCAOB initially said that the existing SAS statements would remain in force until new standards were issued. That meant the COSO internal control standards, as outlined in SAS 78, continue as the definition of an internal control framework. The PCAOB subsequently said that it recognized and accepted the COSO framework.[8]

ORIGINS OF COSO ERM

The release of the COSO internal control framework caused other professionals to suggest there were similar standards in other areas where consistent definitions were lacking. One of these was risk management, a concept that had been receiving multiple definitions and interpretations by various professionals. This was the era prior to SOx and its rules, discussed in Chapter 7, where public accounting firms were increasingly taking responsibility for their audit clients' internal audit functions through what was called outsourcing. Some firms involved in this process began to call themselves risk management professionals, although some were not that clear about what was meant by risk management.

In 2001 COSO contracted the public accounting firm Pricewaterhouse-Coopers (PwC) to develop a common consistent definition for risk management. The result was COSO ERM, which will be discussed in subsequent chapters of this book.

NOTES

1. Report of the National Commission on Fraudulent Financial Reporting (National Commission on Fraudulent Financial Reporting, 1987), The Treadway Report, AICPA, 1987.

2. Committee of Sponsoring Organizations of the Treadway Commission, published by AICPA, Jersey City, NJ, 1992.
3. For a more detailed reference to the COSO Internal Control–Integrated Framework, see Robert Moeller, *Brink's Modern Internal Auditing,* 6th ed., Hoboken, NJ: John Wiley & Sons, 2005.
4. *Internal Control–Integrated Framework,* The Committee of Sponsoring Organizations of the Treadway Committee, New York, 1992.
5. For more information on the Sarbanes-Oxley Act and its internal control reporting requirements, see Robert Moeller, *Sarbanes-Oxley and the New Internal Auditing Rules,* Hoboken, NJ: John Wiley & Sons, 2004.
6. Committee of Sponsoring Organizations of the Treadway Commission, *Internal Control–Integrated Framework,* New York: AICPA, 1992.
7. SAS 78, Consideration of Internal Control in a Financial Statement Audit: An Amendment to SAS No. 55, New York: AICPA, 1995.
8. PCAOB, Rule 3100, Compliance with Public Accounting and Related Professional Practice Standards, February 15, 2005, www.pcaobus.org.

2

Risk Management Fundamentals

Risk management had been considered as primarily only an insurance-related concept for many years. An individual, organization, or enterprise would use a risk-based approach to make a decision as to what type and how much insurance to purchase. The factors of relative risk and the cost to cover that risk have always entered into the decision to purchase insurance. Risks and insurance costs also change over time. Fire insurance to cover an individual's home is an example of this. Back in the days of oil lanterns for light and straw for the horses stored in a nearby stable, there was always a high risk of fires. We only need to think of the great Chicago fire of 1871 where, as legend suggests, a cow kicked over a lantern and caused a fire that devastated the city. The risk of that type of fire is not that great today, and fire insurance is not that expensive, in a relative sense. However, there is always the possibility of a lightning strike or electrical malfunction to cause a fire in the home; mortgage finance companies require fire insurance coverage and, even if having no mortgage, all prudent persons today will purchase such fire insurance even if not required. A destructive fire to one's home presents a low-level but consistent risk. While the cost of homeowner fire insurance is relatively low, an

individual homeowner might assess other types of potential risks, such as for earthquakes, and not purchase insurance because of an assessed very low chance of occurrence. In a given geographic area, the possibility of an earthquake may appear so minimal that an owner may not purchase any insurance despite the low cost of such a policy. In another situation, an individual may live by a body of water where there are damaging floods every several years. Even if one could purchase flood insurance—and some insurance companies will not even offer it—the insurance coverage will be very expensive. Some may decide to accept the risk of a flood in future years and will go without insurance coverage. In all of these cases, there has been a risk management decision to purchase or not purchase insurance.

Starting with its insurance-buying foundations, risk management, as it is practiced today, is essentially a post-1960s phenomenon. Moving beyond concerns about natural weather-related events, risk management began to emphasize protecting organizations against a major catastrophe, such as the risks surrounding a centralized computer system where all information system assets were stored in one facility. The concern about managing risks surrounding that one centralized computer system moved to a general concern about managing a wide range of other business risks.

Enterprises and individuals today face a wide variety of risks and need some help and tools to help sort through all of these in order to make some more rational cost and risk-related decisions. This is the process of risk management. While some in business today just assess an area as high, medium, or low risk and then make quick insurance or risk-protection decisions based on those options, others use more sophisticated qualitative or quantitative tools to help them understand and

evaluate risks. This chapter will briefly survey some fundamental modern risk management approaches with an objective of helping to establish more effective enterprise risk management procedures in an enterprise. The concepts discussed here should be of use in the effective implementation of the Committee of Sponsoring Organizations' enterprise risk management framework (COSO ERM), as discussed in the other chapters of this book.

FUNDAMENTALS: RISK MANAGEMENT PHASES

Risk management should be considered a four-step process: (1) risk identification, (2) quantitative or qualitative assessment of the documented risks, (3) risk prioritization and response planning, and (4) risk monitoring. Whether using COSO ERM or older, traditional risk assessment processes, there is always a need to identify and understand the various risks facing an organization, to assess those risks in terms of their cost or impact and probability, to develop responses in the event of a risk occurrence, and to develop documentation procedures to describe what happened as well as corrective actions going forward.

This risk management process should be enterprise-wide, involving people at all levels and in all organization units. While a larger enterprise may want to organize a specialized team of risk management professionals, as discussed in Chapter 5 on implementing an effective ERM program, smaller enterprises should also designate people to be responsible for managing their organization-wide risk assessment process. Whether a formal risk management function or a designated manager, enterprise risk management should involve a wide range of people. A financial executive will have a different perspective on certain information systems–related risks than would the chief information officer (CIO) or a member of the information technology (IT) operations staff. Each sees and looks at risks from different perspectives. This same analogy is true for all aspects of the enterprise.

This four-step risk management process should be implemented at all levels of the enterprise and with the participation of many different people. Whether a smaller organization with few facilities within a limited geographic area or a large enterprise, common risk management approaches should be developed.

This is particularly important for the worldwide organizations so common today. They may have multiple operating units engaged in different business operations and facilities in different countries. Some risks in one unit may directly impact or be related to risks in another, but other risk considerations may be effectively independent from the whole. These common risks can occur because of a wide variety of circumstances ranging from poor financial decisions to changes in consumer tastes to new government regulations.

Risk Identification

Management should endeavor to identify all possible risks that may impact the success of the enterprise, ranging from the larger or more significant risks to the overall business down to the less major risks associated with individual projects or smaller business units. The risk identification process requires a studied, deliberate approach to looking at potential risks in each area of operation and then identifying those more significant risk areas that may impact each operation in a reasonable time period. The idea is not to just list every possible risk but to identify risks that might impact operations, with some level of probability, within a reasonable time period. This can be a difficult exercise because we often do not know the probability of the risk's occurring or the nature of the consequences if the organization does have to face the risk.

This risk identification process should occur at multiple levels in an organization. A risk that impacts an individual business unit or project may not have that great an impact on the entire organization or beyond it. Conversely, a major risk that impacts the entire economy will flow down to the individual enterprise and its separate business units. Some major risks are infrequent but still can be so cataclysmic that it is difficult to identify them as a possible future event.

A good way to start the risk identification process is to begin with a high-level organization chart that lists the senior corporate-level facilities as well as the operating units. Each of those units may have facilities in many global locations and also may have multiple and different types of operations. Each separate facility will then have its own departments or functions, with some closely connected to one another, while others represent little more than corporate investments. A difficult and sometimes complicated task, an enterprise-wide initiative should be launched to identify all risks in various individual areas. This type of exercise can gain interesting and/or troubling results. For example, the corporate level may be aware of some product liability risks, but a front-line supervisor

in an operating unit may look at the same risks with an entirely different perspective.

Different members of the organization at different levels will look at some of the same risks from different viewpoints. A marketing manager may be concerned about competitor pricing strategies or the risk of pricing activities that would put the organization in violation of restraint of trade laws. An IT manager may be concerned about the risk of a computer virus attack on application systems but will have little knowledge of those same pricing issue risks. More senior management typically will be aware of a different level and set of risks than would be on the minds of the operations-oriented staff. Still, all of these risks should at least be identified and considered on an operating unit-by-unit basis and over the entire enterprise.

To be effective, this risk identification process requires much more than just sending out an e-mail to all operating units with a request to list the key risks in their operating units. This type of request will typically result in a wide range of inconsistent answers with no common approach. A better approach is to identify people at all levels of the organization, who would be asked to serve as risk assessors. Within each significant operating unit, key people should be identified from operations, finance/accounting, IT, and unit management. Their goal would be to identify and then help assess risks in their individual units built around a risk identification model framework. This is the type of initiative that can be led by an enterprise risk management group, if one exists, or a function such as internal audit.

The idea here is to outline some high-level "straw man" risks that may impact various operating units. By straw man, we mean a hypothetical structure that can either be built and enhanced further or can be easily torn down. Knowledgeable people can then look at these lists and expand or modify them as appropriate. Exhibit 2.1 shows such a business risk model framework. It lists major risk areas that may impact the enterprise, such as strategic, operations, and finance risks. This is the type of high-level list that a chief executive officer (CEO) might use to jot down to help respond to a stockholder or journalist question, "What worries you at the end of the day?" Certainly not listing all risks facing the organization; this is the type of first-pass list that an enterprise can use to get started on a detailed identification of its risks. The people responsible in the enterprise—often designated as the enterprise risk management (ERM) team—can meet with senior management and ask some of these "What worries you … " types of questions to identify such high-level risks.

STRATEGIC RISKS

External Factor Risks

- Industry risk
- Economy risk
- Competitor risk
- Legal and regulatory change risk
- Customer needs and wants risk

Internal Factor Risks

- Reputation risk
- Strategic focus risk
- Parent company support risk
- Patenttrademark protection risk

OPERATIONS RISKS

Process Risks

- Supply-chain risk
- Customer satisfaction risk
- Cycle-time risk
- Process execution risk

Compliance Risks

- Environmental risk
- Regulatory risk
- Policy and procedures risk
- Litigation risk

People Risks

- Human resources risk
- Employee turnover risk
- Performance incentive risk
- Training risk

FINANCE RISKS

Treasury Risks

- Interest rate risk
- Foreign exchange risk
- Capital availability risk

Credit Risks

- Capacity risk
- Collateral risk
- Concentration risk
- Default risk
- Settlement risk

Trading Risks

- Commodity price risk
- Duration risk
- Measurement risk

INFORMATION RISKS

Financial Risks

- Accounting standards risk
- Budgeting risk
- Financial reporting risk
- Taxation risk
- Regulatory reporting risk

Operational Risks

- Pricing risk
- Performance measurement risk
- Employee safety risk

Technological Risks

- Information access risk
- Business continuity risk
- Availability risk
- Infrastructure risk

Exhibit 2.1 Business Risk Model Sample

This very general, high-level risk model can serve as a basis to better define the specific risks facing various units of an enterprise. For example, the model lists business continuity risks under technological risks. An IT manager should be able to expand this to a long list of detailed technology-related risks associated with business continuity. An operations manager who is the user of IT resources might look at business continuity risk from a different perspective and introduce other new risks associated with what happens to production operations if IT services are not available. In order to have a better understanding of the risks facing an organization, it is often best to expand these lists to establish a more complete set of risks.

An effective technique to quickly identify risks without a lot of detailed research is to assemble selected teams from the organization to engage in brainstorming sessions to better identify all associated risks. The brainstorming idea is to bring together teams from various levels or units in the organization with a challenge for them to name potential risks in a quick response type of format. The suggestion here is not for the ERM team to assemble an organization-wide meeting, flying in people for a risk identification meeting. Rather, a limited number of these sessions should be convened for selected, higher-profile organization groups. The results of their work can be used as a basis for other units to identify their own area risks, as discussed.

Brainstorming Approaches. This technique is a rapid-response group exercise in which knowledgeable people are asked to state the first things that come to mind in response to a general idea. A moderator might ask a small group, "What is our greatest finance-related risk?" and point to each group member to throw out his or her thoughts, with successive responses building on one after another. This is not a detailed analysis and discussion exercise, but each person's quick thoughts or comments are used to build on the others.

Sessions are usually led by a moderator, who uses a whiteboard or easel chart to ask participants to think of their impressions or thoughts for a topic. An example would be to ask participants what they felt were the greatest risks associated with their organization's IT continuity planning. In a hopefully nonconfrontational manner, participants would offer their thoughts and concerns—usually just a few words—for the moderator to record on the board and for others to use. People from IT might have a variety of more technology-oriented risk-related concerns, while people from finance or shipping might have other perspective. This is a quick-response type of approach wherein people from various units are asked to relate some first things that come to mind regarding risks in the area

discussed. Then, through a quick review of these possible risks in some area, and with member voting, this list of risks can be reduced to a more reasonable level.

Brainstorming is often a good approach to get a group with different backgrounds to focus on some subject. There is no real detailed analysis here, just the opinions of various experts in the area reviewed. Exhibit 2.2 outlines this brainstorming approach as well as voting approach to reduce the list.

Starting with a business risk model that was expanded through brainstorming sessions, a unit of the enterprise should have a good understanding of some of the high-level risks facing it. Next, there is a need to take this list and dig a bit deeper to understand the characteristics of these identified risks. In addition, such a list needs to be better expanded throughout the organization. The ERM team should analyze each of these brainstorm session–identified risks in a bit more detail, asking such questions as:

- Is the risk common across the overall enterprise or is it unique to one business group?
- Will the organization face this risk because of internal events within the company or through external events?
- Are the risks related? That is, will one risk cause another to occur?

This discussion can be expanded. The idea is to gain a strong understanding of the nature of risks that were identified in the brainstorming sessions and then to highlight those risks that can be considered core risks. These identified risks can also be called major risks and include such topics as the risk of a significant fall in customer satisfaction ratings, the risk of a new and very large competitor entering the market, or the risk of an identified significant control weakness as part of the financial statement close. Any of these core risks could present significant challenges to the enterprise. Another example is the risk that external auditors would report one or more significant control weaknesses that could draw regulatory attention, might force a significant drop in the stock price, and would distract organization resources from other, more core tasks as they correct the weakness.

The ERM team should review all of the risks identified from the group brainstorming session that were subsequently designated as core risks. Because of the ongoing discussion and analysis associated with this process, there may have been some changes to the original set of risks as identified. This final set of identified organization risks by the overall enterprise and by specific operating units should be shared with responsible operating and financial management, as well as with the teams that participated in the

Using the Exhibit 2.1 business risk model, teams should be assembled to identify specific risks that may impact each of the designated areas. The idea is to engage in an open discussion and then brainstorm to identify a list of possible risks for the overall enterprise or for a local business unit. With various parties contributing their own ideas, the initial list may include a wide range of possible risks. Then, the team should reduce this list to the "top ten" risks in each area by using the multivoting techniques discussed below.

The Brainstorming Approach:

Use a blackboard/whiteboard or easel with chart paper and appoint a scribe to enter the work. The scribe may also act as the leader, if desired. Everyone should be able to see the easel at once.

1. The leader sets up the session by asking questions based on the Business Risk Model. For example, "What are the compliance risks facing our business operations?" It is best to write the question on the easel.
2. The leader should set the time limits for group inputs for each area (five to ten minutes is usually more than enough).
3. The leader explains the rules of participation:
   - **(a)** Each person can contribute as much as he or she wants, but quick, "top of the head" thoughts often work best.
   - **(b)** No comments, criticisms, or judgments are allowed during the storming phase.
   - **(c)** It is okay to build on others' ideas (it is actually encouraged).
   - **(d)** The storming phase is over at the time limit or when all ideas have been exhausted for each of the risk area topics.
4. At the "go" signal, each person in the team begins by suggesting possible risks in the given area. The scribe must capture each suggested risk as given without editing (abbreviation is okay). The scribe may enforce some order if he or she has trouble capturing the suggestions (one at a time, raise hands, etc.—most sessions don't need these).
5. When all suggested risks in an area have been offered or the time has expired, the leader may attempt to consolidate similar suggestions (with permission of the group) for ease in later selection or prioritization.

It may be necessary to have multiple groups handling different risk areas. A different team may want to identify IT-related risks than another team looking at financial reporting risks. Each session may result in a long list of potential risks, and after each brainstorming session, the group should use multivoting to narrow down the list to ten identified risks in the area.

Multivoting is an approach to take a list of *n* items and quickly narrow the list to what is most important to the group through one or more voting rounds. Even lists of 50 or 60 items can be narrowed to a half dozen by three or four rounds of multivoting.

EXHIBIT 2.2 RISK IDENTIFICATION BRAINSTORMING APPROACHES

1. The leader/scribe displays the full list of *n* items (for example, 50) to everyone in the group. Each team member will be given a ballot list of these selected *n* items.
2. Each person will receive multiple votes (rounded to the next lowest whole number).

$$\text{VOTES} = \text{V} = \frac{n}{2} + 1$$

In this example of 50 items, each person has 26 votes and can 1 up to a maximum of 26 votes to any remaining item.

3. Each person in the group scans the list and decides how to allocate that person's assigned number of votes.
4. The leader will go through the items one at a time and either collect ballots or, if a small number of items and votes, ask for a show of hands. The votes are recorded for each item as cast.
5. Eliminate any item not receiving support from at least 25% of the votes cast. With less than 25% support, the item should be dropped from the list.
6. Repeat the process until the group is satisfied that the list is small enough to deal with effectively (usually three to seven items, or whenever the goal is reached).

EXHIBIT 2.2 RISK IDENTIFICATION BRAINSTORMING APPROACHES *(CONTINUED)*

brainstorming sessions. Any corrections should be made, as appropriate, prior to assessing the risks.

The results of the risk identification brainstorming sessions should then be shared with other units that did not have the opportunity to participate in the original sessions. The results of the identified risks should be expanded for comment and discussion throughout the organization. The potential risks that were developed by a marketing group in Thailand, for example, could be shared with a team who did not participate in these sessions, such as a similar group in Singapore. They would be asked, "These risks were identified by team members in Thailand. Do you agree, disagree, or wish to add others?"

Using brainstorming sessions, management surveys, or other approaches, a first step to ERM or any risk management process is to identify the population of risks that are threatening an enterprise, both at an individual unit level and on a total corporate basis. These will not become the key or core risks but are a starting point for risk assessments as discussed below.

Key Risk Assessments

Having identified the significant risks impacting the enterprise at various levels, a next step is to assess them for their likelihood and relative significance.

This is particularly important for risks identified through quick-response brainstorming techniques. What sounded good in a quick-response group session may not appear as serious when reduced to a relative significance type of analysis. A variety of approaches can be used here, ranging from a relatively quick best-guess qualitative approach to some detailed, very mathematical quantitative approaches. The whole idea here is to help management better decide which of a series of potentially risk event occurrences should give enterprise management the most to worry about.

A simple but often effective approach here is to take the list of identified risks and circulate it back to all brainstorm session participants or others with a questionnaire asking for each risk:

- What is the likelihood of this risk's occurring over the next one-year period? Using a score of 1 to 9, assign a best-guess single-digit score as follows:
  - Score 1 if you see almost no chance of that risk's happening during the period.
  - Score 9 if you feel the event will almost certainly happen during the period.
  - Score 2 through 8 depending on how you feel the likelihood falls between these two ranges.
- What is the significance of the risk, in terms of cost to the organization? Again using a 1-to-9 scale, scoring ranges should be set depending on the financial significance of the risk to the organization. A risk whose costs could lower organization earnings per share by perhaps one cent might qualify for the maximum score of 9.

Questionnaires for this simplified approach should be independently circulated to knowledgeable people to rate or score each of the identified risks per these two measures. As an example, assume that an enterprise has identified six risks, R-1 through R-6. For each of these risks, a team of four people is asked to separately evaluate each risk in terms of likelihood and significance. These scores are then averaged by both factors and are plotted on a risk assessment analysis chart as shown in Exhibit 2.3. R-1 had an average likelihood score of about 3.75 and a significance score of 7.00, and this score is plotted in quadrant I of the exhibit. This shows R-1's level of risk as relatively significant but not that likely to occur.

All of the identified risks should be plotted in this manner. The high likelihood and more significant risks that end up in quadrant II should receive immediate management attention. The ranges here of 1 to 9 are arbitrary;

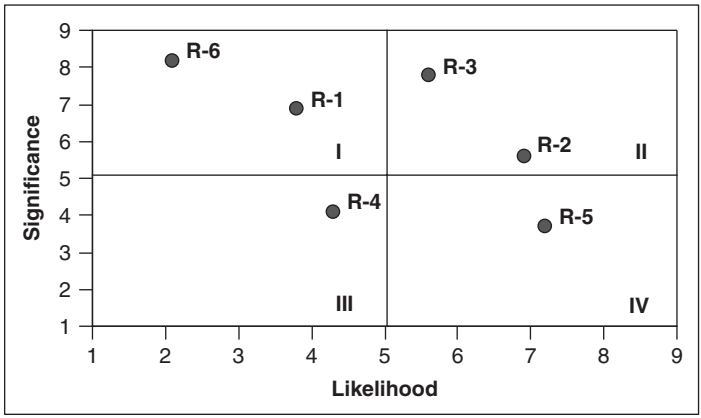

EXHIBIT 2.3 RISK ASSESSMENT ANALYSIS CHART

the enterprise should set some relative guidelines, but staff members should rate matters in terms of how they view the relative likelihood and significance of the identified risks. This risk assessment analysis chart provides a good qualitative measure to understand significant risks surrounding an enterprise.

The high-risk assessment process just described works well when an enterprise has identified a relatively small number of risks. It is fairly easy to look at a risk assessment analysis chart, similar to Exhibit 2.3, and to focus on the high likelihood and significant risks in the upper-right-hand quadrant II and remediation planning for those risks. Often, however, an enterprise has identified a much larger set of identified risks, and ranges of 1 to 9 as well as plots on the chart will not provide sufficient detail. A better approach is to express these significance and impact estimates in terms of a two-digit number representing the percentage estimate (e.g., 72 percent) of achieving some risk or as a probability (e.g., 0.72).

Increasing the number of digits from just a 7 to full 72 percent does not increase the accuracy of the assessment, but it does suggest that the ERM team and the assessment group should devote more attention to accurate estimates. It also helps assessment teams to better understand the relationship between probabilities covering independent and related events.

Probability and Uncertainty. Particularly when a large number of risks have been identified, the assessment teams should think of the individual risks, likelihoods, and occurrences in terms of two-digit probabilities

ranging from almost 0.00 to 0.99. Again, risks essentially never have a zero chance or a 100 percent chance of occurring. Another basic rule of probability is that we cannot add up independent probability estimates to yield a joint estimate. If the probability of risk A's occurring is 60 percent and the probability of risk B's occurring is also 60 percent, we cannot say that the probability of both occurring is 0.60 + 0.60 = 1.20. This 120 percent does not make sense!

The joint probability of two independent events is the product of the two separate probabilities. That is:

$$\Pr(\text{Event 1}) \times \Pr(\text{Event 2}) = \Pr(\text{Both Events})$$

That is, if Event 1 is 0.60 and Event 2 also 0.60, the combined probability of both events occurring is $(0.60) \times (0.60) = 0.36$.

In terms of the assessments, this says that if a risk has a 60 percent significance estimate or that we are 60 percent certain that the risk will occur, and if the impact has been rated at 60 percent, there is a 36 percent probability that we will incur both of those risks. We can also call this the risk score for the individual risk.

An accurate risk assessment process, however, requires more than just "top-of-the-head" estimates, whether stated in a single 1-to-9 range or as a full, two-digit percentage. The ERM team and other interested persons should take a hard look at the risks that were identified during risk identification brainstorming and should gather more information, if required. For example, during the risk identification process, one manager may have identified the consequences of the enactment of a new tariff law as a serious risk. Others in that same brainstorming session may have expanded on that supposed upcoming law as a significant risk. However, before risk-ranking it in terms of significance and impact, the ERM team or other responsible managers may want to do a bit more research to determine the actual consequences. It may be something that is not at all applicable to the unit in question or that does not go into effect until some years into the future. The point here is that all identified risks may need some additional information before they can be accurately assessed.

When estimating occurrences and likelihoods, the ERM team should take care to ensure that all estimates are made over the same period of time. Usually, a one-year interval or at least until the end of the next fiscal year is a reasonable interval of time. There is typically not enough information to make estimates much beyond those periods.

Risk Interdependencies. We have discussed risks at an individual organizational unit level, but risk interdependencies must always be considered. Exhibit 2.4 shows a simple organizational arrangement with Activities A, B, C, and D all operating in parallel and reporting to activity or unit G and then to unit I and ending with unit J. One can think of this as separate operating entities in an overall enterprise or as operating departments with a single plant or facility. In an ERM sense, risks should be identified and assessed at each of these levels. Each of the A, B, C, and D risks would often be independent of each other, although some would often be common. That is, each of these units may share the same risks but with potentially different likelihoods and significances. However, operating department G must consider the impact of the separate risks at each of these units. These separate risks will impact J, but that unit must evaluate the nature of those individual unit risks.

The concern here is that risk interdependencies must be considered and evaluated throughout the organizational structure. Any entity should be

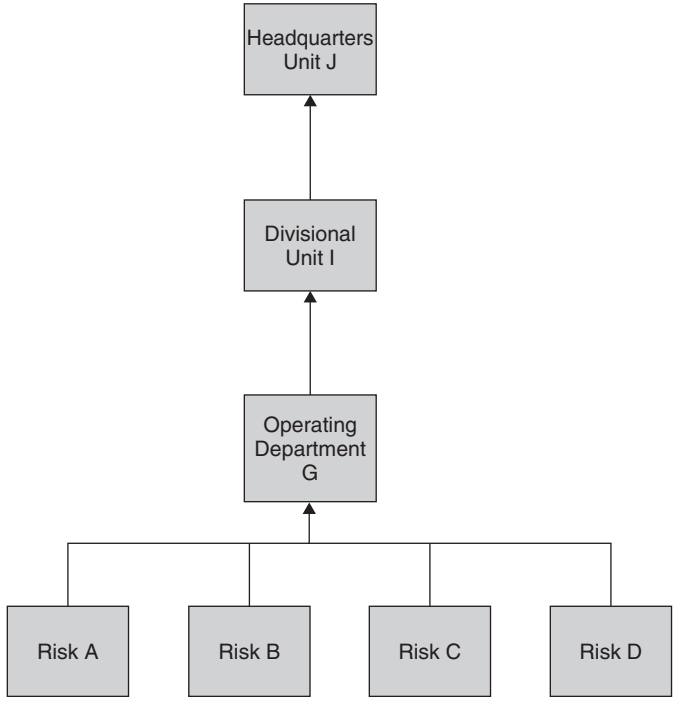

EXHIBIT 2.4 RISK INTERDEPENDENCY HIERARCHY

concerned about risks at all levels of the organization but only really has control over the risks within its own sphere. The 2002 fall of the public accounting firm Arthur Andersen in the wake of the Enron collapse would be an example of considering risks by entity and for the overall enterprise. Each city-by-city and country-by-country unit of that then much esteemed public accounting firm had its own risk assessment procedures, following firmwide standards. However, a risk event at one of their operating offices, Houston, and perhaps at the national practice legal affairs department, caused the whole firm to collapse. An operating office in another area, such as Toronto, might not have even fully anticipated such risks in faraway Houston. The point is that risks are often very interdependent within an enterprise. Each operating unit is responsible for managing its own risks but may be subject to the consequences of risk events on units above or below each in the organizational structure. Every operating unit of an enterprise should realize that whatever risks that local unit is accepting may impact other units in the organization.

Risk Ranking. While the examples used in this chapter have had a relatively short list of identified risks, a typical enterprise that goes through a risk-ranking and assessment process will end up with a very long list of potential risks. A next step is to take the established significance and likelihood estimate, calculate risk rankings, and identify the most significant risks across the entity reviewed. Exhibit 2.5 is an example of this type of analysis. The likelihood and significance scores show where these risks would be plotted on a risk assessment analysis chart, as was shown in Exhibit 2.3, and the product of these two gives the relative risk ranking for them. Risks C and G have the highest risk rank scores and would be plotted in the upper-right-hand quadrant as the most significant risks in this sample. These two are often called the *risk drivers* or the primary risks for this set of identified risks. An organization should then focus its attention going forward on these types of primary risks.

These risk-ranked schedules should be organized on a unit-by-unit basis and adjusted to accommodate all related risks in parallel with as well as above and below the entity being ranked or evaluated. An entity, A, may face a risk that a drop in its production quality will lower its unit's sales and profitability. Another parallel unit, B, has its own production quality risks but may lose business in its operations because of A's production problems. The headquarters unit, C, will be subject to the production quality risks at its subsidiary units. C needs to recognize and identify those unit A and B

Identified Risk	Significance Probability (P)	Likelihood Probability (L)	Risk Score (P × L)	Rank
A	0.55	0.30	0.17	8
B	0.88	0.24	0.21	7
C	0.79	0.66	0.52	1
D	0.77	0.45	0.35	4
E	0.35	0.88	0.31	5
F	0.54	0.49	0.26	6
G	0.62	0.72	0.45	2
H	0.66	0.20	0.13	9
I	0.90	0.45	0.41	3
J	0.12	0.88	0.11	10

EXHIBIT 2.5 RISK-RANKING CHART EXAMPLE

risks, but the simple probability rules just discussed are often much more complex. In addition, adverse publicity or other factors may take what was viewed as a low-significance risk at a subsidiary unit and magnify this significance as the risk event is elevated.

There are no simple answers or solutions here. The ERM team should identify these unit by unit to make certain that risks at all levels have been assessed and the likelihood and significance estimates are appropriate throughout the organization. All too often, risk events that occur far away from corporate headquarters and in distant locations can cause major problems to an organization. An example can be drawn from a risk event at the once major U.S. corporation Union Carbide many years ago. On the night of December 2, 1984, over 40 tons of poisonous gases leaked from a pesticide factory in Bhopal, India, belonging to Union Carbide, killing more than 20,000 residents.[1] After much corrective action and legal wrangling, Union Carbide, which built the plant in 1969, settled a civil suit brought by the Indian government in 1989 by agreeing to pay US$470 million for damages suffered by the half-million people who were exposed to the gas. The company maintained that the payment was made out of a sense of "moral" rather than "legal" responsibility since the plant was operated by a separate Indian subsidiary, Union Carbide India Limited (UCIL). Those court proceedings revealed that management's cost-cutting measures had effectively disabled safety procedures essential to prevent or alert employees of such disasters.

Dow Chemical has since taken over Union Carbide and denies responsibility for this disaster. However, because of the tremendous loss of life there and the fact that Dow Chemical is much larger than what was once Union Carbide and its UCIL subsidiary, ongoing litigation—even as this book goes to press—continues to haunt Dow Chemical.

The Bhopal gas leak is an example of how a risk event at a distant and relatively small unit can have disastrous consequences on a major corporation. While the risk identification and assessment rules outlined in this chapter would not have accounted for a catastrophe of this magnitude, the concept here is that each unit in the organization needs to recognize the likelihood and consequences of risks at each individual unit level. A risk event at a small foreign subsidiary can bring down the entire enterprise. Risk management at all levels should now recognize that catastrophes can happen. We can never predict risks of this major consequence, but an enterprise should always be aware that disasters can happen.

Quantitative Risk Analysis

Expected Values and Response Planning. There is little value in publishing detailed lists of significant risks unless the enterprise or organization has at least made some preliminary plans for the action steps necessary if they incur one of the risks. The idea is to estimate the cost impact of incurring some identified risk and then to apply that cost to a risk factor probability to derive an expected value of the risk. This is also an important time to identify a risk owner, the person or entity responsible for recognizing and monitoring the status of a specific risk. This is often an exercise that does not require detailed cost studies with lots of supporting historical trends and estimates. In the example used previously, risks were identified through a rapid-response brainstorming approach but without any detailed analysis or likelihood and significance estimates. These should be made by knowledgeable people with a general understanding of the risk areas. Expected cost estimates should also be performed by front-line involved people at various levels of the enterprise who would be expected to have a good level of knowledge of the area or risk implications.

The idea is to go through each of the identified risks—or, if time is limited, only the key risks—and estimate the costs of incurring the risk. Because the kinds of risks discussed involve such matters as the failure of a hardware component, the drop in a market share, or the impact of a new government regulation, these are typically not the types of costs that one can just look up in a current vendor's catalog. Some hypothetical risks,

labeled here as A, B, and C, and the ways to think about replacement costs might include this type of thinking:

- *Risk A.* Loss of up to x percent market share due to changing consumer tastes.
  - What will be the reduction in sales and loss of profits due to the x percent drop?
  - How much will it cost to begin to restore the lost market position?
- *Risk B.* Temporary loss of major Florida-based manufacturing facility for up to x days due to hurricane.
  - What are best- and worst-case estimates to get the plant temporarily repaired and back in operation within x days?
  - What will be the extra labor and material production costs incurred during the interim?
- *Risk C.* Loss of total information system for two days due to pernicious computer system virus.
  - How much business and profitability will be lost during the down period?
  - What will be the cost to transfer operations to the business continuity site over the period?

These questions are certainly not precise but illustrate the type of thinking needed to estimate the costs of recovering from some disaster event. It is often easy to identify some risk event but often much more difficult to determine what it would cost to recover from that event. As suggested throughout this chapter, there often is no need to perform detailed, time-consuming analyses here but to ask knowledgeable people who understand the risk area to give some estimates. Teams at the entities that could incur these identified risks should make their cost estimates on the basis of:

> What is the best-case cost estimate if it is necessary to incur the risk? This is an assumption that there will be only limited impact if the risk occurs.
>
> What would a sample of knowledgeable people estimate for the cost? For Risk A as outlined above, the director of marketing might be asked to supply an estimate.
>
> What is the expected value or cost of incurring the risk? This is the type of risk that might include some base costs as well as such other factors as additional labor requirements.
>
> What is the worst-case cost of incurring the risk? This is a "what if everything goes wrong" type of estimate.

The ERM or risk assessment team should work with other people in the organization to develop these risk estimates. We have suggested using four estimates as a starting point to get some idea of the ranges of costs in various people's thinking. However, one best-guess estimate should be selected from the four estimates—usually something between estimates 2 and 3. These estimates and supporting work should be documented, and the selected cost estimate entered as the cost impact on the Exhibit 2.6 risk-ranking response-planning example. These are the same risks that were identified in the Exhibit 2.5 example, but here are ordered by risk rank. This reordering is important when an enterprise has a long list of identified risks.

The "expected value of cost" cells are just the products of the cost impacts and risk scores. These estimates predict what it will cost an organization to incur some risk. Although the numbers selected for these samples are very arbitrary, they show how managers or an ERM specialist can interpret or act on this type of analysis.

Risk C, for example, has a high likelihood and significance as well as a fairly high expected cost to correct. This is the type of risk that management should identify as a candidate for corrective actions. However, the next risk on the schedule, Risk G, also belongs in the upper-right-hand quadrant but with a relatively high cost to implement. This may be the type of risk wherein management decides to accept the risk or to develop some other form of remediation plan, as discussed below.

Risk H is another risk with a high cost to implement. Here, the significance of the risk is fairly high but the likelihood of occurrence quite low. These are the kinds of numbers where management will frequently decide to "hope for the best" and live with the risk. For this risk, it will be expensive if management incurs the risk but also expensive to install preventive action facilities. Assuming the ERM team has done a good job in preparing these estimates of identified risks, this can be a useful approach for making ongoing risk remediation decisions.

Risk Monitoring. The identification of key risks can never be a single, one-time process. The environments surrounding a series of risks identified in a formal brainstorming or other process will soon change as the nature of these identified risks changes. For some, conditions may change such that the risk becomes an even greater threat. For example, the brainstorming team may have identified potential political risks in some less developed country. However, events can often happen quickly, and political changes in that same country can make those concerns even riskier. An enterprise needs a mechanism to monitor these identified risks.

Identified Risk	Significance Probability	Likelihood Probability	Risk Score (P × L)	Rankings	Cost Impact	Expected Value of Cost	Risk Response Planning?
C	0.79	0.66	0.52	1	$120,600	$62,881	Yes
G	0.62	0.72	0.45	2	$785,000	$350,424	No
I	0.90	0.45	0.41	3	$15,000	$6,075	Yes
D	0.77	0.45	0.35	4	$27,250	$9,442	Yes
E	0.35	0.88	0.31	5	$52,350	$16,124	Yes
F	0.54	0.49	0.26	6	$1,200	$318	Yes
B	0.88	0.24	0.21	7	$12,650	$2,672	Yes
A	0.55	0.30	0.17	8	$98,660	$16,279	Yes
H	0.66	0.20	0.13	9	$1,200,980	$158,529	No
J	0.12	0.88	0.11	10	$88,600	$9,356	Yes

EXHIBIT 2.6 RISK-RANKING RESPONSE-PLANNING EXAMPLE

Risk identification processes are not continuous exercises. Just as an organization will prepare an annual budget with revisions perhaps once per quarter, a risk identification process is often an annual or quarterly process. Once these risks have been identified, the enterprise needs to monitor them and make ongoing adjustments as needed. This risk monitoring can be performed by the process owner or an independent reviewer—often an enterprise risk management function or an internal auditor.

Risk Monitoring through Process Owner Follow-up

Often, the process owner or a member of the management team responsible for the risk area is the best resource to provide an ongoing status of the risk. These people should be surveyed on an ongoing basis to provide a current assessment on the likelihood of an identified risk. A process owner is often the best source to provide an unbiased assessment of the nature of the risk at a point in time. If there is a risk of an environmental problem unless certain plant repairs are installed, the process owner often provides the best assessment on the status of those repairs. It is only for certain types of risks that process owners may not provide a fully unbiased status. For example, if the risk is a loss of market share unless a new product initiative is launched, a process owner may be too close to the risk solution to give a fully unbiased follow-up assessment.

Risk Monitoring through Auditor Follow-up

An internal audit can often be a very credible and good source to monitor the current status of identified risks. Auditors may gather this information through surveys or face-to-face reviews. They always have the extra credibility and authority such that when "the auditors" ask about the status of some identified risk area, the people responsible for the area will probably provide some accurate information. If internal auditors are unable to get good information regarding the status of some identified risk, they can always schedule a visit to better understand the nature of the risk area. Of course, internal auditors have their own audit project scheduling and risk assessment issues; they typically cannot just schedule a review in a short time frame to understand the current status of some identified risk. However, if people in the organization know that auditors may sometimes pay a visit to better understand the status of some risk, there will be a strong tendency to provide some strong, accurate status answers.

Accurate monitoring processes are an essential component of risk management. An enterprise may have gone through an elaborate process to identify its more significant risks. However, the current status of those risks

must be monitored on a regular basis, with changes made to the identified risks as necessary.

OTHER RISK ASSESSMENT TECHNIQUES

With our descriptions of brainstorming, we have demonstrated a very informal and easy-to-use method for identifying risks and making some probability estimates. Some managers, however, may object to the quick-response informality of these methods and seek more formal, qualitative processes. In this section, we introduce three other, more qualitative risk analysis and decision techniques: the Delphi method, Monte Carlo simulation, and decision tree analysis. We present a high-level overview of each. Our objective is not to be a primer on probability-based mathematics but to introduce some of the other popular but more mathematically precise risk assessment methods.

The previously described brainstorming method for identifying organization risks is easy to use but can sometimes send a team off in the wrong direction. Brainstorming assumes that all members of the team on the project have about the same level of influence and interest in a subject area. Each should contribute in an open discussion by throwing out individual ideas based on their and other contributed thoughts. Sometimes, however, one or several more powerful personalities can derail a brainstorming session by pushing their personal agenda, whether right or wrong. A good moderator can get around such people, but sometimes it is better to make risk-based decisions through a more thorough and research-oriented approach. While brainstorming and other informal approaches give quick and generally accurate information, some of the methods described here are much more thorough but also more defensible when questions arise.

Delphi Method

The approach, or at least the name, of this decision process goes back to the ancient Greeks of about 500 B.C. or earlier. A temple had been established at the Greek city of Delphi and populated with a group of priestesses, called the oracles. They responded to people's questions and provided answers in a high-level, almost sacred sense. For a thousand years of recorded history, the Greeks and other peoples came to Delphi to consult these oracles, whose words were taken to reveal the rules of the gods. The temple of Delphi was a center of knowledge in the ancient Greek world, and an important center for worldwide decision making.

Although Delphic oracles went away millenniums ago, a similar decision-making predictive approach, called the Delphi method, was developed

in the 1950s by the RAND Corporation of Santa Monica, California. The idea of the ancient Delphi approach was that questions were submitted to an oracle behind a closed screen. After some time for thought and deliberation, an answer was delivered by an unknown party who represented the oracle behind the closed screen. In the more modern RAND approach, decisions did not come from a priestess oracle but came from the results of multiple rounds of collaborative participant surveys. Multiple participants are asked to fill out a survey or questionnaire. The results are summarized, and participants are given the results of the first round and asked to alter their opinions in second or subsequent rounds based on earlier consensus opinions. In each round, they can alter their original assessments if they want to—or stick to their previous opinion. Brainstorming sessions, as discussed previously, are often strong sessions in group dynamics where one or another person in these sessions can dominate things through strong personal opinions. The Delphi method is similar to filling out rounds of opinion surveys. Nobody "loses face" because the survey is done anonymously using questionnaires.

For the risk identification process described earlier, the Delphi method would take the place of the brainstorming session described earlier as follows:

- The ERM team or another group, such as internal audit, would be designated as the "oracles" to administer the assessment process.
- A group of managers would be selected to identify appropriate risks.
- After a briefing of the project's objectives, each selected team member would be asked to identify key risks in the area of interest. People would independently describe their opinions of these risks on forms sent to the ERM "oracles."
- The ERM "oracles" would then review these survey results, find common threads, and develop a second-round survey questionnaire, listing what appear to be the major risk areas of concern.
- The original survey participants would receive this updated list and would be asked to agree, disagree, or to propose modifications. These results would go back to the ERM "oracles."
- These second-round results might again be modified to create a third round. Often, however, a consensus opinion can be reached after only two rounds.

This process of sending a survey to an anonymous coordinator with everyone working independently can often work quite well. No individual completing a survey knows who else is specifically sending in survey

results. Done correctly, every survey respondent's opinion is as valuable and important as all others.

The Delphi method is especially useful for longer-range risk identification forecasting, as expert opinions are the only source of information available. A major negative with the Delphi method is that it can be a fairly time-consuming process. Individuals are asked to list what they feel are the major risks in their area. After submitting these to the ERM team—the oracle—the individuals will get the results back with a summary of what everyone thought were the major risks, along with a request for more information. They now have a chance to review what others think about the same risk area and, based on these inputs, can alter their opinions. Done properly, no participant knows the source of the other opinions, and results can become very collaborative. The process usually goes through two or three rounds in order to establish the key risks in an area.

The Delphi method was particularly a very time-consuming process in the days of paper and pencils. Things usually go much faster in today's era of the Internet and e-mail. A team can assess risk identification inputs and quickly summarize these first responses to ask for opinions and updates. With the ongoing back and forth of e-mail exchanges, the central ERM team acting as the oracle can summarize responses and publish final summarized results. While certainly not the easiest process to administer, the approach develops consensus opinions of complex risk issues rapidly. It is a good tool to be added to the risk manager's toolbox!

Monte Carlo Simulation

While the description of the Delphi method references the ancient Greeks of 500 B.C. or earlier, Monte Carlo simulation refers to a more recent past era. Before today's era of pervasive government lotteries and other sanctioned gambling, much of this activity took place in a few large, formal gambling casinos. While U.S. citizens may think of Las Vegas, Nevada, as the center of all of this, the grand Monte Carlo casino in Monaco once represented gambling to many for generations. Because risks are always uncertain, in terms of their outcome and probability, Monte Carlo simulation is a technique used for understanding and evaluating uncertain risks.

The whole Monte Carlo simulation idea is to go beyond the very general high, medium, or low estimates that are often used in risk estimation to develop some better measures. Using a chance based assessment, the manager can apply probability rules to gain a better understanding of a set of identified risks.

We had previously suggested that each identified risk should be assessed in terms of its likelihood and potential impact, where a manager should focus attention on high-likelihood and high-impact risks. It is relatively easy to go through this analysis, as there are a relatively small number of identified risks. There is a much greater challenge when a large number of these risks have been identified. For example, consider an organization that has gone through a detailed risk assessment where perhaps 500 risks were identified, with 150 of those same risks estimated as having the same high likelihood of occurrence. Since we cannot take all 150 as the first group to address, a tighter and more precise measurement is needed. In addition, not all members of the team that helped to assess each of those high-likelihood risks will rate it in quite the same range.

Using a series of people familiar with the identified risks, each should be asked to estimate a series of factors surrounding the risk, such as the probability of the risk's occurring or the amount of expected loss, if that is the nature of the risk. Assume that an organization faces a risk of warranty returns over a given year. While it is possible that they may have zero returns in a given period, even the most optimistic of managers knows that there will be some minimal or optimistic number of warranty returns. On the other side of things, every product sold could have been returned for warranty, but a more reasonable but pessimistic view will give an estimate here as well. In addition, seasoned managers can rely on past statistics to predict the total estimated value for returns.

These three values can be plotted in a simple triangular chart, as shown in Exhibit 2.7. Because this warranty return process, as described in this example, occurs on a continuous basis, there would not be just one triangular chart to describe the risk but more of a bell jar distribution over time, as shown in the probability distribution in the lower portion of the exhibit. In this example, we have enough information to develop some high- and low-range distribution values, and specialized desktop software is available to develop a distribution estimate.

The whole idea of Monte Carlo simulation is to build a series of models describing various identified risks and to assess those risks using a computer simulation. Looking at each probability distribution, the multiple risks and potential outcomes can be combined to develop a series of best- and worst-case estimates. We have mentioned the difficulty of assessing the 150 high-risk areas out of 500 identified risks that an organization may face. A simulation model will look at the various combinations of risks and develop some joint probability estimates for all of the multiple combinations. We know that clearly not every one of the individual 150 identified

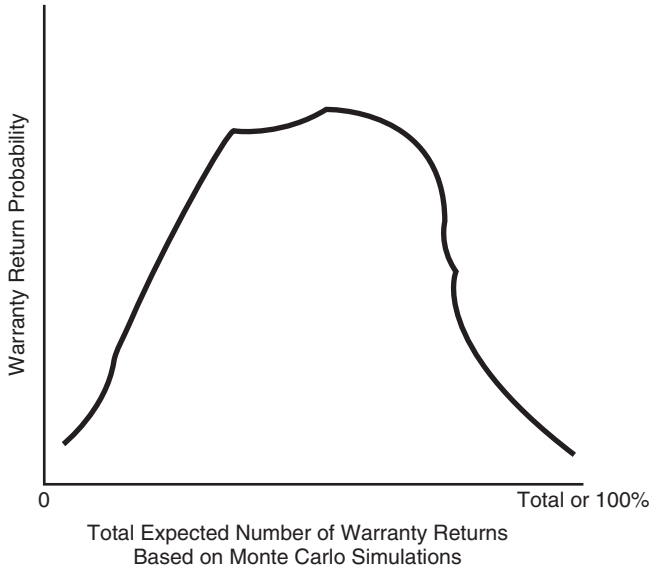

EXHIBIT 2.7 MONTE CARLO SIMULATION EXAMPLE

high risks will end up in a worst-case situation, nor can we take the most optimistic view for all of them at some single point in time. A detailed analysis using Monte Carlo techniques will allow a risk manager to make some better combined probabilistic estimates of the multiple risks that may face an enterprise.

This is not a technique where an individual with limited mathematical skills can go to the local bookstore and pick up a copy of a "Monte Carlo Estimation Techniques for Dummies"-type book, if such a publication exists. Expert help would be needed. However, our point here is that there are some rather sophisticated techniques available to help assess the impacts of multiple risks. Even with our hypothetical example of 150 out of 500 identified high risks, all of this will be of little value if one or another significant risk has been missed in one of the risk identification processes.

Decision Tree Analysis

The probability and impact of various combinations of multiple risks occurring is often a major concern. Decision tree analysis is a simple, and often graphical, technique to connect multiple risk combinations to come up with some estimates of the outcomes. A technique that historically was used in project planning critical path charts, it can be an effective technique for looking at probabilities covering a limited set of risks. The process is

particularly useful for looking at related risks. That is, we may have one risk that may or may not occur, but there will be related risks with their own likelihood probabilities. Using decision tree analysis and the rules of joint probability, we can assess the likelihood of multiple risk events.

The real strength of the decision tree graphical approach is to illustrate the impact that certain risks may have on subsequent risk-based matters. A risk event at a small unit may have an impact on other elements of operations when all of these risks are strung together. It can be a useful risk analysis tool.

RISK MANAGEMENT FUNDAMENTALS GOING FORWARD

This chapter has described a few of the classic and fundamental concepts associated with risk management. There are many other approaches, such as decision theory or Bayesian probability analysis, that can be useful but are beyond the scope of this book. The typical manager should not need a graduate degree in probability or mathematics to understand risk assessment or analysis.[2]

The cut-down and simplified tools and techniques described in this chapter will also be referenced in other chapters. Things like identifying potential risks and then estimating their probability of occurrence are the same, whether using classic traditional risk assessment approaches or the enterprise-wide scope of COSO ERM. These new risk management approaches will not change the manner in which we look at individual risk assessment techniques but how we should consider the big picture view of risks facing an enterprise.

NOTES

1. "Bhopal faces risk of poisoning," November 14, 2004, http://news.bbc.co.uk/2/hi/south_asia/4010511.stm. *Note:* This is one of many Web references on this issue. A search for *Bhopal, India,* and *Dow Chemical* will yield a large amount of information.
2. For a very good, but mathematically challenging technical book on the topic, see David Vose, *Risk Analysis: A Quantitative Guide,* 2nd ed. New York: John Wiley & Sons, 2000.

3

COMPONENTS OF COSO ERM

Chapter 1 discussed some of the developments that have led to concerns about the need for a definition of internal control and then to the Committee of Sponsoring Organizations' enterprise risk management (COSO ERM) framework, and Chapter 2 introduced some classic risk management and measurement techniques that have been used by risk management professionals in many areas of operations, such as credit management, information technology (IT) systems development projects, and business continuity planning. This chapter will take these introductory developments and discuss the components or elements of the COSO ERM framework. As a three-dimensional model, COSO ERM looks very similar to the COSO internal controls framework discussed in Chapter 1 and consists of a series of key components as objectives and entity-based perspectives. Although all three dimensions are necessary to understand COSO ERM and how they should interact, this chapter will introduce two of the COSO ERM dimensions, while the third objective and entity components dimension of the framework will be discussed in Chapter 4. This COSO ERM framework will help all levels of managers to better understand and

assess risks from a total enterprise perspective rather than just by individual risk areas and concerns.

ERM DEFINITIONS AND OBJECTIVES: A PORTFOLIO VIEW OF RISK

Every organization, whether for-profit commercial, not-for-profit, or a governmental agency, exists to provide value for its stakeholders; these include the employees and stockholders for a commercial organization or voters for a governmental entity. That stakeholder value is created, preserved, or can be eroded through management decisions at all levels of the organization and in all activities. These activities may range from day-to-day regular operations to setting strategy for some future but uncertain endeavor. All of them are subject to uncertainties or risks. Whether it is the challenge caused by a new and aggressive competitor or the damage and loss of life caused by the 50-foot-plus tsunami redundant that hit the Southeast Pacific region beyond Indonesia in late 2004,[1] killing tens of thousands, we all face a wide range of risks. While it is essentially impossible to estimate the probability of a totally cataclysmic event such as that late 2004 tsunami, individuals and organizations balance the amount of risk that they are willing to accept against the potential and adjusted returns from accepting most risks. This is the risk versus risk-adjusted return trade-off, discussed in Chapter 2, where a manager attempts to operate in a position where there will be some risks but the returns will be at a maximum point given those risks. As the insurance industry has demonstrated, there are numerous good practices in place to assess risks and to anticipate both their potential occurrence and returns for accepting a given risk.

Organizations generally have two problems with this risk versus adjusted return decision model. First, there has not been a good and consistently accepted definition of risk across the overall organization, and second, we often do not think of risks in a total organization sense but only component by component. An example of this lack of definition can be found in many business environments today. This author once worked in an environment where persons requesting new software application development work had to complete an authorization form that contained a box for the requester to describe whether the risks associated with the proposed new system were high, medium, or low. Requesters, anxious to get the new systems or enhancement approved, consistently described these new systems risks as ‘‘low,’’ with no further management analysis. This type of assessment

would not even be questioned unless there was some type of massive failure. In most cases, the people asked to assess the level of risks associated with a new project typically did not have enough information to assess risks on the particular project and certainly not to make any kind of credible enterprise-wide assessment. To quote John Flaherty, the first and now past chairman of COSO, "Although a lot of people are talking about risk, there is no commonly accepted definition of *risk management* and no comprehensive framework outlining how the process should work, making risk communication among board members and management difficult and frustrating."[2] This was the same environment that faced the Treadway Commission in the early 1980s, discussed in Chapter 1, when they looked at internal control and its supporting definitions. The result was a general understanding of the lack of a consistent definition and the need for such a definition. The result was the COSO internal control framework.

A second risk-versus-return problem is that we often take a silo approach to our understanding of risks rather than considering them in terms of the total organization. *Silo approach* refers to the tall and narrow agricultural storage containers used on farms. Everything within a silo is secure and protected, but there is no interaction between one silo and another nearby. While this may be appropriate when each individual silo is used to store a separate commodity with no need for interaction, separate processes each stored in their own silos often need connections and interactions with other processes that may exist in other such silos. An organization may have a good risk management process for credit operations housed in the silo covering that area of operations as well as a good risk assessment process in the silo covering IT continuity planning, but there is often a need for these two processes to communicate and to use some common approaches. Risks should be considered on a total enterprise level.

As discussed in Chapter 1, COSO ERM is a framework that will help organizations to have a consistent definition of what is meant by their risks and to consider those risks across the entire organization in a consistent manner. The COSO organization launched ERM in a manner similar to the development of their internal control framework. An advisory council of members from the sponsoring organizations was formed, and PricewaterhouseCoopers (PwC) was contracted to develop and draft the framework description. A draft version of the ERM framework was released for comment in mid-2003, with the final version published in September 2004. The remainder of this chapter and Chapter 4 summarize COSO ERM in some detail. The reader also is encouraged to access the entire description of COSO ERM.[3]

Just as the COSO internal controls framework started by proposing a consistent definition of its subject, the ERM framework starts by defining enterprise risk management as follows:

> Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in a 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.

A rather almost academic sounding definition, an enterprise manager should perhaps just consider and remember the key points here rather than memorizing this definition in order to recite it at a staff meeting! Key points to always consider when using COSO ERM include:

- *ERM is a process.* An often misused expression, the dictionary definition of a process is a set of actions designed to achieve a result. However, this definition does not provide help for many professionals. The idea to remember is that a process is more than a static procedure, such as the use of an employee badge that is designed and built to allow only certain authorized persons to enter a locked facility. Such a badge procedure—like a key to a lock—only allows or does not allow someone entry to the facility. A process tends to be a more flexible arrangement. In a credit approval process, for example, acceptance rules are established with options to alter credit-granting rules when given other considerations. An organization might bend the credit rules for an otherwise good credit customer that is experiencing a short-term problem. ERM is that type of a process. An organization often cannot define its risk management rules through a small, tightly organized rule book. Rather, there should be a series of documented steps to review and evaluate potential risks and to take action based on a wide range of factors across the entire organization.
- *The ERM process is implemented by people in the organization.* ERM will not be effective if it is implemented only through a set of rules sent in to an operating unit from a distant corporate headquarters, where those corporate people who drafted the rules may have little understanding of the various decision factors surrounding them. The risk management process must be managed by people who are close enough to that risk situation to understand the various factors surrounding that risk, including its implications.

- *ERM is applied through the setting of strategies across the overall organization.* Every organization is constantly faced with alternative strategies regarding a vast range of potential future actions. Should the entity acquire another complementary business or just build internally? Should it adopt a new technology in its manufacturing processes or stick with the tried-and-true? An effective ERM should play a major role in helping to establish those alternative strategies. Since many organizations are large, with many varied operating units, ERM should be applied across that entire organization, using a portfolio type of approach that blends a mix of its high- and low-risk activities.
- *The concept of risk appetite must be considered.* A new concept or term for many managers, *risk appetite* is the amount of risk, on a broad level, that an organization and its individual managers are willing to accept in their pursuit of value. Risk appetite can be measured in a qualitative sense by looking at risks in such categories as high, medium, or low; alternatively, it can be defined in a qualitative manner. An understanding of risk appetite covers a wide variety of issues that will be discussed further as part of our discussions of implementing ERM in a variety of organizational environments. The basic idea is that every manager and, collectively, every organization have some levels of appetite for risk. Some may accept risky ventures that promise high returns, while others prefer more guaranteed-return low-risk ventures. One can think of this appetite for risk concept or measure in terms of two investors. One may prefer to invest in very low risk but typically low-return money market or index funds, while another may invest in low-cap start-up technology stocks. That latter investor can be described as having a high appetite for risk. As an example, on a street intersection with a Walk/Don't Walk crossing light, the person who keeps crossing the intersection when the light begins to flash "Walk," warning that it will soon change to Don't Walk, has a higher appetite for risk.
- *ERM provides only reasonable, not positive assurance on objective achievements.* The idea here is that an ERM, no matter how well thought out or implemented, cannot provide management or others with any assured guarantee of outcomes. A well-controlled organization, with people at all levels consistently working toward understood and achievable goals, may achieve those objectives period after period—even over multiple years. However, an unintentional

human error, an unexpected action by another, or even a natural disaster can occur. The previously referenced December 2004 Southeast Pacific tsunami is an example of such an unexpected event. The last recorded major tidal wave in that part of the world took place some 400 years previously. Despite an effective ERM process, an organization can experience such a major and totally unexpected failure. Reasonable assurance does not provide absolute assurance.

- *ERM is designed to help attain the achievement of objectives.* An organization, through its management, should work to establish high-level common objectives that can be shared by all stakeholders. Examples here, as cited in the COSO ERM documentation, are such matters as achieving and maintaining a positive reputation within an organization's business and consumer communities, providing reliable financial reporting to all stakeholders, and operating in compliance with laws and regulations. The overall ERM program for an organization should help it to achieve those objectives.

ERM-related goals and objectives are of little value unless they can be organized and modeled together in a manner that management can look at the various aspects of the task and understand—at least sort of—how they interact and relate in a multidimensional manner. This is a real strength of the COSO internal control framework model; it describes, for example, how an organization's compliance with regulations impacts all levels of internal controls, from monitoring processes to the control environment, and how that compliance is important for all entities or units of the organization. In a similar manner, COSO has developed an ERM framework model that provides some common definitions of risk management as well as helping to achieve key risk objectives throughout the organization.

COSO ERM FRAMEWORK MODEL

The COSO Internal Control framework, as discussed in Chapter 1 and described in Exhibit 1.1, did a very effective job in describing and defining internal controls and has become a worldwide model. Perhaps because some of the same team members were involved with both the internal controls and the risk management project, the COSO ERM framework—at first observation—looks very similar to COSO internal controls. The COSO ERM framework is shown in Exhibit 3.1 as a three-dimensional cube with the following components:

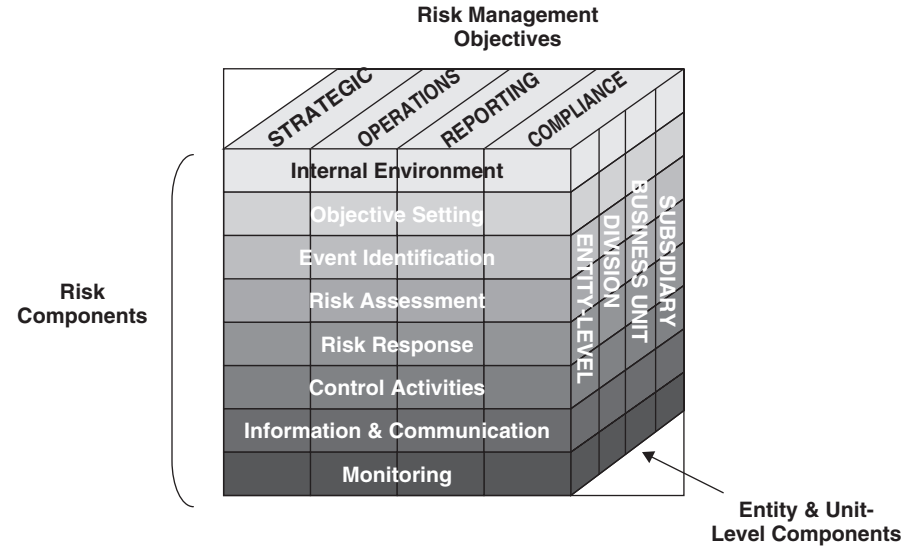

EXHIBIT 3.1 COSO ERM FRAMEWORK

- Four vertical columns represent the strategic objectives of enterprise risk.
- Eight horizontal rows or risk components.
- Multiple levels of the organization, from a "headquarters" entity level to individual subsidiaries. Depending on the organization, there can be many "slices" of the model here.

This chapter describes the horizontal components of COSO ERM, while Chapter 4 discusses the other two dimensions and how they all relate to one another. The concept behind the ERM framework is to provide a model for organizations to consider and understand their risk-related activities at all levels of the organization as well as their impacts on one another. As discussed in Chapter 1, the objective of this book is to help professionals at all levels—from board members to staff auditors—to better understand and manage the risks facing their organizations.

This COSO ERM framework description looks very similar to the COSO internal controls framework that has become familiar to many professionals over recent years. Some initially and incorrectly viewed COSO ERM as just a new update to their familiar COSO internal controls framework. However, although looks can be deceiving, COSO ERM has different objectives and uses! *COSO ERM should not be considered just a new and improved or revised version of the COSO internal controls framework!* It is much more. The following sections outline this framework from a risk components perspective, while Chapter 4

introduces COSO ERM from a risk management objective-setting perspective with a focus on how ERM is applied within an organization.

Internal Environment

The internal environment is placed at the top of components in the COSO ERM framework. This is in contrast to the control environment placed at the lowest or foundation level for the COSO internal control framework. Here, one should similarly think of the ERM control environment as the basis for all other enterprise management components. Using some old terminology, the internal environment may be thought of as the capstone to the COSO ERM framework. Going back to the ancient era of bridges constructed of bricks, the capstone was a stone that held together the brick arches rising from each side of a span to hold the overall bridge together. This capstone component is also similar to the box at the top of the organization chart that lists the chief executive officer (CEO) or the designated head of the function. This level defines the basis for all other components in an organization's ERM model, influencing how strategies and objectives should be established, how risk-related business activities are structured, and how risks are identified and acted upon. While the control environment for COSO internal controls focused on current practices in place, such as human resources policies and procedures, ERM takes these same areas and looks at them in a more future philosophy–oriented approach. The ERM internal foundation component consists of the following elements:

- *Risk management philosophy.* This is a set of shared attitudes and beliefs that will tend to characterize how the organization considers risk in everything it does. While often not the type of message published in a code of conduct, a risk management philosophy is the kind of attitude that will allow managers and others at all levels to respond to some high-risk proposal with an answer along the lines of "No, that's not the kind of venture our company will be interested in." Of course, an organization with a different philosophy might respond to this same proposal with an answer such as "Sounds interesting—what's the expected rate of return?" Neither response is really wrong, but an organization should try to develop a consistent philosophy and attitude to how it accepts risky ventures.
- *Risk appetite.* A concept or expression unfamiliar to many managers, risk appetite is the amount of risk an organization is willing to accept in the pursuit of its objectives. This appetite for risk can be

measured in quantitative or qualitative terms, but all levels of management should have a general understanding of this concept as well as the overall organization's risk appetite. The term *appetite* is often not used by managers or professionals, but the term represents an overall philosophy.

- *Board of directors' attitudes.* The board and its committees have a very important role in overseeing and guiding an organization's risk environment. The independent, outside directors in particular should closely review management actions, ask appropriate questions, and serve as a check-and-balance control for the organization. When a strong senior organization officer has an "it can't happen here" attitude when considering the possible risks surrounding some new endeavor, members of the board are often the best people to ask the hard questions about how the organization would react to a "can't happen" event that actually happens.
- *Integrity and ethical values.* This important ERM internal environment element requires much more than a strong published code of conduct and includes strong integrity and standards of behavior for members of the enterprise. There should be a strong corporate culture here that guides the organization, at all levels, in helping to make risk-based decisions. The Johnson & Johnson Tylenol crisis of 1982 provides a good example of the importance of a strong corporate set of ethical values as a compass to provide direction and to help manage risks. Johnson & Johnson, a major medical products provider, manufactured the popular over-the-counter pain reliever medication Tylenol. In those days, such medications were sold in stores over the counter in screw-top bottles. Someone in the Chicago area opened a few of these store-shelf Tylenol bottles, adulterated the contents with cyanide poison, and replaced the bottles on the store shelves. Several people who purchased this tainted Tylenol subsequently died from cyanide poisoning, and an investigation quickly pointed to Johnson & Johnson and the poison-tainted Tylenol.

  This whole matter put Johnson & Johnson under massive pressure. The corporation knew that it had extremely strong quality control processes in place that would prevent such a poison contamination from occurring within their own manufacturing facilities. They also knew that the contaminated products had appeared only in the Chicago area, while Tylenol was found on store shelves worldwide. A total product

recall would be extremely expensive. However, Johnson & Johnson did not go through a long series of internal investigations or denials but quickly did the right thing. They recalled all of the Tylenol from store shelves worldwide and subsequently re-released it in a newly designed sealed package. When asked why they were able to make such a very expensive recall decision so quickly with no evidence that they were at fault, the corporation stated that there was no need for a delayed decision. The Johnson & Johnson credo, their ethical values statement, dictated their decision. That credo stated very strongly that the company's first responsibility is to supply high-quality products to their customers.[4] At the time of the Tylenol crisis, everyone at Johnson & Johnson knew this credo (it was posted widely in organization facilities) and there was no need for a decision. The whole unfortunate matter really highlights the importance of a strong level of integrity and ethical values for an organization.

A strong corporate mission statement, as well as written codes of conduct, is an important element of an organization's integrity and ethical values. Although most organizations will not face a crisis on the level of Johnson & Johnson with its tainted Tylenol in 1982, a stronger anchor of this sort might have helped some organizations to better avoid the more recent accounting scandals in recent years that led to the situations at Enron, WorldCom, and others as well as the enactment of the Sarbanes-Oxley Act (SOx). This area should be an essential component in every ERM framework.

- *Commitment to competence.* Competence refers to the knowledge and skills necessary to perform assigned tasks. Management decides how these critical assigned tasks will be accomplished through developing appropriate strategies and assigning the proper people to perform these often strategic tasks. We have all seen organizations that do not have this type of commitment. Senior management will make grand and loud plans to accomplish some goal but often will make no positive effort to achieve the goal. The stock market often punishes such activities. With a strong commitment to competence, managers at all levels will take steps to achieve their promised goals.

- *Organizational structure.* While every enterprise will develop an organizational structure that meets its current needs and often satisfies its heritage, that same organizational structure should have clear lines of authority and responsibility along with appropriate lines of reporting. A poorly constructed organizational structure makes it difficult to

plan, execute, control, and monitor activities. Every professional has seen situations where an organizational structure does not allow appropriate lines of communication. For example, prior to SOx, many internal audit groups reported to their board of directors audit committees only on paper but with limited day-to-day communications beyond periodic audit committee meetings. While SOx has changed this situation today, those past environments where the audit committee had only very limited communications with its internal audit function represented a failure in organizational structure. While this situation has been corrected through the passage of SOx, there will always be many situations where the organizational structure needs improvement in order to achieve effective ERM.

- *Assignments of authority and responsibility.* The assignment of authority refers to the extent or degree to which authority and responsibility is assigned or delegated in an organization. The trend in many organizations today is to push such matters as levels-of-approval authorities down the organization structure, giving first-line employees greater authorization and approval authority. A related trend has been to "flatten" organizations by eliminating middle-management levels. These organizational structures usually encourage employee creativity, faster response times, and greater customer satisfaction. This type of customer-facing organization requires strong procedures that outline the "rules" for all members of the staff, as well as ongoing management monitoring of these actions so that decisions can be overruled if necessary. All individuals in the organization should know how their actions interrelate and contribute to the overall objectives of the organization. A strong code of conduct is a critical element here. This should be the type of document that is communicated to all stakeholders in the organization, with a formal requirement that all persons who receive this code acknowledge that they have read, understand, and agree to comply with the code. While there are many variations of this type of document, Exhibit 1.2 lists the topics that may be found in a typical organization code of conduct.
- *Human resource standards.* An organization's practices regarding employee hiring, training, compensating, promoting, disciplining, and all other actions send messages to all of its members regarding what is favored, tolerated, or forbidden. When management winks at or ignores some "gray area" activities rather than taking a strong

stand, that type of message is often quickly communicated to others throughout an enterprise. A strong set of standards is needed that is both communicated to all stakeholders and enforced.

The previously referenced COSO ERM guidance materials have many other examples of the necessary components to build an effective internal environment. While many of these refer to the standards and approaches an organization will implement to accept and manage various levels of risk, others refer to just good business practices that are necessary for effective operations. Whether an organization has a high or low appetite for risk, it needs these control environment practices to manage those risks. For example, the organization can give its sales force a rather free rein to "do deals" without much management supervision and approval. Yet, everyone should know the legal, ethical, and management policy limits of those free-rein practices. Processes should be in place such that if anyone "steps over the line" regarding the limits of any of those practices, remedial actions will be swift and widely communicated.

There are many methods for an organization to communicate its risk management standards, but a formal statement in the annual report or information on the organization's Web site home page often is a good place to formally communicate this strategy to investors and interested others. A search of the Web for such risk statements brings many examples, although most seem to be insurance and finance-related organizations. Exhibit 3.2 is a compliance and risk management statement that was extracted from the annual report of an Australian energy utility, Energex. Similar examples can be found in other such reports, but this is interesting because it highlights the need to monitor adherence to the standards for risk management and the organization's risk appetite.

Note: Energex, Ltd. is an Australian electrical utility corporation. This statement is adapted from their 2004 annual report. www.ruesges.com

Compliance and risk management.

Continually seeking to improve standards for compliance and risk management, ENERGEX's compliance and risk management structure includes Board and Executive committees.

The Board and Executive Management recognize the importance of compliance and risk management through the implementation of an effective legal compliance system which is in accordance with the Australian Standard for Compliance Programs - AS 3806.

EXHIBIT 3.2 ENERGEX COMPLIANCE AND RISK MANAGEMENT STATEMENT

Corporate governance.

The Queensland Government Owned Corporations Act requires the ENERGEX Boards to:

- Be responsible for commercial policy and management.
- Ensure the economic entity achieves and carries out objectives set out in the Statement of Corporate Intent.
- Be accountable to its shareholders for performance.
- Ensure that functions are performed in a proper, effective and efficient way.

The Directors and Management of ENERGEX Limited and its subsidiaries are committed to the highest possible standards of corporate governance. Mechanisms and processes are in place to give assurance that the economic entity undertakes its duties and responsibilities in:

- accordance with the law
- the best interests of its shareholders
- a legal and ethical environment which meets contemporary standards
- a manner that is responsible to all stakeholders.

Audit and Compliance Committee.

The Audit and Compliance Committee assists the ENERGEX Limited Board to discharge its responsibility under the Government Owned Corporations Act, Corporations Law, Electricity Act and other relevant legislation.

The ENERGEX Limited Board and the Chief Executive Officer are committed to continuous improvement in a 'culture of compliance' within ENERGEX. The Committee has been established to provide assurance to the Board that the Corporation is properly meeting its obligations in relation to:

- financial integrity
- legal compliance
- business risk management

Risk Management and Compliance Committee.

The Risk Management and Compliance Committee assist the Board of Directors of ENERGEX Limited and the Chief Executive Officer to monitor the effectiveness and efficiency of the Corporation's systems for management of risk and legal and regulatory compliance. Objectives:

- provide assurance that the corporate systems for management of risk and legal and regulatory compliance are operating effectively and efficiently
- provide advice to the Chief Executive Officer on organizational changes to effect strategic and tactical improvements to the systems which manage risk, and legal and regulatory compliance

EXHIBIT 3.2 ENERGEX COMPLIANCE AND RISK MANAGEMENT STATEMENT *(CONTINUED)*

- monitor adherence to the standards for risk management and the organization's risk appetite as prescribed by the ENERGEX Ltd Board and Chief Executive Officer

Compliance and Risk Management.

The Trading Risk Management Committee assists the ENERGEX Retail Board to fulfill its oversight responsibilities in energy purchasing, trading and associated risk management. It undertakes its activities within the following broad areas:

- philosophy, policies and processes
- compliance audit
- performance review

EXHIBIT 3.2 ENERGEX COMPLIANCE AND RISK MANAGEMENT STATEMENT *(CONTINUED)*

Source: Used with permission of Energex Ltd.

The internal environment component of COSO ERM has two major outputs that feed other elements of the COSO ERM framework: the organization's risk management philosophy and its relative appetite for risk. While risk management philosophy was discussed in the preceding paragraphs in terms of board of directors' attitudes and human resource policies, among others, risk appetite is often a softer measure in which an organization has determined that it will accept some risks but reject others in terms of their likelihood and impact. Exhibit 3.3 shows a risk appetite map where an enterprise should decide the range in which it will be willing to accept risks in terms of their likelihood and impact. This diagram suggests that an organization might be willing to get involved in a high-negative-impact project if there is only a low likelihood of an occurrence. There is a third dimension to this chart as well. An organization will sometimes have a greater appetite for a more risky endeavor when there is a higher potential return.

Objective Setting

Ranked right below the internal environment component, the objective-setting component of COSO ERM outlines some necessary preconditions that must be established before management can establish an effective ERM environment. This component says that in addition to the internal environment outlined above, an organization must establish a series of strategic objectives covering its operations, reporting, and compliance activities. These strategic objectives are high-level goals that should be aligned with an organization's mission or vision.

A formal mission statement often is a crucial element in the strategic planning of an enterprise. It is a general statement of purpose and can be a building block both for an overall strategy and the development of more specific functional

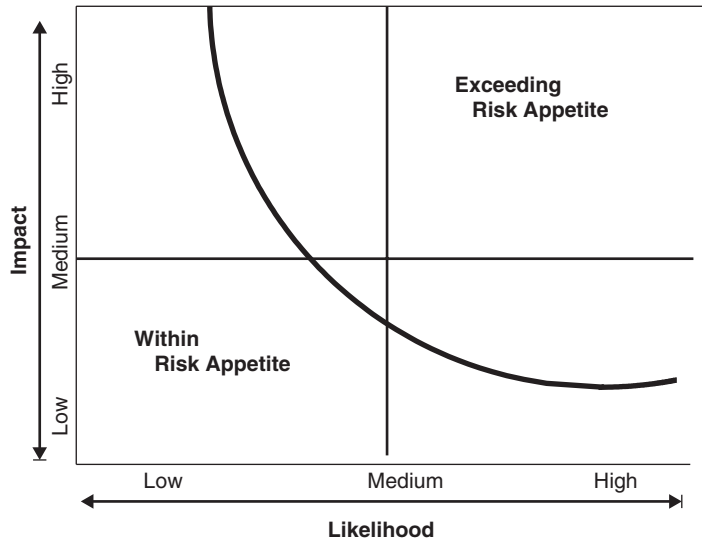

EXHIBIT 3.3 RISK APPETITE MAP

strategies. It is a statement of organizational purpose. Often just a simple, straightforward statement, a mission statement states an organization's objectives and its overall attitude toward risks. Exhibit 3.4 lists some older and newer mission statements from major corporations. These statements say a lot about what a corporation wants to achieve and also defines attitudes toward risk. Although very much out of date at present, both the early Honda and PepsiCo mission statements outline objectives where each organization will tolerate risks in order to achieve their objectives. Disney's much softer statement implies a more measured, less risky approach.

Ford Motor Company (early 1900s): "Ford will democratize the automobile."

Sony (1950s): "Become the company most known for changing the worldwide poor-quality image of Japanese products."

Boeing (1950): "Become the dominant player in commercial aircraft and bring the world into the jet age."

Honda (1960s): "We will crush, squash, and slaughter Yamaha."

PepsiCo (1980): "Beat Coke."

Wal-Mart (1990): "Become a $125 billion company by the year 2000."

3M: "To solve unsolved problems innovatively."

Merck: "To preserve and improve human life."

Walt Disney Company: "To make people happy."

EXHIBIT 3.4 CORPORATE MISSION STATEMENT EXAMPLE

Properly done, a mission statement will allow an organization to first develop some high-level strategic objectives to achieve its mission statement and then to help it select, develop, and implement a series of operations, reporting, and compliance subobjectives. PepsiCo's "Beat Coke" mission statement from an earlier time was made by a much different company. Whether or not they ever totally achieved that mission, the corporation developed some strategic objectives at that time that have turned them into a very different company. From the mission statement to strategic objectives, a next step is to develop a series of operational, reporting, and compliance objectives. While operations objectives pertain to the effectiveness and efficiency of the organization in its goals of achieving profitability and performance, the reporting and compliance goals cover how the organization will report its performance and comply with laws and regulations.

COSO ERM also suggests that an enterprise should formally define such goals with a direct linkage to its mission statement. Starting here and throughout our discussion of the COSO ERM components as well as in other chapter materials when appropriate, we will be referring to a hypothetical computer products manufacturer called Global Computer Products. Exhibit 3.5 gives an overview and background of this example company, while Exhibit 3.6 summarizes some of the various risks that may impact such a sample company. An understanding of these risks would allow the sample company to develop an effective risk assessment approach.

Our example company is a hypothetical $2.4 billion sales manufacturer and distributor of hardware and software-based computer security products. We will reference Global Computer Products in other chapters as an example of how an organization can assess its risks and develop an effective ERM strategy. This description represents the type of medium-sized organization today that is operating internationally in a higher-technology but sales-driven area.

Some key risk-oriented characteristics of Global Computer Products include:

- *Locations and operations.* The company has a headquarters office in the Chicago, Illinois area with a computer security development facility in San Jose, California, and four product distribution centers in smaller-city locations in the United States, as well as a distribution office in Belgium. In addition, the company has two hardware manufacturing facilities in China and a software production and distribution facility in India. All facilities are leased or licensed, and customer service functions have been outsourced.

EXHIBIT 3.5 CORPORATE BACKGROUND: GLOBAL COMPUTER PRODUCTS EXAMPLE

- *Management team*. The company's CEO was originally the founder of the company. He and three senior engineers are the only employees left over from the early days and its initial public stock offering (IPO). Due to turnover often typical in the industry, most employees have fairly short tenures. The CFO is quite new, as the prior officer was asked to resign because of a Sarbanes-Oxley–related dispute with the audit committee. The company makes extensive use of nonemployee contract workers. Reporting to the CAO, Global has a relatively small internal audit department as well as a single general counsel.
- *Product description*. Global developed a computer security product that consists of both a hardware device plugged in to a user's computer along with software drivers. The hardware device consists of a plug-in card based primarily on standard hardware chips along with some embedded programming. The software is based on proprietary algorithms. Elements of the product design are protected by patents, although these rights have been both challenged in courts and also have been somewhat copied by some competitors.
- *Marketing*. Global's product is marketed by advertisements in professional publications as well as through a team of sales representatives. On a worldwide basis, 80% of sales are to individuals, with the balance to smaller businesses. The United States accounts for about 75% of product sales, with the balance from Europe. There is also a small but growing segment of sales in Brazil, where an independent agent is distributing the product. Global ships products from its distribution centers direct to computer equipment retailers as well as shipping to individual customers, based on their Internet, mail, or telephone orders.
- *Sales and finances*. Global's $2.4 billion in sales is split in the following categories:

Consumer cash sales through credit card purchases	41.0%
Sales to wholesale distributors	23.4%
Export sales to agents	12.7%
Licensing fees and royalties	4.9%

Global is a public company, traded on NASDAQ. With its stock broadly distributed, private equity venture capitalists hold 12% of the shares, and management holds 3%. Long-term debt totals $450 million, with the majority of that based on debentures sold to the venture capital investors. That debenture issue included warrants that could be converted into a substantial block of common stock.

EXHIBIT 3.5 CORPORATE BACKGROUND: GLOBAL COMPUTER PRODUCTS EXAMPLE *(CONTINUED)*

The following are some — but certainly not all — of the key risks that could impact the example company Global Computer Products referenced throughout these chapters. These risks may be expanded or modified as the example organization improves and perfects its risk environment. These risks are not listed in any order of importance, and any could be more critical than another.

The nature of these various risks shows the difficulty of classifying a risk as operational versus financial or determining whether it belongs to a business unit or operating division. These risks often cross the lines of the COSO ERM cube. They should just be considered risks that impact the enterprise.

- Organization strategic risks that could impact the effectiveness of products or operations:
  - Changes in technology that impact the effectiveness of company products
  - A currency crisis at one or another of the international operations countries causing major operations problems
  - Increased tariffs or import/export regulations
  - A major weather disturbance, such as a tornado or military actions
  - New competitors offering attractive alternative products
  - Interest rate increases or other factors limiting the ability to finance expansion
  - The failure of a key customer or vendor
- Company operations risks:
  - A computer system or network failure at one or several locations
  - The unexpected resignation of a key management or technical senior manager
  - Labor unrest or related problems at one or another facility
  - The failure to complete several key information systems planned upgrades
  - Product licensing disputes and resulting litigation
  - The failure of an ISO or some other standards audit
  - A major loss in stock market capitalization value due to reported operating losses or other negative information
- Financial and operational reporting risks:
  - Significant internal control weaknesses identified through a SOx Section 404 review
  - Failure of one or another subsidiary units to secure a "clean" external audit opinion

EXHIBIT 3.6 GLOBAL COMPUTER PRODUCTS CORPORATE RISKS SUMMARY

- Errors in individual unit financial or operations reported that are not readily detected at headquarters
- Service support reporting weaknesses

- Compliance risks:
  - Financial reporting errors or missed reports
  - Compliance reporting failures at any level of local or national operations
  - Failure to establish appropriate company-wide ethical and financial reporting compliance standards
  - Failure to meet product quality standards

EXHIBIT 3.6 GLOBAL COMPUTER PRODUCTS CORPORATE RISKS SUMMARY *(CONTINUED)*

Following our discussion of general corporate mission statements and with the introduction of the example company, Exhibit 3.7 shows a mission statement for Global Computer Products with a linkage to strategic and specific related objectives. Our discussion here—and certainly not a goal of COSO ERM—is not to suggest approaches to developing organization mission statements and formal strategic objectives. Rather, the message here is that any and every organization should develop a mission statement and then have some formal objectives to achieve that mission. In addition, the organization should develop some units of measure to allow them to assess whether they are achieving those risk management objectives.

The Internal Environment component of COSO ERM, discussed previously, has two principal outputs: an understanding and definition of the organization's risk management philosophy and a recognition of the organization's risk appetite. These two outputs allow the objective-setting component to

Global Computer Products is one of the leading worldwide suppliers of desktop computer system security protection products. With strong attention given to computer security risks and threats, we strive to offer one of the most secure but easy-to-use combined software and hardware products in today's marketplace.

In order to build our products and market them in ever-expanding circles, we will assemble a worldwide team of superior computer security technical talent to produce our products while selling them in an efficient and ethical manner. We will continue to monitor our strategic and operational risks in this complex and ever-changing world of computer security risks and threats.

EXHIBIT 3.7 MISSION STATEMENT: GLOBAL COMPUTER PRODUCTS EXAMPLE

develop a series of objectives to achieve risks as well as to formally define that risk appetite in terms of its tolerances for risk. Tolerances are formal guidelines or measures that an enterprise should use—at all levels—to assess whether it will accept risks. Establishing and enforcing risk tolerances can be very difficult for organizations. There will be problems if the rules are not clearly defined, well understood, and strictly enforced. It is often difficult to enforce rules. For example, in March 2005, the Boeing board terminated their CEO because of a "consensual relationship" with a female employee.[5] This is the type of relationship that has often been "winked at" in the past, but was recognized here as a violation of the code-of-conduct rules, and the board took swift and decisive action. If an organization wants to establish a strict set of rules, they should be enforced throughout the entity. (As an aside, subsequent reporting on the matter suggested that events might have been handled differently if the Boeing CEO had evidently not been so sloppy in failing to secure his passionate e-mail messages!)

A better approach for an organization is to establish some acceptable forms of risk tolerance; that is, they might establish a tolerable range of risks they will accept. For example, all products coming off the production line might have acceptable preestablished error rates of less than some value, such as producing goods at an error rate no greater than 0.005 percent. That is an extremely low error rate in many areas, and production management in that case would accept the risk of any product warranty claims or damage to their reputation if there were errors within that very narrow limit. Of course, the ranges for an organization involved in health care products would be infinitesimally tighter.

The point here is that an enterprise should define its risk-related strategies and associated risk objectives. Within those guidelines, it should decide on its appetite and tolerances for risk. That is, what level of risk is it willing to accept, and given those risk tolerance rules, how much is it willing to deviate from these preestablished measures. Exhibit 3.8 outlines the relationship of these portions of the objective-setting component of COSO ERM with reference to our example company. Starting with an overall mission, the approach is to (1) develop strategic objectives to support accomplishment of that mission, (2) establish a strategy to meet objectives, (3) define any related objectives, and (4) define risk appetites to complete that strategy. In order to manage and control risks at all levels, an organization needs to set its objectives and define its tolerances for having to engage in risky practices and for its adherence to these rules. Things will not work if the organization establishes some risk-related objectives but then proceeds to ignore them. This author can reflect on service in the U.S. Army in the late

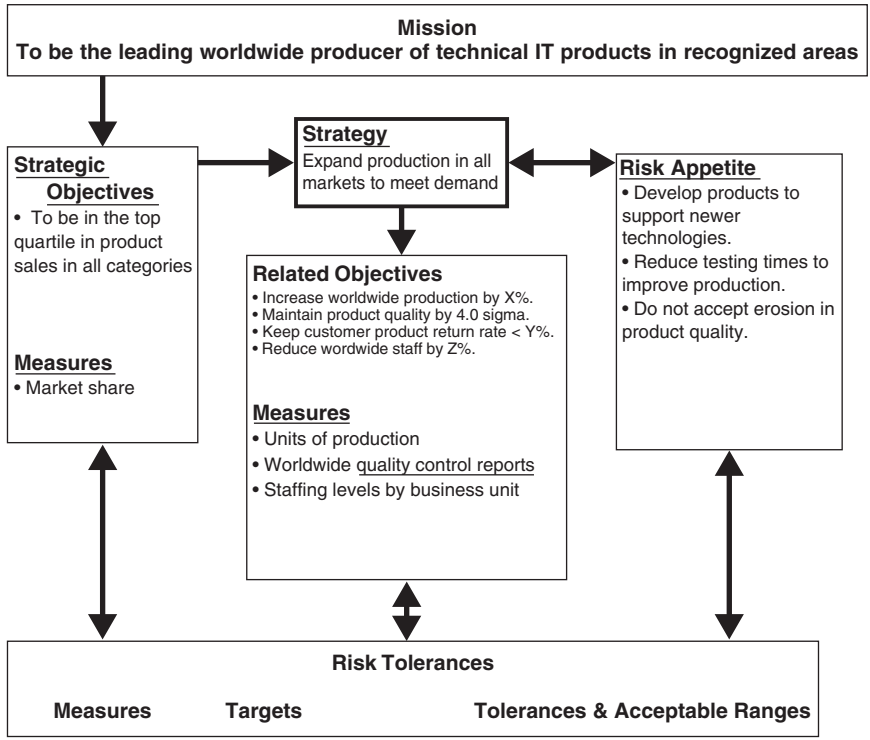

EXHIBIT 3.8 COSO ERM RISK OBJECTIVE SETTING COMPONENTS

Source: Adapted from *Enterprise Risk Management—Integrated Framework: Application Techniques.* New York: COSO, April 2004.

1960s during the time of the Vietnam conflict. There was an Army "zero defects" program in place at the time, at least at this author's Washington, D.C.–area base, where all members of the Army were requested to sign a pledge that they would perform no work-related mistakes—a zero defects pledge. Perhaps this was far too tight a risk tolerance range at that time and in that environment; these pledges were ignored by many as little more than another scrap of paper, there was no follow-up, and the rest is history.

Event Identification

Events are incidents or occurrences, external or internal to the organization, that affect the implementation of the ERM strategy or the achievement of its objectives. While the tendency is to think of such events in a negative sense—determining what went wrong—they can be positive, negative, or

both. There is a strong level of performance monitoring taking place in many organizations today, but that monitoring process tends to emphasize such matters as costs, budgets, quality assurance compliance, and the like. The ERM risk objectives, discussed previously, can become lost in this process of monitoring more operational and process-oriented objectives. Organizations usually have strong processes to monitor such events as favorable and particularly unfavorable budget variances, but often do not regularly monitor either the actual events or the influencing factors that are the drivers of such budget variance events.

The COSO ERM executive summary framework documentation[6] lists a series of the types of influencing factors that should be part of the framework's event identification component, including:

- *External economic events.* There is a wide range of external events that need to be monitored in order to help achieve an organization's ERM objectives. Ongoing short- and long-term trends may impact some elements of an organization's strategic objectives and thus have an impact on its overall ERM framework. As an external economic event example, in December 2001 and after some ongoing currency market turmoil, Argentina declared a major default of its public debt. This type of external event had a major impact on many enterprises in many different areas, whether they were credit markets or suppliers of agricultural commodities, or had other business dealings in South America.

  External economic event identification here requires some function in the organization to go beyond reported news headlines and raise the flag to suggest that "yes," such a currency default may highlight an organization risk-related event. In our example corporation, a unit of this company, Global Computer Products, may have a major customer who did a lot of business with Argentina. The challenge here is that some individual or function in the organization should be in a position to raise a "What are the implications of this?" type of question. Approaches to this type of event identification are discussed in Chapter 12 on establishing an enterprise-wide risk management culture.
- *Natural environmental events.* Whether it is fire, flood, or earthquakes, numerous events can become identified as incidents in ERM risk identification. Impacts here may include loss of access to some key raw material, damage to physical facilities, or unavailability of personnel.

- *Political events.* New laws and regulations as well as the results of elections can have a significant risk event–related impact on organizations. Many larger enterprises have a government affairs function that reviews developments here and lobbies for changes. However, such functions may not always be aligned with ERM objectives.
- *Social factors.* While an external event such as an earthquake is sudden and arrives with little warning, most social-factor changes are slowly evolving events. These include demographic changes, social mores, and other events that may impact an organization and its customers over time. The growth of the Hispanic population in the United States is such an example. As more and more Hispanic people move to a city, for example, both the language-related teaching requirements in public schools and the mix of selections in grocery stores will change. As another example of societal change, the previously referenced dismissal of a major corporation CEO for a consensual sexual relationship with another company employee would probably have been ignored in another era. Changing social mores today led to that dismissal.
- *Internal infrastructure events.* Organizations often make benign changes that trigger other risk-related events. For example, a change in customer service arrangements can cause major complaints and a drop in customer satisfaction. Strong customer demand for a new product may cause changes in plant capacity requirements and the need for additional personnel.
- *Internal process–related events.* Similar to infrastructure events, changes in key processes can trigger a wide range of risk identification events. As with many such items, risk identification may not be immediate, and some time may pass before the process-related events signal the need for risk identification.
- *External and internal technological events.* Every organization faces a wide assortment of ongoing technological events that will trigger the need for formal risk identification. Some may be gradual over time, while others will be more sudden. The Internet and the World Wide Web have been with us for some time, and the shift to an Internet environment has been somewhat gradual for many. In other cases, a company may suddenly release a new improvement that causes competitors everywhere to jump into action. Although the idea seems very commonplace today, when Merrill Lynch launched its Cash Management Account (CMA) concept in the mid-1980s, it

caused a major stir in the financial services industries. CMA offered a service wherein the customer could have stock brokerage, banking, checking, and other financial services all under one roof. In the past, all such accounts were with separate providers with essentially no linkages between them.

An organization needs to clearly define what it considers significant risk events and then should have processes in place to monitor all of those various potentially significant risk events such that the organization can take appropriate actions. This monitoring should come out of the Chapter 12 discussion on establishing an effective risk culture, and is really a forward-thinking type of process that is often difficult to recognize in many organizations. Although we were not talking about risk at that time but growing the business, this author recalls working for a then major retail organization in the mid-1990s and making a presentation to both the CEO and CIO, among others, about the need to develop an Internet strategy. Although the Internet at that time certainly did not at all have the capability and recognition that it has today, this set of recommendations to that retail organization's senior executives was met with only a set of "thanks but no thanks" responses. The CIO at that meeting advised the CEO that the Internet would never "catch on" and the Internet strategy recommendation was rejected.

The process of looking at the various internal and external potential risk events and deciding which of those events require further attention can be a difficult process. Some are immediate needs and others very future directed. The COSO ERM application techniques volume offers some help here. It suggests that an organization establish some formal processes to review potentially significant risks and then to begin the process of taking action. The COSO ERM guidance material suggests that organizations consider some of the following approaches:

- *Event inventories.* COSO ERM recommends that management should use risk-related listings of events common to the organization's specific industry and functional area. This is saying that an organization should consider establishing some type of "lessons learned" archive source. This is the type of data that his historically been supplied by longer-tenure members of an organization who can offer "We tried this several years ago, but …" types of comments. This type of history is often lost in today's organizations, and an effective risk culture, as discussed in Chapter 12, can provide some help here.
- *Facilitated workshops.* An enterprise can establish cross-functional workshops to discuss potential risk factors that may evolve from various

internal or external events. The result from these would be action plans to correct the potential risks. This is one of those suggested approaches that sounds good, but most organizations typically will not allocate their precious time to meet in cross-functional groups to talk about risks in a "What would happen, if …" type of format.

- *Interviews, questionnaires, and surveys.* Information regarding potential risk events can come from a wide variety of sources such as comments on customer satisfaction letters or exit interview comments from departing employees. There is a need to capture and classify information here in order to identify any that might point to a risk event. People throughout the organization should be aware of these issues, and an organization risk management culture, discussed in Chapter 12, will provide this information.
- *Process flow analysis.* The COSO ERM application techniques materials recommend the use of flow diagrams to review processes and to identify potential risk events. For many organizations, the process flow diagrams are very similar to the internal control documentation that was prepared as part of their SOx Section 404 work, where an organization's internal controls are stated and any control weaknesses identified. Although in the absence of COSO ERM that Section 404 work does not focus on risk event identification, this ERM analysis can conveniently be combined with the Section 404 work in future update periods. These processes are discussed in Chapter 7 on SOx and ERM.
- *Leading events and escalation triggers.* The idea here is to establish a series of business unit objectives, the measurement criteria necessary to meet those objectives, and risk tolerance criteria to promote remedial action. For example, an organization's IT group may establish an objective to maintain strong security controls over system intrusion. With a measure of the number of intrusion attempts identified during a period, perhaps over three intrusions in a given month would trigger further action. There are very good software tools available today to monitor all aspects of organization performance. Called dashboards, these tools are available through such software suppliers as Business Objects or COGNOS. Often very complex, the previously referenced COSO applications techniques material has a simplified example of such a dashboard report. They operate similar to the controls on the dashboard of an automobile, where indicators will flash signals for such conditions as low oil pressure or overheating. Exhibit 3.9 is an example of such a risk event dashboard, tracking the risk status of the

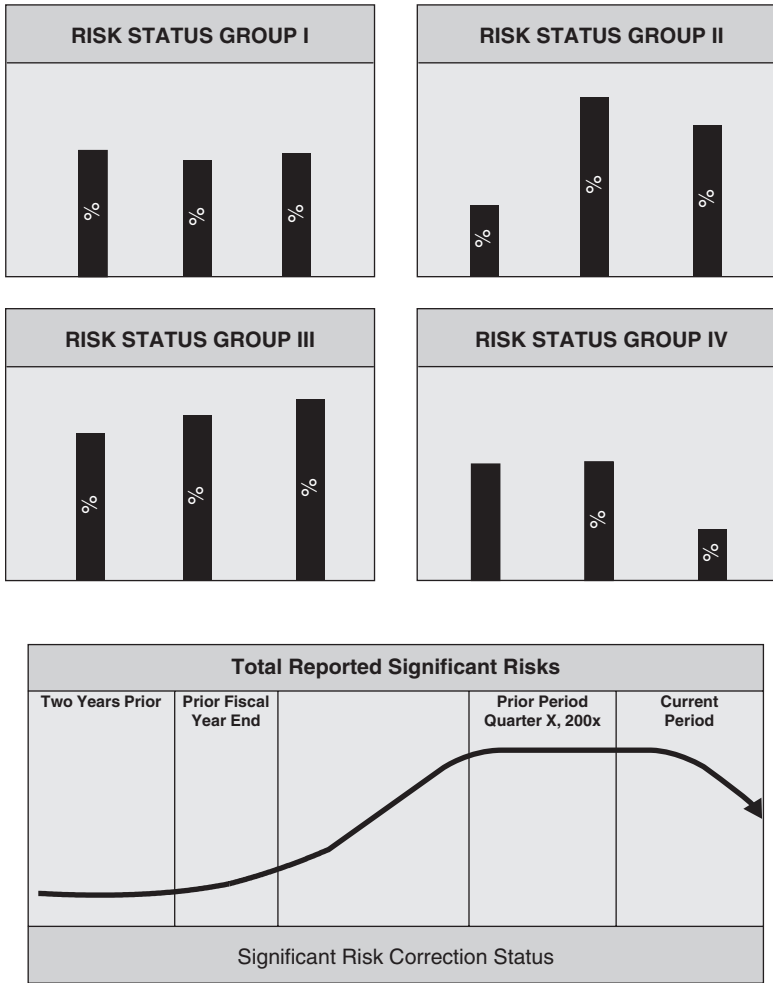

EXHIBIT 3.9 RISK EVENT DASHBOARD TRACKING EXAMPLE

Global Computer Products sample company. The idea is to report on risk status through some simple, easy-to-comprehend graphics, such as the up or down arrows shown, usually displayed in red, yellow, and green, as well.

- *Loss event data tracking.* While the dashboard approach just introduced monitors risk events as they happen, it is often valuable to put things in more perspective after the passage of some time. Loss event tracking refers to using both internal and public database

sources to track activity in areas of interest. These sources can cover a wide variety of areas ranging from leading economic indicators to internal equipment failure rates. Again, here, an organization should install effective risk identification processes to track both internal and external risk–related events.

The risk identification tools and approaches just discussed can yield some very valuable and useful information to an organization that identifies either risks, opportunities, or a combination of both. The key here is the need for good analyses of the data as well as initiating plans for action, whether to shield from the risk or to take advantage of potential opportunities. This should be part of the organizational risk management culture, discussed in Chapter 12.

Risk Assessment

We have talked about the internal environment component as being the cap or cornerstone of COSO ERM framework. In a later section we will discuss the monitoring component as a key foundation component to support COSO ERM. The risk assessment component is really about in the center of this framework model, as shown in Exhibit 3.1, and represents the core of COSO ERM. Risk assessment allows an organization to consider the extent to which potential risk-related events may have on an organization's achievement of its objectives. These risks should be assessed from two perspectives: the likelihood of the risk's occurring and its potential impact. This component of COSO ERM reintroduces some of the classic risk management fundamentals that were discussed in Chapter 2.

As a key part of this risk assessment process, management needs to consider both the inherent and residual risks. The following are key risk management concepts:

- *Inherent risk.* As defined by the U.S. government's Office of Management and Budget, inherent risk is the "potential for waste, loss, unauthorized use, or misappropriation due to the nature of an activity itself." Major factors that affect the inherent risk of any activity within an organization are the size of its budget, the strength and sophistication of the group's management, and just the very nature of its activities. Inherent risk is outside the control of management and usually stems from external factors. For example, the major retailer Wal-Mart is so large and dominant in many of its markets that it faces certain inherent risks due to its sheer size.

- *Residual risk.* This is the risk that remains after management responses to risk threats and countermeasures have been applied. There will virtually always be some level or residual risk.

These two risk concepts imply that enterprise management will always face some risks. After they have addressed the risks that came out of the risk identification process, they will usually still have some residual risks to remedy. Following this, there will be a variety of inherent risks about which they can do little. The major retailer Wal-Mart, for example, can take some steps to reduce its market dominance–related inherent risks, but it can do essentially nothing regarding the inherent risk of a major earthquake.

Likelihood and impact are two other key components necessary for performing risk assessments. Likelihood is the probability or possibility that the risk will occur. In many instances, this can be a key management assessment stated in the terms of high, medium, or low likelihood of the risk's occurring. There are also some good quantitative tools here as well, but it does little good to estimate the likelihood of a risk's occurring in terms of multiple decimal points if there was no basis for developing that precise a number beyond a normal or regular statistical calculation.

Estimating the impact if a risk event occurs is a bit easier. Chapter 11, for example, discusses IT-related risks such as the impact of a data server and network center catastrophic loss or failure. An organization can develop some relatively accurate estimates of such matters as the cost of replacing facilities and equipment, the cost of restoring a system, and to some extent, the cost of lost business due to the failure. However, the whole concept behind ERM is not to develop precise, actuarial-level calculations regarding the risk but to gain some measure to provide for an effective risk management framework. Those detailed calculations can be delegated to insurance estimators and others.

An analysis of risk likelihoods and potential impacts can be developed through a series of qualitative and quantitative measures.[7] These sources provide guidance on approaches to determine relative probabilities or other measures regarding risk likelihoods and potential impact. The basic idea, however, is to assess all of the identified risks, as discussed in the previous section, and to rank them in terms of likelihood and impact.

Without going through a detailed quantitative analysis, each of the risks identified at a point in time can be ranked on an overall relative scale of 1 to 10, with separate estimations made for the impact and the likelihood of each. This can be achieved through a focused management group decision

process where each of the identified risks is reviewed and then ranked with respect to this scale. Exhibit 3.10 provides an example of how a series of sample risks for the example company would be evaluated and then assigned relative values. The example shows only three risk areas, although this would be a much larger and comprehensive list for any organization. Those risk results, scaled from 1 to 10, can be plotted with greater granularity. The idea is to identify relative risks and assign some relative rankings. The whole idea of this type of analysis and any subsequent charting is to identify the upper-right-hand quadrant high-impact and high-likelihood risks for the organization. These are the risks that should receive the most thorough management attention.

A key to this overall process of identifying high-risk events with strong likelihoods and potential impacts is an accurate and balanced review and assessment process. One of the most powerful earthquakes in U.S. history occurred in the winter of 1811–1812 in the central Mississippi Valley near St. Louis, Missouri, in an area called the New Madrid fault. This earthquake

Risk Name	Risk Definition	Impact	Likelihood	Risk Ranking
1. Accounting risk	Failure to record sales activity accurately and timely may misstate financial reports.	**High**: Accounting errors may have a material impact on financial and operational information.	**Medium**: Despite strong procedures, newer personnel in various locations may make errors.	8
2. Legal risk	Failure to understand current and changing laws and regulations may result in inability to comply with laws in multiple operation jurisdictions.	**Medium**: Even small, technical violations of most regulations should not have a material effect on operations.	**High**: With worldwide operations in multiple jurisdictions, violations—if only technical—can occur.	7
3. Segregation of duties	Inadequately controlled segregation of duties may allow employees to process unauthorized, fraudulent transactions.	**High**: Fraudulent operations could have significant impacts on company operations.	**Low**: Ongoing internal audits and stronger management control practices should prevent such control breakdown events.	5

EXHIBIT 3.10 RISK LIKELIHOOD AND IMPACT MAPPING EXAMPLE

changed the course of the Mississippi River, and damage from it occurred as far away as Philadelphia and Washington, D.C. That was nearly 200 years ago, and it could happen again! However, if an enterprise has a business operation in that part of the world today, should it factor in the likelihood and impact of another New Madrid fault event in their analysis? We would argue perhaps not. Unless there were some risk event warnings of active seismic activity in that area, this is an inherent risk that exists but should not be part of the risk analysis here.

The idea is that an organization should use the best data sources available here but view its risks with a level of perspective. That view of potential risks can be influenced by management overconfidence or pessimism. A team approach is needed here, where the enterprise should look at all of these identified risks on a total organizational basis and on a unit-by-unit level. Looking at risks across organizational units represents another dimension to this framework model that is discussed in Chapter 4 on COSO ERM organization objectives. In addition, the risk assessment team needs to consider the relationship between different or connected risks. One risk may involve the potential of unfavorable foreign currency fluctuations in several foreign operations, one with a fairly stable national economy and another with an unstable government. However, the country with the least currency risk may be the operation with the greatest manufacturing plant product quality risk. An enterprise must balance these two conflicting national entity higher risks to determine the most effective plan of action.

Overall approaches to reviewing these various likelihood and impact risks will be discussed in Chapter 5 on implementing an effective ERM program. As suggested at the beginning of this section, risk assessment is a very key component of the COSO ERM framework. This is where an organization evaluates all of the various risks that might impact its various objectives, considers the potential likelihood and impact of each, considers the interrelationship of them on a unit-by-unit or total organization basis, and then develops strategies for responses to these risks. In some respects, this COSO ERM risk assessment process is not too different from the classic risk assessment techniques that have been used over the years. What is unique to COSO ERM is the suggestion that an organization should take a total approach, across all of its operating units and covering all major strategic concerns to identify its spectrum of risks in a consistent and thorough manner. Having identified appropriate risks, the next step is to develop a risk response approach that appropriately covers the various and significant inherent and residual risks identified in this risk assessment process, with consideration given to the organization's risk tolerances.

Risk Response

Having assessed and identified its more significant risks, the next step is to determine how to respond to these various identified risks. This is a management responsibility to perform a careful review of estimated risk likelihoods and potential impacts, and with consideration given to associated costs and benefits, to develop appropriate risk response strategies. These risk responses can be handled following any of four basic risk management approaches:

1. *Avoidance.* This is a strategy of walking away from the risk—such as selling a business unit that gives rise to the risk, exiting from a geographic area of concern, or dropping a product line. The difficulty here is that organizations often do not drop a product line or walk away until after the risk event has occurred with its associated costs. Unless an organization has a very low appetite for risk, it is difficult to walk away from a business area or product line just on the basis of a potential future risk if all appears to be going well at the present in other respects. Avoidance can be a potentially costly strategy if investments were made to get into an area with a subsequent pull-out to avoid the risk.

   A collective "lessons learned" understanding of past activities can often help with this strategy. If the organization had been involved in some area in the past with unfavorable consequences, this may be a good way to avoid the risk once again. With the tendency of constant organizational changes and short employment tenures, this collective history is often lost and forgotten. An organization's well-understood and -communicated appetite for risk is perhaps the most important consideration when deciding if a risk avoidance strategy is appropriate.

2. *Reduction.* A wide range of business decisions may be able to reduce certain risks. Product line diversification may reduce the risk of too strong a reliance on one key product line. Splitting an IT operations center into two geographically separate locations will reduce the risk of some catastrophic failure. There is a wide range of often effective strategies to reduce risks at all levels that go down to the mundane but operationally important step of cross-training employees.
3. *Sharing.* Virtually all organizations as well as individuals regularly share some of their risks by purchasing insurance to hedge or share their risks. Many other techniques are available here as well. For financial transactions, an organization can engage in hedging operations to

protect from possible price fluctuations. A common example of hedging is the investor's use of put or call options to hedge bets on strong price movements. It can also share potential business risks and rewards through joint venture agreements. The idea is to arrange to have another party accept some of a potential risk with the recognition that there will be costs associated with that activity.

4. *Acceptance.* This is the strategy of taking no action. An enterprise can "self-insure" rather than purchase an insurance policy. They might regularly put aside resources to cover or shield them from some event. Essentially, an organization should look at a risk's likelihood and impact in light of its established risk tolerance and then decide whether or not to accept that risk. For the many and varied risks that approach an organization, acceptance is often the appropriate strategy for some risks. However, in too many situations the enterprise will assume the risk might "never happen" and will not adequately fund itself for such a risk event.

Management must develop a general response strategy for each of its risks using an approach built around one of these four general strategies of avoidance, reduction, sharing, or acceptance. In doing so, it should consider the costs versus benefits of each potential risk response and which of these strategies best align with their overall risk appetite. For example, an organization's recognition that the impact of a given risk is relatively low would be balanced against a low risk tolerance that suggests that insurance should be purchased to provide a potential risk response. For many risks, appropriate responses are obvious and almost universally understood. An IT operation, for example, spends the time and resources to back up its key data files and to implement a business continuity plan. There is no question regarding this basic approach but various levels of management may question the frequency of backup processes or how often the continuity plan needs to be tested. This particular issue is discussed in Chapter 11 on IT risk management, but the concept applies to a wide range of other organization risks.

An organization, at this point, should go back to the several risk objectives that have been established as well as the tolerance ranges for those objectives. Then, it should readdress both the likelihoods and impacts associated with each of the identified risks within those risk objectives to develop an assessment of both of the risk categories and an overall assessment of planned risk responses. This will help in understanding how those risks will align with overall corporate risk tolerances. At this point in the risk assessment process, an enterprise will have assessed the likelihood and

potential impact of each of the risks surrounding its objectives as well as some estimates for each. The next step is to develop a set of potential risk responses. This is perhaps the most difficult step in building an effective COSO ERM program for the enterprise. It is comparatively easy to identify a 5 percent likelihood risk that there will be a fire in the scrap materials bin and then to outline a risk response to install a nearby fire extinguisher. However, the responses to most risks are much more complex and require fairly detailed planning in the risk response plans.

The organization should initially go through its key high-impact and high-likelihood identified risks and develop a series of tentative risk response plans. However, this can be a challenging management process! While it is relatively easy—to follow our earlier example—to install a fire extinguisher to provide protection from a scrap materials bin fire, things are usually not that simple. If there is a risk that an organization could lose an entire manufacturing operation due to recognized ancient but still working plant production equipment, potential risk responses here could include:

- Acquire a set of backup production equipment to serve as spare parts for cannibalization.
- Shut down the manufacturing production line with plans to move it elsewhere.
- Arrange for a specialized shop to rebuild/reconstruct the equipment.
- Reengineer the manufactured product along with any necessary plans for the new product introduction.

The point here is that the process of developing risk responses requires a significant amount of planning and strategic thinking in itself. The several risk response alternatives involve costs, time, and detailed project planning. In addition to the planning and strategic thinking, this risk response planning process requires significant management input and approval to recognize the various alternative risk responses and to have action plans in place to satisfy the appropriate responses. For example, one of the old equipment response strategies outlined above is to acquire a set of duplicate backup equipment. If that is to be the approved strategy, action must be taken to complete these various planned steps before this activity can be listed as an approved risk response strategy. Exhibit 3.11 is a worksheet that management could use to analyze alternatives and develop one or more approved responses. We have said “one or more” because an organization should always think of alternative risk response strategies.

This sample document shows only one entered risk. However, the idea is to list, as thoroughly as possible, all of the identified risks of concern. These would be the higher-concern risks that would have been identified in

Risks	Inherent Risk		Risk Response Alternatives		Residiual Risk	
	Likelihood	Impact on Revenue			Likelihood	Impact on Revenue
I. Competitor reaches market first with new product under development.	40%	($5,000,000)	A. Accept	Provide additional resources to speed up R&D to complete new products.	30%	($25,000) less profit due to development costs.
			B. Avoid	Take no specific action. Keep current product offerings in place.	10%	Estimated 10% reduction in profits for line each year.
			C. Share	Offer incentives to current customers to encourage use of current product versions.	20%	
			D. Reduce	Lower prices on current product offerings to discourage conversions to new versions.	40%	
2. Identified Risk # 2	X%	$$	A. Accept B. Avoid C. Share D. Reduce			

EXHIBIT 3.11 RISK RESPONSE PLANNING WORKSHEET

Exhibit 3.10. For each of these, the management team should attempt to estimate the probable inherent risk of occurrence. In the example shown, the team would estimate the likelihood that a competitor will be first to market with a product similar to the one being analyzed. This is the type of estimate that might be made through communication with development personnel and marketing. This is admittedly a best guess, but it should be coupled with an estimate on the impact of the risk's occurring. This example shows the impact on estimated revenue, but other factors can be used to measure the impact, such as market share. The idea is that all risks listed on such an analysis should be measured against the same impact factors.

For each risk, risk response alternatives should be considered. This single example shows different strategies based on an accept, avoid, share, or reduce type of strategy, with a brief description of each strategy. There is no need to list these four approaches for each identified risk. For example, another risk may have multiple possible avoidance strategies but none to reduce risk. For each, however, the team should estimate the likelihood of that strategy's occurring, given the initial risk event's occurring. Again, the impact for each should be estimated, whether revenue or some other consistent measure throughout the analysis.

The concept behind this type of analysis is to look at all risks across a given area in a consistent manner. This can sometimes be a difficult process in a large, multiunit, multiproduct enterprise, but it provides a starting point for getting all of the various risks organized together for better identification of the more significant risks. For an enterprise, the idea is to look at these various potential risks, their probability of occurrence, and the impacts of each. With a good analysis, this should highlight areas for more detailed attention.

Once a series of various risk responses has been developed, a next step is to look at multiple identified risks, by objective, and to consider the various selected risk responses to assess whether those responses will bring the organization within its identified risk tolerances. While this can be a fairly elaborate analysis if there have been multiple identified risks and alternative response, the enterprise can use this data to develop high-level strategies to cover it for these various risk areas. If this type of analysis shows that a response does not appear to meet the organization's risk tolerances, it will be necessary to rethink and revise the risk response to achieve risk tolerance ranges.

COSO ERM calls for risks to be considered and evaluated on an entity or portfolio-wide basis. Entity refers to the total overall organization, but to get to that total view approach, risks should be evaluated and assessed by business, by department, by function, and by other approaches to look at an

organization's risks. This organization-level approach of looking at risks is discussed in Chapter 4, and each of the approaches discussed here should be used for each area of operations and for each major risk area. Risks should be summarized on a business unit or on some other entity-level basis into a risk portfolio. Senior management can then focus on its various risks across the organization to assess their overall impacts. As will be discussed in Chapter 4, it is essential that each unit preparing its own risk portfolio perform this analysis in a consistent manner in order to measure relative from one group to another and across the overall organization. This type of risk portfolio is shown in Exhibit 3.12. This example report is based on the sample report shown in the previously referenced COSO application techniques materials, and it shows the various identified risks by potential financial impacts as well as by the estimated frequency of occurrence. This is the type of communication that should be prepared for senior management and the board of directors to help them to understand the overall portfolio of risks facing an organization and to help develop high-level risk response priorities. The importance of this COSO ERM framework for board of directors management and information is discussed in Chapter 8.

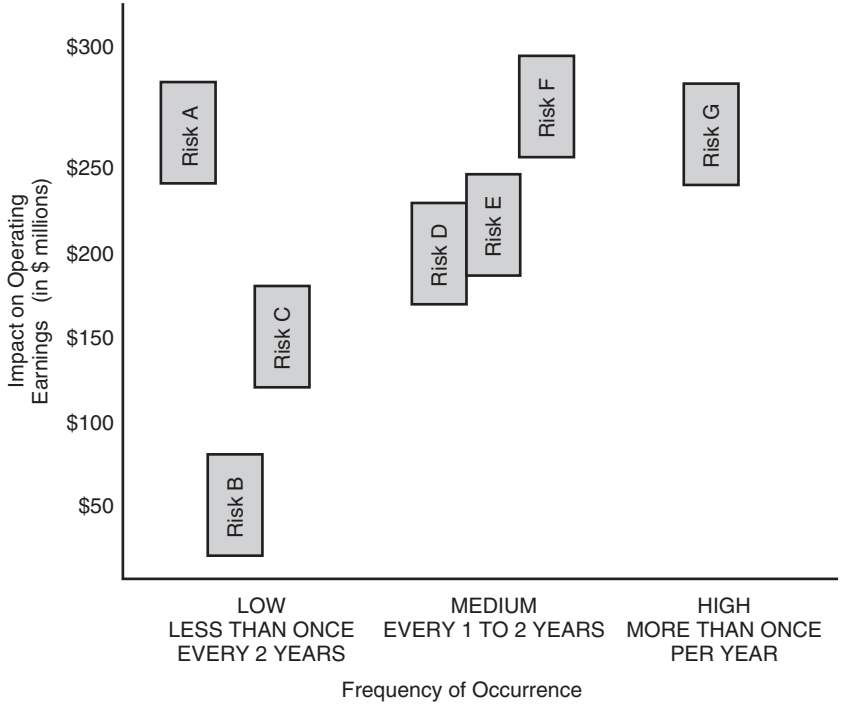

EXHIBIT 3.12 PORTFOLIO VIEW OF RISK SUMMARY

Control Activities

COSO ERM defines what it calls control activities as the policies and procedures necessary to ensure that identified risk responses are carried out. Although some of these activities may relate only to an identified risk and approved risk response in one area of the organization, they often overlap across multiple functions and units. The control activity component of COSO ERM should be tightly linked with the risk response component previously discussed.

Having selected appropriate risk responses, organization management should select the control activities necessary to ensure that those risk responses are executed in a timely and efficient manner. The process of reviewing if control activities are acting or performing properly is very similar to the process that many enterprises have exercised as part of their SOx Section 404 internal control assessments.[8] While with SOx, organizations identified, documented, tested, and then validated internal accounting controls, COSO ERM calls for a similar approach. Having gone through the COSO ERM risk event identification, risk assessment, and risk response processes, risk monitoring can be executed by the following steps:

Step 1. Develop a strong understanding of the identified significant risks and develop control procedures to monitor or correct for these risks.

Step 2. Create testing procedures to determine if those risk-related control procedures are working effectively.

Step 3. Perform tests of the control procedures to determine if the risk-monitoring process tested is working effectively and as expected.

Step 4. Make adjustments or improvements as necessary to improve risk-monitoring processes.

This four-step process is essentially what organizations subject to the requirements of SOx, and its Section 404 requirements, have been doing to review, test, and then assert that their internal control processes are working adequately. A major difference between COSO internal control procedures under SOx rules and ERM, is that an organization *is legally required* to comply with SOx procedures in order to assert the adequacy of their internal controls to their external auditors as part of the Securities and Exchange Commission's (SEC's) financial reporting requirements. There are no such legal requirements with COSO ERM at this time. A prudent organization, however, should seek to install risk-monitoring control activities to monitor

the various risks it has identified. Because of the critical nature of many risks to an enterprise, risk management monitoring can be very critical to an organization's overall health due to the nature of the various risks it may encounter.

Many control activities under COSO internal controls are fairly easy to identify and test due to their accounting controls relates nature. They generally include the following internal control areas:

- *Separation of duties.* Essentially, the person that initiates a transaction should not be the same person that authorizes that transaction.
- *Audit trails.* Processes should be organized such that final results can be easily traced back to the transactions that created those results.
- *Security and integrity.* Control processes should have appropriate control procedures such that only authorized persons can review or modify them.
- *Documentation.* Processes should be appropriately documented.

These control procedures and others are fairly well recognized and applicable to many if not all internal control processes in place in an organization and also somewhat apply to many risk-related events. Many professionals—whether or not they have an accounting and auditing background—can often easily define some of the key controls necessary in many business processes. For example, if asked to identify the types of internal controls that should be built into an accounts payable system, many professionals would identify as significant control points that larger value checks issued from the system must be authorized by several persons, that accounting records must be in place to keep track of the checks issued, and that the check-issuing process should be such that only authorized persons can initiate such a financial transaction. These are generally well and widely understood control procedures. An organization, however, often faces a more difficult task in identifying control activities to support their enterprise risk management framework.

As discussed as part of the ERM event identification component and will again be discussed in Chapter 4, management needs to think of their risk categories in terms of major risk process areas, such as revenue, purchasing, capital spending, information systems, and others. Specific risk-related control activities can be defined within each of these categories, whether for the overall organization or covering some unit or function. Although there is no accepted or standard set of ERM3 control activities at

this time, the COSO ERM documentation suggests several areas such as the following:

- *Top-level reviews.* While senior management may be somewhat oblivious to the "Do the debits equal the credits?" internal control procedures that are covered by their financial teams and auditors, they should be very aware of the identified risk events within organizational units and should perform regular top-level reviews of the status of identified risks as well as the progress of risk responses. This type of regular review coupled with appropriate top-level corrective actions is a key ERM control activity.
- *Direct functional or activity management.* In addition to the top-level reviews outlined above, functional and direct unit managers should have a key role in risk control activity monitoring. This is particularly important in a large, diverse organization where control activities should not just take place at a local unit level and then bump up the organizational hierarchy to some central management level. Rather, risk-related control activities should take place within the separate operating units, with communications and risk resolution taking place across organization channels.
- *Information processing.* Whether it be hard types of IT systems processes or softer forms such as paper or messages, information processing procedures represent a key component in an organization's risk-related control activities. Appropriate control procedures here, with an emphasis on an organization's IT processes and risks, are discussed in greater detail in Chapter 11.
- *Physical controls.* Many risk-related events involve physical assets such as equipment, inventories, securities, and physical plants. Whether it is physical inventories, inspections, or plant security procedures, an organization should install appropriate risk-based physical control activity procedures.
- *Performance indicators.* The typical modern organization today employs a wide range of financial and operational reporting tools. Many of these tools can be used as is or modified to support risk event–related performance reporting. In many instances, an organization's overall performance tools can be modified to support this important control activity component.
- *Segregation of duties.* This is a classic control activity, whether for business process internal controls or for risk management. The person

who initiates certain actions should not be the same person who authorizes or approves those actions. This key internal control activity is important, whether it be in a smaller business unit where an employee's supervisor would be required to inspect and approve employee actions or with a CEO who should obtain the oversight approval of the board of directors.

While the above are highlighted in the COSO ERM guidance materials, these control activities can be expanded to cover other key areas. Some will be specific to individual units within the organization, but each of them, singly and collectively, should be important components of supporting the organization's ERM framework.

Information and Communication

Although described as a separate component in the Exhibit 3.1 COSO ERM framework diagram, the component of information and communication is less a separate set of risk-related processes than a set of tools and processes linking other COSO ERM components. Rather than a separate horizontal level in both COSO ERM and its internal control framework, when the very first draft versions of COSO internal controls were released, the information and communications component was illustrated not as a separate horizontal-level component but as an on-the-edge component covering multiple other levels. The information and communication component of COSO ERM is the process or unit of the framework that links together each of the other components. This concept, also shown in the COSO application techniques materials, is illustrated in Exhibit 3.13, showing the information flows across the COSO ERM components. For example, the risk response component received residual and inherent risk inputs from the risk assessment component as well as risk tolerance support from the objective-setting component. ERM risk response then provided risk response and risk portfolio data to control activities as well as risk response feedback to the risk assessment component. Standing alone, the monitoring component does not have any direct information connections but has overall responsibility for reviewing all of these functions.

While it is relatively easy to draw such a simple flow diagram of how information should be communicated from one COSO ERM component to another, this is often a far more complex process of linking various systems and information paths together than what is shown in this very-high-level

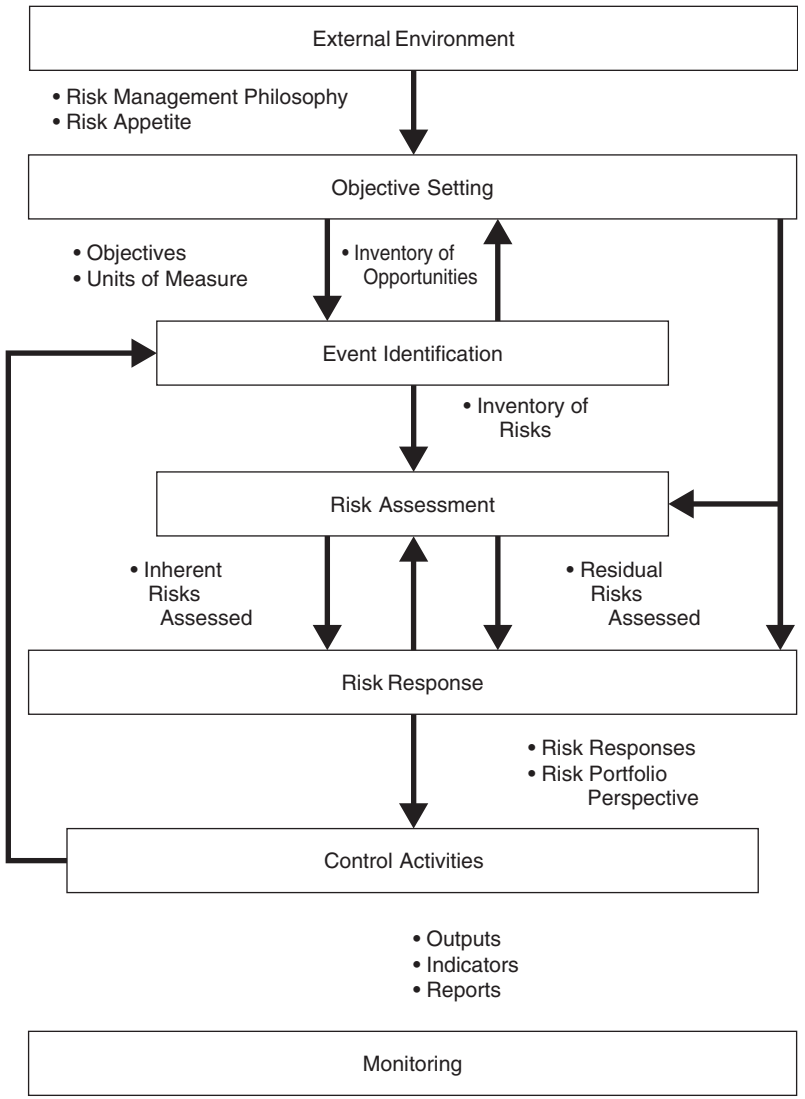

EXHIBIT 3.13 INFORMATION AND COMMUNICATION FLOWS ACROSS ERM COMPONENTS

Exhibit 3.13. Many organizations have a complex web of often not very well-linked information systems for their basic operational and financial processes. These linkages become even more complex with attempts to link various ERM processes, given that many basic organization applications do not directly lend them themselves to risk identification, assessment, and risk response–type processes. Some of these risk-monitoring functions can

be built into the comprehensive enterprise-wide applications, called enterprise resource planning (ERP systems), that are becoming increasingly common in larger organizations. Although more oriented to financial and operational areas, an ERP type of systems application could provide the basis for an organization's ERM information system.

Going beyond a comprehensive ERM information application for an organization, there is often a need to develop risk-monitoring and communications systems that links with customers, suppliers, and other stakeholders. While this was once a difficult process, today's wide use of Web-based databases with external information and the cooperative attitude of many suppliers and customers in larger organizations makes these information linkages more reasonable at present.

While the information half of the information and communication COSO ERM component is normally thought of in terms of IT strategic and operational information systems, ERM communication is the second aspect of this component. COSO ERM also talks about communication beyond just IT applications such as the need for an organization to establish some strong internal communication mechanisms to make certain that all stakeholders receive messages regarding the organization's interest in managing its risks and communicating appropriate levels of information to stakeholders. A major component of these messages is to introduce a common risk language throughout the enterprise as well as the roles and responsibilities of all stakeholders regarding their role in ERM. An appropriate place to introduce these issues may be in conjunction with SOx compliance efforts, as discussed in Chapter 7, or through the Chapter 12 discussion on establishing a risk management culture throughout the organization.

An enterprise risk initiative will be of little value to an organization unless the overall message of the importance of the ERM initiative gets communicated to all organization stakeholders. This should be in the form of a message from the CEO type of letter or other steps to build an effective risk culture as discussed in Chapter 12. The idea is to communicate the message about the importance of ERM throughout the organization. These types of messages are particularly valuable when an organization wants to deliver a message, for example, that all stakeholders should be very cautious regarding taking on certain potentially risky ventures. The process is more difficult if the organization wants to communicate that some factors should let go a little and occasionally accept some risks. An incorrectly interpreted message can effectively open the floodgates in inappropriate, risky decisions and ventures.

Monitoring

Placed at the base of the stack of horizontal components in the ERM framework model, the monitoring component is necessary to determine that all components of an installed ERM continue to work effectively. People in the organization change as well as do supporting processes and both internal and external conditions. In order for all members of the organization to have a level of assurance that the installed ERM is working effectively on a continuous basis, ERM monitoring processes should be installed and activated. This often takes place either by installing ongoing monitoring activities or through a series of separate evaluations covering various aspects of the ERM process. An organization may want to install ongoing monitoring for some critical areas and conduct special reviews of ERM processes.

Ongoing and continuous monitoring processes can be an effective method to flag exceptions or violations in some aspects of the overall ERM process. An accounts receivable billing function may provide some overall financial and operational risks if customer bills are not paid on a timely basis. An ongoing—almost real-time—credit collections monitoring tool could provide senior management with other day-to-day and trending data on the status of collections. There are many mechanisms to provide this kind of information to management, and the dashboard reporting shown in Exhibit 3.9 is that sort of risk-monitoring tool. These are automatic reporting devices, not unlike a low oil pressure warning light on an automobile dashboard, that monitor the status of certain enterprise risk controls and send warnings when necessary. These types of monitors often are difficult to install for the entire organization, but can work quite well on a process or departmental unit basis.

Going beyond monitoring through the use of dashboard tools and the like, organization management at various levels should take an overall responsibility for ERM monitoring. Management at all levels monitors an organization's operational and financial performance as part of their basic duty as managers. In order to establish an effective ERM framework, that monitoring should be expanded to include ongoing reviews of the overall ERM process, ranging from identified objectives to the progress of ongoing ERM control activities. The COSO ERM application framework document suggests this monitoring could include the following types of activities:

- Implementation of a strong and ongoing management reporting mechanism such as cash positions, unit sales, and other key financial and operational data. A well-organized organization should not have to wait until fiscal month end or worse for these types of operational

and financial status reports. Reporting tools should be expanded to include key ERM measures. This type of flash reporting should take place at all appropriate levels of the organization.

- Periodic reporting processes should be installed to specifically monitor key aspects of established risk criteria. These might include such things as acceptable error rates or items held in suspense. Rather than just reporting periodic statistics, such reporting should emphasize statistical trends and comparisons with prior periods as well as with other industry sectors. This type of reporting will highlight potential risk-related alerts.
- The current and periodic status of risk-related findings and recommendations from internal and external audit reports. This periodic reporting should include the status of ERM-related SOx identified gaps.
- Updated risk-related information from sources such as government revised regulations, industry trends, and general economic news. Again, this type of economic and operational reporting should be available for managers at all levels. That same information reporting should be expanded to include ERM issues as well.

Separate or individual evaluation monitoring refers to detailed reviews of individual risk processes by a qualified reviewer, such as a corporate risk management group or an internal audit function. Here, the review can be limited to specific areas or cover the entire ERM process for an organizational unit. In this latter type of review, qualified outside consultants may be hired to assess the effectiveness of ERM in the entire organization. However, for many organizations, a strong risk assessment group or an internal audit organization may be the best internal source to perform such specific ERM reviews. Of course, internal audit is an independent function in an organization, reporting to the audit committee of the board, and responsible for planning and scheduling its own internal audit reviews. A division controller, for example, cannot just go to internal audit and request that they perform an ERM review of that division' operations. An effective internal audit function will normally have many other review activities on its plate, and any review would need to be coordinated with other planned internal audit activities. The role of internal audit in the ERM process and with monitoring, in particular, is discussed in Chapter 9. The establishment of an overall enterprise risk management function is discussed in Chapter 12.

Whether it is internal audit, a risk management team under a chief risk officer (CRO), outside consultants, or other trained staff from within the

organization, any specific individual reviews of an ERM process might use the following tools:

- *Process flowcharting.* As part of any identified ERM process, the parties responsible should have developed flowcharts documenting that process. If not for any other reason, such flowcharts would have been developed as part of their SOx Section 404 review work. These same process flowcharts can be very useful in completing an ERM review of an individual process. This requires looking at the documentation prepared for a process, determining if the process documentation is correct given current conditions, and updating the process flowcharts as appropriate. This update should determine if those identified risks still appear appropriate and if risks have been identified appropriately.
- *Reviews of risk and control materials.* An ERM process often results in a large volume of guidance materials, documented procedures, report formats, and the like. There is often value to review the risk and control materials from an effectiveness perspective. A dedicated ERM team, internal audit, or the organization's quality assurance function can perform such reviews.
- *Benchmarking.* Although an often misused term, benchmarking here is the process of looking at the ERM functions in other enterprises to assess their operations and to develop an approach based on the best practices of others. Gathering such comparative information is often a difficult task, as competing organizations are often reluctant to share competitive data. The process works best when one-to-one professional contacts can be developed, but information regarding how others have attempted to solve similar problems is often very valuable.
- *Questionnaires.* A good method for gathering information from a wide range of people, questionnaires can be sent out to designated stakeholders with requests for specific information. This is a valuable technique for monitoring when the respondents are scattered geographically, such as a risk-monitoring survey of employees in a nationwide retail organization.
- *Facilitated sessions.* Valuable information can often be gathered by asking selected people to participate in a focus group session led by a skilled conference leader. This is the approach used by many organizations for gathering market research information through what are called focus groups. This same general approach can be used to

gather a team of people—often from different positions in the organization—to review the enterprise risk status of a particular area. People with different responsibilities can often work together to provide some good information about the risk-related status of selected activities.

The purpose of this monitoring process is to assess how well the ERM framework is functioning in an organization. Deficiencies should be regularly reported to the managers responsible for enterprise risks in the specific area monitored as well as to the ERM or risk management office. The roles and responsibilities of the CRO and steps to building an effective risk management program in an organization management office are discussed in Chapter 5. The concept behind this monitoring is not just to find faults or deficiencies but to identify areas where the ERM framework can be improved. For example, if some event monitoring work points to areas where a function is assuming excessive levels of risk, processes need to be in place to install corrective actions.

OTHER DIMENSIONS OF THE ERM FRAMEWORK

As discussed at the beginning of this chapter and described in Exhibit 3.1**,** COSO ERM is a three-dimensional framework with its eight categories as one dimension in the sections just discussed. The other dimensions are its four objective categories represented by its vertical columns and its entity and units described in the third dimension. While the eight categories just described are very important to understanding and using COSO ERM, those other two dimensions of its strategies and organizational units are important as well. To understand the risks surrounding an organizational objective, one must evaluate that risk in terms of, possibly, the reporting concerns associated with that risk and the specific organizational unit that becomes the main focus of the risk.

COSO ERM needs to be understood from all three of these ERM framework dimensions. This chapter has discussed COSO ERM's eight key components in one dimension, while Chapter 4 discusses the other two dimensions of COSO ERM—the objective categories and the entity or unit dimensions. Chapter 4 also discusses some applications of the use of COSO ERM in several organizational environments.

To repeat and reaffirm our comments of Chapter 1, an effective ERM process, no matter how well designed and operated, provides only reasonable—but not positive—assurance that the organization will achieve its

risk-related objectives within management's established philosophy and appetite for risk. However, no matter how well an ERM is designed and managed, there can be failures due to human errors of any of a wide range of unexpected events.

NOTES

1. There are numerous references to this December 2004 devastating tsunami. A physical description can be found at *www.ruesges.com*.
2. "Bringing ERM Into Focus," *Internal Auditor,* June 1, 2003.
3. A full copy of COSO ERM or some supporting summary material can either be downloaded or purchased through the AICPA or the COSO Web site at www.coso.org.
4. This credo can still be found on the Johnson & Johnson Web site at www.jnj.com/our_company/our_credo/index.htm.
5. "Boeing Board Ousts Chief, Citing Relationship with Executive," *New York Times*, December 7, 2005.
6. Enterprise Risk Management—Integrated Framework: Executive Summary. New York: COSO, September 2004.
7. For more information, see the previously referenced COSO ERM application techniques materials or visit the Web site of the Project Management Institute (PMI) special interest group on risk, www.risksig.com.
8. For more information on Section 404 internal control reviews, see Robert Moeller, *Sarbanes-Oxley and the New Internal Auditing Rules.* Hoboken, NJ: John Wiley & Sons, 2003.

4

COSO ERM Organizational Objectives

This chapter discusses the other two dimensions of the Committee of Sponsoring Organizations' enterprise risk management (COSO ERM) framework: its objective categories and the business unit through entity-level risks in the framework. The discussion here covers the other two dimensions of the COSO ERM framework in conjunction with the internal environment through monitoring risk components described in Chapter 3 and the ERM framework diagram shown in Exhibit 3.1. This chapter will again reference our hypothetical example company, Global Computer Products, which was introduced in Chapter 3. A basic concept behind COSO ERM is that enterprise management, at all levels, should take a portfolio view of risk—how the various individual risks that a unit manager or the overall organization may face will interrelate with other risks impacting the organization.

An understanding of this overall COSO ERM framework should help managers at any level in the organization to better understand, accept, or manage the various risks they face in the course of day-to-day operations. For example, an organization launching a new product line should recognize all of the risks

associated with that product line launch in terms of all three dimensions of the COSO ERM framework.

ERM RISK OBJECTIVE CATEGORIES

Chapter 3 introduced eight COSO ERM components, ranging from the internal environment to risk monitoring. Each component was discussed in terms of its relationships with other component categories. For example, as shown in Exhibit 3.13, the risk assessment process receives an inventory of risks from risk identification as well as risk tolerance guidance from the objective-setting component and risk response inputs. Using these inputs, risk assessment provides data and information on inherent and residual risks for help in a risk response process. Of course, this is not a simple process where materials will move from one output box directly to another input slot. Rather, this is a continuous process where these component outputs are only some of the input factors that should be considered when accepting and managing risks through a subsequent component. Each of these risk components should also be considered and managed in terms of their strategic, operational, reporting, and compliance-related risks. Overall consideration of these various strategic risk objectives becomes the second important dimension of the three-dimensioned COSO ERM framework. A message that will be repeated here and throughout this book is that a manager should always consider and act upon enterprise risks in terms of the individual identified risk as well as with respect to all other dimensions of this COSO ERM framework.

ERM Strategic Risks

Every organization, whether a major corporation, a small business, or a not-for-profit entity, should have some level of a strategic vision or plan. Sometimes, these appear in a formal statement of long-range vision published in the annual report or just in the words of the chief executive officer (CEO) in comments to various stakeholders. In other instances, this strategic vision may be little more than the plans of a smaller operating unit to continue doing things in the same manner as at the present, and for a troubled enterprise that vision objective may be only to hopefully stay in business for the next period! In all cases, the entity faces the risk of not achieving these strategic objectives as planned.

Very much a part of the internal environment component of the ERM framework, an organization's strategic objectives should be an important consideration for all ERM-related activities. For example, if an enterprise had a high-level objective to become number one in total worldwide revenues in its industry class, that strategic objective should be reflected in all components and entity levels within the ERM framework. The internal environment component would try to define a risk appetite and management philosophy that would encourage that growth by perhaps accepting higher-risk ventures. That same high-level objective also should be reflected throughout the ERM framework. The COSO ERM component of risk responses would emphasize activities that would enhance that planned growth, while control activities would emphasize top-level reviews and reporting mechanisms to help the organization achieve this high-level strategic objective.

There should always be a hierarchy of these strategic objectives. A strategic plan or vision, typically communicated by the CEO, should serve as a guide to other units within an organization. If, because of various political pressures, senior management has a stated objective to stop doing business in some area of the world or to drop some marketing approach, an operating unit should not ignore these high-level goals and continue operating in a "business as usual" manner. Effective communication is critical here, assuming that everyone will understand the "tone at the top" type of message. Processes such as management reporting requirements or a good program of internal audits should highlight any unit that does not seem to be "getting the message" regarding these high-level strategic objectives. Any organization, of course, should have more than just one high-level strategic objective. Their single major objectives should be combined with others to allow the enterprise to grow and prosper. An objective to be the best in some class of activities must be combined with various sub-objectives to make that high-level objective more achievable. These same strategic risk objectives should also be communicated to all units or levels within the enterprise.

The ability to achieve COSO ERM strategic-level risks is a major determinant in assessing the overall effectiveness of the organization's ERM processes. The type and extent of these objectives says much about an organization's appetite for risk, as discussed in Chapter 3. COSO ERM is based on the concept of reviewing the portfolio of the differing risks that may impact an organization. While this varying assortment or bundle of risks will be blended and customized, the strategic objective can have a high priority over many other matters. That previously referenced enterprise objective to become number one in total revenues in an industry class can have a major influence on risk-related decisions throughout the organization.

In the context of the three-dimensional COSO ERM framework, this component of strategic risk should have an influence on all components, from the internal environment and objective setting down to monitoring. Similarly, every unit or element of the organization should be aware of these often big-picture strategic risks. Managers at all levels should consider how their planned actions will impact and can interface with defined and communicated ERM strategic risks.

Operations-Level Risks

While the Exhibit 3.1 COSO ERM framework diagram shows each of the objective categories as having the same relative size or width on that diagram, the category of operations-level risks is often viewed as a much broader and higher-exposure risk category than the other three. The objective of operations-level risks refers to the wide number and often differing types of special risks that can impact any area of organization operations. The ERM framework suggests that an organization should develop and document a general set of its operational risks along with related risk likelihood estimates. This operations-level risk estimate is very similar to the objective-setting component of ERM discussed in Chapter 3. The difference is that risks identified through objective setting are often very broad and may tie in with concerns to meet high-level corporate objectives, with potential legal compliance risks as well as general operations risks. The ERM operations-level risk objective calls for a set of identified risks for each unit or component of the organization.

Exhibit 4.1 provides examples of operational risks for a manufacturing organization, using our Global Computer Products example company. While it may be relatively easy to meet with the board and CEO to document high-level strategic risks or to work with the chief financial officer (CFO) and internal audit for some compliance-level risks, the identification of operations-level risks often requires a fair degree of detailed information gathering and analysis. This is particularly true for a larger organization operating in multiple geographic areas or product lines. The direct managers of these multiple units usually have the best understanding of their unit's operational risks, even though that information can become lost when consolidated for higher-level reporting. In order to gather more detailed background information on potential operational risks, the organization's chief risk officer (CRO), the risk management office, or a group such as internal audit should circulate an operational risk awareness survey. Again using Global Computer Products, Exhibit 4.2 is a survey covering

one of the operational risks described in Exhibit 4.1, risk 2 on information security. The idea here is to take these high-level operational risks and direct "on-the-floor" members of the organization to better describe the nature of these risks. This type of survey, along with follow-up questions, will allow the development of a consistent set of cataloged operational risks across all levels of the enterprise. The questions asked here would be similar to the types of detailed questions often used in internal audit internal control assessments, and the results of any available data here could become a basis for developing better understanding.

---

1. *Organization and management-related risks*. Global Computer Products' organization and management structure, in its different activities, is constantly assessed for potential risks. This is to enable efficient and competent organization, and to avoid such risks as unsuitable recruits, lack of training, and excessive rotation of personnel.
2. *Information security risks*. Global Computer Products' activities are dependent on external, internal, and embedded information technology (IT) services and solutions. The enterprise aims at using reliable IT solutions and information security administration to avoid exposure to data loss, lack of data confidentiality, availability, or integrity. Severe disruptions in global service availability or lack of confidentiality of critical business information may have negative effects on Global Computer Products' business.
3. *Production, process, and productivity risks*. In order to maintain safe and productive production, Global Computer Products utilizes ISO 9001 and other similar procedures in its main production units. The enterprise develops product-specific safety manuals, risk assessments, and environmental evaluations, and highlights cooperation with customers. Although these issues have been evaluated to present low risks to the company, severe interruption in key production areas may have adverse effects on Global Computer Products' business.
4. *Profitability operational risks*. One of Global Computer Products' key targets is to operate as a profitable business. There is a risk, however, that the actual costs of transactions cannot be initially estimated accurately, and it is not always possible to determine correct transaction prices or to assess whether the market price level, due to competitiveness factors, are sufficient. To manage pricing risks, Global Computer Products' businesses apply various quality systems, operating guidelines, and profitability analyses that consider, among other things, the product to be sold, the customer, and the payment terms.

EXHIBIT 4.1 MANUFACTURING ORGANIZATION OPERATIONAL RISKS: GLOBAL COMPUTER PRODUCTS

5. *Business interruption risks*. Risks related to the management of software and materials, suppliers, and subcontractors can be significant, and delivery problems can influence the price and availability of materials used in Global Computer Products or can cause disruptions in deliveries to customers.

   The organization is also very dependent on a wide range of IT and telecommunications systems, many expected to be operational on a 24/7 basis. While these processes are supported by strong and effective business continuity plans, any failure of these plans to operate during a business interruption can cause a severe risk to operations.

6. *Project activity risks*. Global Computer Products' operations consist of many new or custom-tailored products, where deliveries can involve project-specific risks concerning delivery schedules as well as equipment start-up, capacity, and end-product quality. In addition, risks may also arise from new technology included in these deliveries. While the risks of individual projects are generally not significant compared to the entire scope of the Global Computer Products' business, the aim is to reduce project-specific risks by assessing risk potential already at the offer stage and by preparing for risks through the use of detailed terms and conditions in sales contracts and through quality management.

7. *Contract and product liability risks*. Global Computer Products is occasionally involved in product liability claims typical for companies in comparable industries. The aim is to minimize product liability risks by improving product safety through research-and-development investments, automation, and customer training, and by detailed sales contract terms. Although the insurance coverage is currently estimated as adequate to cover normal liability risks, Global Computer Products may be held responsible for damages beyond the scope of the insurance coverage.

8. *Crisis situations*. While Global Computer Products has developed an ability to deal with different crisis situations through a flexible crisis and incident management organization, the main goal of major crisis management is to secure personnel. Since Global Computer Products' own resources are limited, and possible global catastrophes may exceed the ability to adequately respond to the threat, Global Computer Products has identified the limits of its crisis management capacity, and uses external consultants for advice on crisis situations like natural catastrophes that may have adverse effects on personnel and business.

EXHIBIT 4.1 MANUFACTURING ORGANIZATION OPERATIONAL RISKS: GLOBAL COMPUTER PRODUCTS *(CONTINUED)*

9. *Illegal acts*. Illegal acts may be a threat to Global Computer Products' activities. To prevent the possibility of illegal acts such as fraud, misconduct, and crime, Global Computer Products promotes its values and ethical principles as part of personnel training. Internal procedures, controls, audits, and practical tools like "whistleblower" processes are used to reduce the possible risk exposure. The magnitude of exposure is considered to be low, but even limited illegal acts may have adverse effects on Global Computer Products' results and reputation.

EXHIBIT 4.1 MANUFACTURING ORGANIZATION OPERATIONAL RISKS: GLOBAL COMPUTER PRODUCTS *(CONTINUED)*

Circulated through all levels of an organization, with a message encouraging stakeholders to respond in a candid manner, these types of surveys can often gather important information regarding potential risks at a detailed operational level. These types of organization-wide surveys are

This survey example is based on one of the operational control risks identified in Exhibit 4.1. The idea is to take these management-identified risks and gather more information about the extent of each of these risks through detailed operating unit surveys. The compiled results will provide a better understanding of overall unit risk environments.

Risk 2. Information security risks.

Global Computer Products Operating Unit: _____ Date Prepared: _____

a. Does the operating unit have effective information security standards and procedures, and are they consistent with corporate standards?

b. Are there strong password and other controls in place to restrict unauthorized access attempts?

c. Are unauthorized access attempts regularly monitored?

d. Are firewalls and other network security perimeter controls established and operating effectively?

e. Has internal audit or another appropriate Global Computer Products unit assessed detailed information security risks, and have appropriate corrective actions been implemented?

f. Has the operating unit experienced any information security violations over the past 12 months, and have corrective actions been installed to remedy those risks?

EXHIBIT 4.2 OPERATIONAL RISK AWARENESS SURVEY

also similar to the type of survey an enterprise might use to launch an organization-wide ethics function. A manager of a remote operating plant may not have adequately communicated or have not had direct management hearing concerns about some plant-level operational risk. A broadly based and confidential survey will allow people to communicate those often local-level operational risks up through the enterprise.

With ERM's portfolio view of risks, an organization can face a level of danger if it regularly rolls things up to a summary level, missing or rounding off its lower-level risks. Whatever the level in an organizational hierarchy or the geographic location, a message should be communicated to managers at all levels that they are responsible for accepting and managing their risks within their own operational units. Too often, unit managers may gain an impression that risk management is only some senior-level, headquarters type of concern. The importance and concepts of COSO ERM and operations risk management should be communicated to all levels of an organization.

Reporting Risks

This risk objective covers the reliability of an organization's reporting, including both the internal and external reporting of financial and nonfinancial data. Accurate reporting is critical to organization success in many areas or dimensions. While we frequently see news regarding the discovery of inaccurate corporate financial reporting and the resultant financial repercussions for the offending officers or entity, that same inaccurate reporting can cause problems for organizations in other areas. An example of the risks related to inaccurate reporting can be found with a recent problem with the major petroleum company, Royal Dutch Shell. Not an actual financial number, oil and gas exploration companies are required to regularly report their reserves, the amount of oil and gas on their properties that are still in the ground and have not yet extracted. In January 2004, Royal Dutch announced that due to bad estimates and sloppy record keeping, they had been significantly overreporting their estimated petroleum reserves. They subsequently reported another reserve estimate error in May of that same year. While this error did not affect their reported financial results and Securities and Exchange Commission (SEC) guidelines are not that strong in this area, the market battered their stock upon the announcement, and the CEO, the head of oil exploration operations, and others were forced to resign. The company, under a new chairman, then announced a raft of changes and internal control improvements to repair the damage.

No matter what its industry or line of business, every enterprise faces some major risks with the potential of inaccurate reporting at any unit or area. The operating unit must make certain that numbers are correct before they are reported to corporate headquarters, and consolidated numbers must be accurate, whether financial reports, tax returns, or any of a myriad of other areas. Systems and processes installed as part of the internal environment should ensure accurate reporting, and established as components of the event identification and risk assessment components of the ERM framework. The objective of accurate reporting should be a major driver in all ERM activities.

While good internal controls are necessary to ensure accurate reporting, ERM is concerned about the risk of authorizing and releasing inaccurate reports. While strong internal controls should minimize the risk of errors, an organization should always consider the risks associated with inaccurate reporting. While we do not have all of the details in the matter, Royal Dutch Shell could be an example of this risk area. Reporting reserves requires a management estimate following the SEC's three categories—proved reserves, proved developed reserves, and proved undeveloped reserves. Small errors and discrepancies can be ignored over time until there is a major error that needs to be disclosed. The risk of inaccurate financial reporting should be a concern at all levels of the organization.

Legal and Regulatory Compliance Risks

Organizations of any nature operate in environments where they must comply with a wide range of government-imposed or industry regulations. In addition, they are always subject to any of a wide variety of legal risks. While compliance rules and risks can be monitored and recognized in many instances, legal risks are sometimes totally unanticipated. In the United States, for example, an aggressive plaintiff legal system can pose a major risk to otherwise well-intentioned organizations. Asbestos litigation in the United States during the 1990s and beyond is an example. A fibrous mineral, asbestos has three extraordinary characteristics: It works as an insulator for heat and electricity; it resists chemical corrosion; and, when inhaled, it has now been found to cause cancer and other illnesses that can take decades to develop.

A natural insulation material, previously used extensively in construction building materials and considered totally benign, it has been subsequently found that too much direct contact with asbestos fibers over time can cause severe lung problems and even death. Miners working underground and extracting asbestos have met that fate. Extracted asbestos was

used in many other products, such as sealed wrappers to insulate heating pipes or fire protection wall barriers. Here, the risks to persons working or living in a structure with these asbestos-sealed pipes are often very minimal. Nevertheless, aggressive litigators have brought actions against corporations, claiming that anyone who could have had any contact, no matter how minimal, with a product that used asbestos could be at risk sometime in the future. The result was litigation damage claims against companies who had manufactured products containing some asbestos, calling for damages for potential human risks in future years. Because of huge damage awards, virtually all major corporations that once used asbestos have gone bankrupt; are now out of business or have had to pay huge court-imposed damage losses. This is the type of legal risk that is very difficult to anticipate but that can be disastrous to an organization.

COSO ERM recommends that compliance-related risks be considered for each of the risk framework components, whether in the context of the internal environment, objective setting, or risk monitoring, as well as across the organization. The ERM guidance material does not offer much additional material on this compliance objective other than to state that this objective refers to conformance with applicable laws and regulations. These are important elements of the risk management framework that need to be communicated and understood.

Understanding Regulatory Compliance Risks. As organizations become more interconnected on a worldwide basis and as our laws frequently become ever-more complex sets of rules, all organizations face a wide range of regulatory rules. The number and extent of these is very broad, with some impacting virtually all organizations and others related to only single business units of an enterprise in a specialized industry sector. The nature of those compliance risks needs to be communicated and understood through all levels of an organization. This is also an area where an enterprise may accept a certain level of risk in terms of its concerns regarding legal compliance. We are not suggesting that an organization should deliberately ignore a major law because of a feeling they never will be caught, but they should always take a reasoned approach to risks in conjunction with their overall philosophy and risk appetites. For example, many regulatory rules specify that all expenditures must be supported by a receipt. While there usually are no reasonableness guidelines, one organization may decide that "all expenditures" may go down to an employee travel expenses of less than $1.00, while another will require receipts of anything above $25.00. The latter organization has made a

decision that the costs of documenting these small expenditures is greater than any penalty it might receive if caught in a regulatory compliance issue. When an organization establishes such guidelines, it should be communicated to all levels and units.

In order to manage and comply with these many regulatory risk requirements, an enterprise needs to have an understanding of the nature and extent of all of the regulatory risks it faces and the organization's overall position on each. This is an area where information is often lacking within an organizational unit. The board of directors and senior management needs to have information on these key regulatory risk areas and how the organizational unit has taken action. A sample regulatory risks status report, as shown in Exhibit 4.3, provides information regarding some of the various legal regulatory risks facing an organization. This report covers our hypothetical Global Computer Products organization and shows just a few of the many risks ranging from major to minor. In a different industry such as pharmaceuticals it almost certainly will cover a different set of risks. The problem here is that regulatory risks are never "minor" when an organization is found to be in violation of one or another of them. Any can have a variety of consequences ranging from legal actions to just negative publicity.

This type of risk compliance status document becomes an action status report that would be circulated to various operating units to indicate the status of any specific regulatory risks as well as to provide information on the current status of risks to the board of directors and senior management. The risk management office, as will be described in Chapter 5, is an appropriate group to circulate such a report, to ask questions and follow up on status. If such a risk management office or CRO function has not been established, another organizational unit such as internal audit could take responsibility for maintaining the status here.

The idea behind this status report is to provide an overall synopsis of compliance with various regulatory risks. This is a report to recognize where there are unit-level Sarbanes-Oxley (SOx) internal control deficiencies yet to be corrected or to highlight an objective in place to bring the group in compliance with an International Organization for Standardization (ISO) standard or some other measure.

Organization Legal Risks. While the status of regulatory compliance risks is relatively easy to monitor through something along the lines of the

Note: This report summarizes examples of some of the many rules and requirements impacting an enterprise such as Global Computer Products. The organization risks being in violation of many of these example rules.

1. **Equal Employment Opportunity Commission Employer Information Report (EEO-1) rules.**

   Rule Summary: The Company must file an employer information report (EEO-1) annually regarding employees and their demographics.

   Current Status: Reports have been filed on schedule, but offshore operations have experienced problems with reporting on occupational categories and this data must be aggregated.

2. **Environmental Protection Agency Export Notification Requirements.**

   Rule Summary: Global Computer Products is required to notify the Environmental Protection Agency (EPA) when exporting substances or products that contain chemicals listed on the Export Notification 12(b) list under the Toxic Substances Control Act (TSCA); 15 U.S.C. s/s 2601 et seq. Since current rules do not have a low-level cutoff, many minor substances or product ingredients trigger large amounts of paperwork.

   Current Status: Rules are difficult to understand, and the company may be out of compliance even though the level of export business here is very low.

3. **EPS Pretreatment Streamlining Rule under Clean Water Act; 33 U.S.C. ss/1251**

   Rule Summary: A 1999 EPA rule defines pretreatment requirements to remove unnecessary burdens on Publicly Owned Treatment Works (POTWs), industry, and agencies.

   Current Status: May be out of compliance at some facilities. This rule should be finalized because it reduces burdens on POTWs without negatively impacting the environment.

4. **Health Insurance Portability and Accountability Act of 1996 (HIPAA)**

   Rule Summary: HIPAA rules are intended to improve portability and continuity of health insurance coverage for all Global Computer Products employees, and to simplify the administration of health insurance. Implementation of HIPAA has been problematic because of multiple effective dates and the need to reengineer existing processes to eliminate or reduce exposure.

   Current Status: Considerable time and money have been spent trying to comply with these complex requirements, and the company may still be technically out of compliance.

EXHIBIT 4.3 KEY REGULATORY RISKS STATUS REPORT: GLOBAL COMPUTER PRODUCTS

Exhibit 4.3 sample report, monitoring legal risks is often a greater challenge. As an example of organization legal risks, in 1963 Crown Cork and Seal, an old-line Philadelphia-based packaging company, purchased a cork company, Mundet Cork, which had an insulation business that made one product that, many years ago, contained asbestos. Prior to this acquisition, Mundet had manufactured products containing asbestos, but it ceased doing so long *before* its acquisition. Crown acquired Mundet in order to take over Mundet's metal bottle-cap production division.

On the basis of that acquisition, Crown became the target of thousands of tort claims filed by individuals who claimed to have been "injured" by exposure to the Mundet insulation products containing asbestos. Those suits drove Crown itself to the verge of bankruptcy with cash flow costs as high as $90 million in one year. Crown survived as a much different and much reduced organization because of all of this.

The point here is not to discuss the many problems in the United States associated with asbestos litigation, but to mention the types of legal risks that can very much impact an organization. There are many litigation risks that are unanticipated and difficult to control.

A corporate legal counsel can often play an important role here by circulating legal risk status data to all members of the organization and serving as a sounding board for reviewing newer legal risk–related questions. While corporate legal functions are too often involved with day-to-day litigation and advising the board of directors, they should become more of an internal consulting function providing some guidance on the relative legal risks surrounding some proposed new move or venture. This type of background reporting information on legal issues may help managers at all levels to assess any new potential risks when seeking to make a decision.

Legal and regulatory compliance objectives are important elements in any organization's COSO ERM framework. The current status of issues as well as any actions to be taken will help to define and shape the organization's overall appetite for risk. Whether considering risk event identification or risk control activities on a total enterprise level or within an individual unit, legal and regulatory actions play a major role in understanding and accepting enterprise risk.

These various organization, compliance, and reporting risks form another dimension to the COSO ERM framework. All of the risk elements included in the framework should be evaluated in terms of this dimension of the COSO ERM framework. For example, no matter what the level of risk or the organizational unit, a manager should consider whether there are any legal or regulatory risks related to the matter being considered.

COSO ERM ENTITY- AND UNIT-LEVEL RISKS

The third dimension of the COSO ERM framework says that risks should be considered on an organization or entity unit level. The Exhibit 3.1 COSO ERM framework shows four divisions or slices in this dimension of the model: entity-level, division, business unit, and subsidiary risks. This is not a proscribed division, and ERM suggests that risks be considered at all significant organization levels. This division often closely follows the official organization chart. Again in consideration of the ERM portfolio view of risk management, risks should be identified and managed within each significant organizational unit. Our discussion here will include the consideration of risks on an entity-wide basis and risks for individual business units.

An enterprise with four major operating divisions and with multiple businesses or subsidiary units under each would have an ERM framework that reflected all of these significant business units. While these risks are important on an overall organizational level, there should be a level of consideration on a unit-by-unit basis to as low of a level as necessary to allow the organization to understand and manage its risks. COSO ERM does not specify how thinly these unit-level risks should be sliced, and the criticality and materiality of individual business units should be given consideration. For a major fast-food restaurant chain with thousands of individual units, it almost certainly would not be reasonable to include each of these multiple units as a separate component in the risk model. Rather, management should define its organizational-level risks at a level of detail that will cover all significant, manageable risks.

Risks Encompassing the Entire Organization

Multiple business unit-level risks will roll up to a set of entity-level risks. While it is easy for an organization to consider some unit-level risks–using public accounting terminology as being "not material"–an organization has to think of all risks as potentially significant. For example, an enterprise can have a relatively small subsidiary in a "third-world" country that is manufacturing fairly low-level casual clothing goods. Often, such a unit would be so small in terms of corporate revenue contributions or in terms of its relative size, that it can slip "under the radar screen" on a senior corporate level. However, there could be issues regarding child labor at that host country that could bring all operations there to the attention of any of several aggressive journalists. As a result of news articles, the organization may soon find itself at the center of attention regarding this small subsidiary operation. Such a situation often results in cases where a CEO is asked

to publicly comment on policies and procedures at that subsidiary operation even though the CEO may only vaguely know of its existence.

Our point here is that both major as well as seemingly small risks can impact an entire enterprise. The delivery of tainted food produced at one small unit of a large fast-food chain can impact the prospects and reputation of the total organization. While it is relatively easy to identify high-level entity-wide risks such as compliance with SOx Section 404 (discussed in Chapter 7), and to identify and monitor these as part of the COSO ERM process, care must be taken that smaller potential risks do not "slip between the cracks." As risks are identified through the operations objective, described previously, or through organization-wide objective setting, these risks should be considered on a total entity-level basis.

The COSO ERM framework suggests that risks should be considered on an entity-wide basis as well as by individual operating units. Those individual operating or business unit risks should be reviewed and consolidated on an overall basis by the organization to identify key risks that may impact the overall organization. In addition, a series of organization-wide risks should be identified. These pages have talked about entity-wide risk identification in several places or dimensions in the COSO ERM framework:

- Identification of entity-wide risks through the ERM objective setting and event identification ERM categories.
- Identification of risks through COSO ERM objectives, with an emphasis on operations objectives.
- Consolidation of all of the unit-level risks into entity-level risks.

Each of these approaches should result in essentially the same list of key organization-wide risks. The ERM function should take inputs from each of those approaches and consolidate them in one board-level entity major risk report. This is the type of entity-level risk report that should receive the attention of senior management and the board of directors. An active CRO and an ERM function, as described in Chapter 5, would be responsible for maintaining this data. Although COSO ERM, with its multidimensional and portfolio approach to risk, may look at all potential risks, there is often a need for one consolidated status report to show total or outstanding enterprise risks.

Business Unit-Level Risks

Risks occur at all levels of a large organization, whether a major production division with multiple plants and thousands of employees or a small minority ownership position in a foreign country sales company. Risks must be

considered in each significant organizational unit. The risks that have been identified in the minority ownership position in a foreign country sales company are risks unique to that unit but then will roll up to another organizational unit, to the operating division, and then to the entity. We have cited the example of entity-level risks that might result from failures in manufacturing or human rights standards from a small subsidiary in a "third-world" country. Risk issues here can cause an embarrassment to the overall organization on an entity level, but they should have been controlled all the way down to the small "third-world" company unit.

Depending on the complexity of the organization and its number of operating units, enterprise risk responsibility should be divided among various responsible units in the organization. This can often best start as a push-down process where entity- or corporate-level management will formally outline their major risk-related concerns and ask responsible management at each of the major divisions to complete these surveys by passing them down to operating units within that division. By pushing this type of exercise down through the organization, significant risks can hopefully be identified at all levels and then managed where they can receive the most direct, local support.

An organization risk survey is an exercise that requires a great amount of education, learning, and communication throughout the enterprise. Exhibit 4.4 is an example of such a business unit risk survey document. The general format of this document has been adapted from COSO ERM published materials.[3] After some review and understanding of their risk management processes, individual business units would be asked to initially identify their key strategic, operational, reporting, and compliance risks, to estimate the probabilities and impacts of those risks, and then to monitor the ongoing status of those risks. The corporate ERM function can coordinate this process, but responsibility should be passed down to front-line management functions at all levels. Units would be asked to report periodically on the status of these identified local unit risks. These reports could be consolidated as they climb up through organizational levels, but the idea is to place a level of risk management responsibility at the most direct level in the organization.

PUTTING IT ALL TOGETHER

The COSO ERM framework has not been with us that long to point to a series of successful organizations that have publicly embraced this new model or standard. In addition, the term *risk management framework* has

RISK		Corp. Business Unit Contribution	Entity 1 Business Unit Contribution	Entity 3 Business Unit Contribution	Entity 1 Business Unit Contribution	Entity Earnings per Share
Decrease in local currency in relation to U.S. dollar by 0.01%	Impact	($1,000.00)	$600.00	$300.00	$100.00	$0.00
	Likelihood			20%		
An increase in interest rates greater than 0.5%	Impact	(750.00)	1600.00	800.00	100.00	(0.35)
	Likelihood			20%		
Increase in raw materials prices by greater than 10%	Impact		10000.00	5000.00	5000.00	(0.40)
	Likelihood		20%	30%	15%	
Pending union negotiations halt production for more than 10 days	Impact		5000.00	0.00	1000.00	0.12
	Likelihood		10%	0%	55%	

EXHIBIT 4.4 BUSINESS UNIT RISK SURVEY ANALYSIS

been used in other instances with poor or loose definitions. Some of these other risk frameworks focus narrowly on risk management in specific areas rather than the broader COSO ERM focus. Other risk frameworks cover specific industries or specific types of risk. In addition, many of these emphasize mechanisms for reducing—rather than managing—risk. In contrast, the COSO ERM framework described here and in Chapter 3 addresses ERM applicable to all industries and encompassing all types of risk. With its focus on recognizing an organization's appetite for risk and the need to apply risk management within the context of overall strategy setting, COSO ERM presents some fundamental differences from most risk models that have been used to date.

COSO ERM is designed to be applied to the total organization and to as many smaller supporting units as manageable. This is in contrast to many of the preexisting risk frameworks that stood by themselves, and thus tended to be implemented within silos or specific parts or functions of an organization. Consequently, earlier approaches to risk management may be done very well in one unit of an organization with little consideration of how actions of other parts of the organization affect specific risks or overall organization risks. COSO ERM presents an enterprise-wide perspective of risk and standardizes terms and concepts to promote effective implementation across the organization. We will be discussing the effective application of COSO ERM in the forthcoming chapters of the book, whether to understand risks within internal audit, the IT function, the corporate boardroom, or many other areas.

NOTES

1. See Robert Moeller, *Sarbanes-Oxley and the New Internal Auditing Rules,* Chapter 4. Hoboken, NJ: John Wiley & Sons, 2004.
2. "Reporting Problems at Shell," *The Guardian,* London, *www.ruesges.com,* March 24, 2004.
3. *Enterprise Risk Management—Integrated Framework, Applications Techniques*, COSO, September 2004.

5

Implementing an Effective ERM Program

In many enterprises today, the risk management department or function does not receive the respect it should deserve. Often just called the insurance department, risk management functions usually are not structured at a senior or "C-level" status in enterprise organization charts. A currently trendy term, *C-level* refers to a function headed by a very senior manager or officer-level person, such as a chief information officer (CIO) or chief audit executive (CAE). While perhaps not reporting directly to the CEO, C-level group heads often have a direct reporting relationship one level below the CEO—such as to the chief financial officer (CFO) or some other very senior manager. An effective risk management function here would be headed by a chief risk officer (CRO), an executive whose responsibility is to ascertain that enterprise risks are properly understood and translated into meaningful business requirements, objectives, and metrics. CROs were mentioned in Chapters 3 and 4, but their typical roles and responsibilities were not defined.

If an enterprise has a traditional "insurance department," the Committee of Sponsoring Organizations' enterprise risk management (COSO ERM) framework provides the enterprise with an excellent opportunity to reengineer its existing insurance-based risk management function along the lines of the COSO ERM framework or to create a separate new ERM function for the enterprise. Given a growing recognition of the importance of risk management in today's enterprise, an ERM function should operate at a higher level than the traditional insurance-based risk groups of the past that sometimes operated side by side with such facility support functions as property perimeter security and loss prevention. While these latter functions are important to an enterprise, the ERM department should take a higher and more prominent role.

This chapter considers how to establish an effective risk management function following the COSO ERM framework, and suggests duties and responsibilities for this important function as well as for its CRO leadership. We will also suggest potential reporting connections for the group as well as the appropriate levels and skills for the professionals who should manage the risk management function in today's enterprise. Although very much part of that risk management function, the chapter will provide insights on the roles and responsibilities of the CRO. The duties of this important risk management officer will vary across different enterprises depending on their size and type of operations, and while there certainly will never be a one-size-fits-all description here, the chapter includes some CRO best practices.

ROLES AND RESPONSIBILITIES OF AN ERM FUNCTION

The responsibilities of the modern enterprise risk function have moved from just an insurance department type of function and have very much broadened and deepened to include professional and governmental regulations, capital markets, financial reporting, the many issues surrounding globalization, intellectual capital, and, of course, all aspects of information technology (IT). To be effective, the modern enterprise risk function and its CRO must have their eyes wide open regarding the various levels of risks impacting all levels of the enterprise. A more traditional risk management function, along the lines of an insurance department, should take steps to reorganize and reengineer themselves to follow the COSO ERM framework model. Of course, if there had never been such a formal function in place, the launch of an ERM function provides an opportunity to strengthen controls and governance through the establishment of this risk management function.

We have described the COSO ERM framework model in Exhibit 3.1 as a three-dimensional cube with various enterprise units along one dimension and functions across another. An enterprise will certainly not have a need for separate risk management functions for each of these units. An enterprise risk function generally should be a corporate-level function with authority covering the entire enterprise. For a larger enterprise with multiple and differing business operations, there may be a need for separate multiple risk management units, but all should report to a single responsible risk unit headed by a CRO. A single enterprise with several very different business units, such as a corporation with a consumer lending unit and another doing legal document processing, may see some significant risk exposure differences across these multiple and differing lines of business and may want to have separate risk management groups to monitor and control the separate exposures in each. However, each of these groups should follow some similar procedures and should report up to a central, corporate risk management function led by a CRO.

Exhibit 5.1 describes the general functions or responsibilities of an ERM function or department. Whether a relatively small company or a multidivision, multicountry type of enterprise, any risk management function should follow these same general operational standards and guidelines. Many of these activities are referenced in other chapters, but the following sections outline the activities and responsibilities of such an enterprise risk function following COSO ERM. That enterprise risk function should develop policies to respond to both specific risks and regulatory requirements and then push this guidance down to the lines of

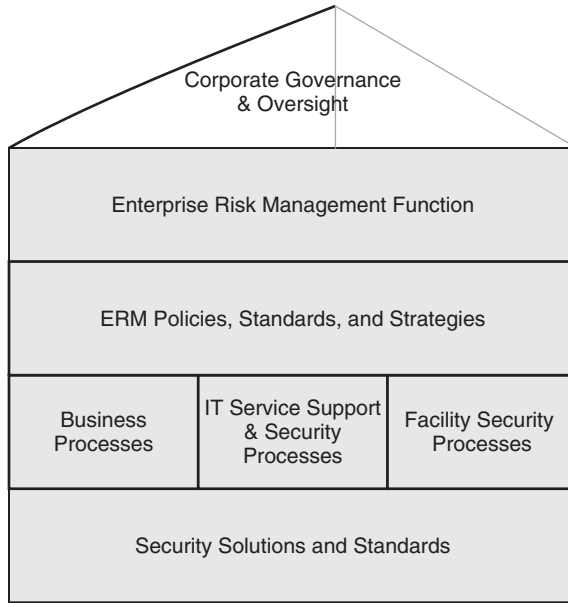

EXHIBIT 5.1 ENTERPRISE RISK ORGANIZATION RESPONSIBILITIES

business for execution, usually at their discretion. Given the closely interrelated business risks and strong regulatory environment penalties for noncompliance, this central risk management leadership is especially important because weak performance by one business unit can place the entire enterprise at risk.

CRO Responsibilities

A key component to an effective ERM function is to have some level of enterprise leadership responsible for the overall risk management process. This is the responsibility of the CRO, a designated senior enterprise officer responsible for administering and monitoring the overall ERM function in an enterprise. Although persons with a title of CRO have existed in some industries ranging from financial services to the electrical power industry for some years, this was once not a common C-level title, but today an increasing number of enterprises are appointing persons with the title of CRO to manage their risk functions. However, that title of "chief" means little unless the CRO has the authority and responsibility to effectively manage the enterprise's risk program and to both initiate appropriate actions and communicate these activities to all levels of enterprise management.

The major responsibility of the CRO should be to manage the process of assessing risks throughout the enterprise, to implement appropriate corrective actions, and to communicate risk issues and events to all levels of the enterprise. The CRO should be responsible for the overall risk management function in an enterprise and should direct and manage a supporting risk management function. An effective CRO, along with the supporting risk management department, should have a status and supporting group similar to internal audit functions in many enterprises today. Just as the internal audit department has a staff of specialists to review all levels of internal controls and provide recommendations for corrective actions, an enterprise risk function should operate in a similar manner. It should monitor the overall risk environment in the enterprise as well as make recommendations for corrective actions as appropriate.

While internal audit functions, with their reporting relationships to the board audit committees, have been very much defined by internal auditing standards and legal requirements, the ERM process has not yet been given that level of recognition today. If we have established a CRO, where or at what level does that individual belong or report? An enterprise's CRO should report and manage a function with many similarities to internal audit in today's enterprise. We say "almost similar" because, while SEC financial reporting rules require that internal audit reports to the board of directors' audit committee, there is no board risk management committee requirement in today's enterprises. However, as discussed in Chapter 8 on the importance of ERM in the corporate boardroom, some corporations have already established board-level risk committees, and many of today's boards of directors are assuming an increasingly strong interest in their enterprise's ERM function.

We suggest that an ERM function, headed by a CRO, should be one of the senior-level management functions in today's enterprise, reporting to the CEO or at least one level down, such as to the CFO or chief operating officer (COO). This is a function that should have the authority to review risks throughout the enterprise and to facilitate corrective actions to repair or minimize those risk situations. Using our Global Computer Products example enterprise, Exhibit 5.2 describes a general position description for a CRO, reporting administratively to the CFO and directly to the chair of a board risk committee. The CRO could report in this manner or alternatively to the CEO on the same level as the CFO and other senior corporate officers. The function would have the responsibility to assess and evaluate risks throughout the enterprise, making recommendations for corrective actions as appropriate.

This description defines the roles and responsibilities of a chief risk officer (CRO) using this book's Global Computer Products example company as a model. There are few standard or example descriptions published at present for this new and evolving position.

- **General Responsibilities**
  The chief risk officer is responsible for assessing all risks that may impact the company—financial, operational, IT-related, and environmental—and for developing appropriate actions to minimize those risks. Responsibilities include direct management of enterprise risk management (ERM) functions at both corporate headquarters units and domestic operations as well as advisory responsibilities over all nondomestic international risk management functions.
- **CRO Reporting Relationships**
  Reporting directly to the chief financial officer (CFO) for administrative purposes, the CRO reports to the chair of the board of directors' risk committee for action and strategy guidance. The CFO also has a strong advisory relationship with the management risk committee, under the CFO, for collaborating on the development and implementation of risk management policies and procedures.
- **Duties and Responsibilities**
  - Develops, initiates, maintains, and revises policies and procedures for the general operation of the enterprise risk program and its related activities to prevent illegal, unethical, or improper conduct. Manages day-to-day operation of the program.
  - Performs an overall assessment of all risks impacting the corporation, and reports to the board of director's risk committee on the status of these risks and actions taken to control them, at least on a quarterly basis.
  - Collaborates with other departments (e.g., internal audit, employee services, etc.) to direct enterprise risk issues to appropriate existing channels for investigation and resolution. Consults with the corporate attorney as needed to resolve difficult legal enterprise risk issues.
  - Responds to all identified fiscal, operational, IT, or general environmental threats through coordination with appropriate managers in the organization. Develops and oversees a system for uniform handling of such risk-related threats.
  - Acts as an independent review and evaluation body to ensure that enterprise risk issues/concerns within the organization are being appropriately evaluated, investigated, and resolved.
  - Monitors and, as necessary, coordinates enterprise risk activities of organization units to remain abreast of the status of all enterprise risk activities and to identify issues and trends.

EXHIBIT 5.2 CHIEF RISK OFFICER (CRO) POSITION DESCRIPTION

- Identifies potential areas of enterprise risk vulnerability and risk; develops/implements corrective action plans for resolution of issues, and provides general guidance on how to avoid or deal with similar situations in the future.
- Provides reports on a regular basis, and as directed or requested, to keep the board enterprise risk committee and senior management informed of the operation and progress of enterprise risk efforts.
- Establishes and provides direction and management of the enterprise risk hotline.
- Institutes and maintains an effective enterprise risk communication program for the organization, including promoting (1) use of the enterprise risk hotline, (2) heightened awareness of all levels of evolving risk threats, and (3) understanding of new and existing enterprise risk issues and related policies and procedures.
- Works with the human resources department and others as appropriate to develop an effective enterprise risk training program, including appropriate introductory training for new employees as well as ongoing training for all employees and managers.
- Monitors the performance of the enterprise risk program and relates activities on a continuing basis, taking appropriate steps to improve its effectiveness.

EXHIBIT 5.2 CHIEF RISK OFFICER (CRO) POSITION DESCRIPTION *(CONTINUED)*

While a single CRO could theoretically perform all of the duties and responsibilities described in this example position description, there will normally be a need for multiple risk management specialists reporting to the CRO. These are persons with the abilities to understand and help implement corrective actions for general business, IT, and basic insurance-related risks. Whether it be recommending improved internal controls or helping to secure appropriate insurance coverage, an effective enterprise risk management function should have several staff specialists to help review and help minimize enterprise risks. ERM specialists should have the authority and responsibility to both identify specific enterprise risks and actually help implement corrective actions to minimize those identified risks.

While an ERM function may look similar to an internal audit department, there are some key differences. Internal auditors review internal controls and make recommendations for improvement but often take no active role in helping to implement those recommended changes. The effective ERM group, however, often will take a more proactive role in helping to implement the necessary corrective actions. This often can be a challenging set of roles and

tasks for risk analysts in an enterprise. Some examples of how an effective enterprise risk management function might operate in an enterprise include:

- An ERM analyst reviews the potential new product liability risks in a given business area. Rather than just recommending that the unit search for appropriate insurance coverage, the analyst might take an active role with other members of the enterprise risk group to help secure appropriate coverage.
- Either as part of a direct review or from general information, the risk management function may identify governmental actions that may place some foreign country operations at risk. The risk analyst might work with legal counsel, foreign unit management, or outside advisors to take actions to limit the effect of those governmental actions.
- An ERM specialist with strong IT skills may assess system access vulnerabilities in the firewall perimeter surrounding an area of IT network operations. Perhaps working with technical IT staff members, the ERM specialist would help to implement a more effective enterprise-wide security strategy.

Another very important difference between an ERM function and internal audit is that the ERM group will usually go beyond just reviewing an area and making recommendations for subsequent follow-up. While their professional standards allow internal auditors to act as active consultants helping with solutions, they often just report their recommendations for responsible managers to take corrective actions. While the Institute of Internal Auditors' (IIA's) professional standards do allow internal auditors to act as consultants as well as reviewers, many internal audit groups today only review and make recommendations but do not help to implement those recommendations. The effective enterprise risk management consultant, in contrast, often takes a very active role in helping to implement effective solutions. External auditors, with their former strong affiliated consulting functions, once were very involved in reviewing an area and then suggesting that their own consultants take appropriate corrective actions. The rules in the Sarbanes-Oxley Act (SOx) have eliminated that function, and external auditors today are focused only on attesting to the adequacy of financial systems' internal controls. The role on internal auditors in ERM is discussed in Chapter 9.

Risk Management Enterprise Governance and Oversight

As discussed, risk management historically was not a top-level function in many enterprises. With its frequent association with the enterprise's casualty

and liability insurance functions, these old-line groups were sometimes called risk management but primarily just handled the corporate insurance function. For many enterprises, these old-line risk management groups operated as lower-level support functions with essentially no role in entity-wide risk issues and limited access to senior management. Under COSO ERM, today's risk management group should be much more than just the insurance department. An effective risk management function, led by its own CRO, should report to a senior level in the enterprise. That explains the cap or upper enterprise level in Exhibit 5.1. While SOx mandates that internal audit must report to the audit committee, there is no such reporting requirement at this time for the risk management function.

Chapter 8, on the importance of ERM in the boardroom, suggests the establishment of a formal risk committee, separate from the audit committee and reporting to the full board. That chapter provides some examples of how such a committee functions. We recommend that a board-level risk committee should be considered. Otherwise, and without such a special risk committee, the CRO and risk management should regularly and periodically report to the audit committee or even some other designated board committee. This additional reporting responsibility can be a challenge for many audit committees. Given the internal audit management requirements that SOx has imposed on both audit committees and the board in general, those board committees typically are busy enough that they may not need another set of meetings and reporting relationships. However, the enterprise's risk management function is sufficiently important to the overall welfare of the enterprise that time should be allocated for the CRO to meet with the audit committee or the full board on a periodic basis to describe risk management activities in the enterprise as well as any identified problems or concerns. Because they already have established lines of communication, the CEO, CFO, or the CAE should work with appropriate board members to make arrangements for establishing this review process as well as periodic risk management briefings. These arrangements are discussed in greater detail in Chapter 8.

Whether it be to a committee of the board or to the CEO, many risk management activities are sufficiently critical to the overall enterprise that decisions and planned actions should be passed over to the appropriate persons to make any risk-related decisions. For example, the Gramm-Leach-Bliley (GLB) law mandates that enterprises establish privacy protection over certain personal and financial data. However, there is some level of ambiguity in these rules, and there can also be legal penalties if the rules are not followed. The CRO can help establish an effective implementation here, but others such as the CEO and

legal counsel should review and help decide how to establish effective compliance processes to operate within those GLB rules. If the enterprise gets in trouble with such a violation, it is better to have other senior officers or even an appropriate level of the board to at least review and approve approaches rather than just pointing fingers at the CRO. This is corporate governance!

The reference to GLB highlights just one of the many U.S. laws or other rules today where risk-based decisions are needed. In addition, Chapter 8 discusses the importance of ERM in the corporate boardroom and how that function should become more involved with this very important process. Whether it be members of the board, the CEO, or others of sufficient stature, there should always be some level of governance and oversight above the ERM facility to review and make any necessary hard decisions.

ERM Activity Scope and Review Planning

Other chapters describe many different and important ERM activities. For example, a process for estimating the likelihood and consequences of various risks facing an enterprise is discussed in Chapter 2, while Chapter 11 provides guidance in understanding the various levels of risks in an IT environment. These and others are all important activities of the enterprise risk function. An effective ERM function should not, however, just go from one risk-related area to another without any type of organized plan or approach. While a risk management group, by its nature, will be somewhat crisis-driven, that same ERM function should still follow a risk review plan covering an extended time period. By its very nature, risk management will always be responding to crises as they occur, but that response should try to follow a standard, consistent approach throughout the enterprise.

The ERM function should first develop an understanding of and document the risk areas that are in their scope of operations. There are always some risk areas that are either too big or too minute to be included within the scope of the ERM group. We are referring to very major events such as violent weather, major economic disruptions, and the like. The CEO, along with the risk management enterprise, may be able to have some high-level risk response plans in place for such events, but often cannot realistically do much beyond having some very general contingency plans or statements of support in place. Similarly, there will always be some risk areas that are perhaps troublesome difficulties but are not within the scope of the ERM function or department. An ERM group needs to formally document the risk areas that are within its scope as well as any that are just “too big” or “too small.” Of course, the risk management group should never post signs

on its front doors stating "Don't call us unless …" but should have some internal guidelines covering the types of risks it can realistically manage.

These enterprise risk scope declarations should be formally reviewed and approved by the board or CEO-level management. This type of scope information, however, does not need to be communicated to all levels throughout the enterprise. There is no need to formally declare that grocery thefts in employee dining rooms. Kitchens worldwide are outside of ERM's scope. That will only raise "no one cares" types of potential actions. Just as an internal audit function will develop some general scope–related statements, the enterprise risk group should do the same.

Our example company, Global Computer Products, provides a method to describe this risk scope approach. The risk environment there is described in Exhibits 3.5 and 3.6. Using these descriptions, Exhibit 5.3 summarizes the risk activity scope for this hypothetical sample company. Again, this type of risk responsibility scope document should be an internal ERM policy statement and should not be for distribution to the enterprise at large. Rather, it should document ERM's areas of risk management expertise, which in the enterprise is responsible for various risks, and the acceptance of other entities, such the legal department or local fire departments, for handling other risks. This is the type of document that the CRO should

Global Computer Products

RISK ACTIVITY SCOPE

The corporate enterprise risk management (ERM) group is responsible for monitoring and developing remediation plans for all major corporate operational risks. Operational risks will include, but are not limited to, all major activities involving the development of new company products, acquisition and maintenance of assets, legal and regulatory issues, financial reporting, and internal controls. ERM will establish guidelines for all risk management processes and will assign the management of some risks to the operating units but will assume the direct management of others.

ERM recognizes that there are some market, economic, or environmental risks that are beyond its scope and ability to take corrective actions. ERM will communicate these risk issues to the board of directors' risk committee and will assist in risk remediation where appropriate.

EXHIBIT 5.3 RISK ACTIVITY SCOPE: GLOBAL COMPUTER PRODUCTS SAMPLE

share in a board or CEO-level briefing so that they are aware of the ERM's planned area of scope. The CRO should gain approval and endorsement for these high-level plans or should adjust them in light of suggested changes.

Beyond these high-level scope statements, the risk management group should establish a strong understanding of the higher-risk areas that are with their defined scope and develop risk management project plans for these enterprise risk areas. This is the process of defining risk likelihood and criticality as discussed in Chapter 3. Regarding the selected higher-risk areas, risk management needs to develop an ongoing monitoring or review approach. That is, if a risk area has been selected as a risk management concern, the ERM group should place the area on its "radar screen" for potential situation status reviews. This risk-monitoring approach differs from the activities of internal audit that typically selects some area for review and then performs an internal control review of just that area. Such reviews will typically result in a formal internal audit report with its findings and recommendations.[2]

Based on its estimate of the higher likelihood and loss probability risk areas, the ERM function should monitor and review risk areas taking one of the following approaches:

- *Initiate immediate action to resolve the risk.* Based on initial risk assessment reviews and input from others in the enterprise, there may be some outstanding risks that appear about to occur and can be fixed or corrected almost at once. Examples include an item of production machinery that looks as if it were to soon fail, or compliance with some regulation where governmental authorities have not asked any questions as yet, but the enterprise knows that its compliance seems shaky. Through either their own actions or coordination with others, risk management should schedule corrective actions as soon as possible.
- *Review the risk area and propose corrective actions to reduce risk exposures.* With this approach, the ERM group acts somewhat like internal auditors or internal consultants. They will review some potentially higher-risk areas and make suggestions for corrective actions to improve the risk. They may not have the same "clout" as internal audit with its audit committee and SOx 404 continuous monitoring responsibilities, but its special knowledge of understanding risk management situations should give the enterprise risk group a special level of respect. This process of enterprise risk reviews is discussed later in the Risk Assessment Reviews and Corrective Action Practices sections following.

- *Arrange with internal audit to perform a review of high-risk areas.* In some instances, the nature of a high-risk area may be caused by or based on poor internal controls. While the enterprise risk group can assess internal controls and business risks, in some instances it may be more efficient for the overall enterprise to request that internal audit perform an internal controls review, following their internal audit standards, over the potential higher-risk area. This will require some coordination but can be very effective if there are strong communication links between risk management and internal audit. These arrangements are discussed in Chapter 9.
- *Monitor the risk area on a continuous basis.* Some identified risks represent areas where a risk event may not occur because of weak internal controls that could be improved but because of external factors that require monitoring. An example might be the risk of currency devaluation in a foreign country unit. Risk management needs to assign someone from the ERM team as well as local management to monitor these types of events. While plans for corrective actions should be in place, there is no need to activate them until the actual event occurs.
- *Develop plans to take action only in the event of a risk occurrence.* This is a more passive approach, but can still be appropriate for some lower-likelihood but higher-impact risks that still should at least be on the "radar screen." With plans in place and frequently updated, the risk management group would need to go into action only if the risk event occurs or appears to have a high probability of occurrence in the very near future. This is a "fire extinguisher on the wall" type of risk management approach. It is important the fire extinguisher remain charged, but it is only used in the event of an actual fire.

Based on this set of potential risk events ranging from those that need to get corrected at once to others only placed on a watch list, risk management should develop an annual risk assessment action plan. Such a plan would assign responsibilities for the coverage of various risk events, estimate the enterprise risk group's time to correct and review, and include some time and budget estimates. This document becomes the enterprise risk group's action plan for the period. The plan should be reviewed and approved by senior management, and when others such as internal audit are expected to complete portions of the action plan, planned events should be coordinated. Exhibit 5.4 shows this type of action plan using the Global Computer Products example company.

Global Computer Products—Fiscal Year 07						
Operating Division	**Planned Risk Assessment Activity**	**Responsibility**	**Planned Actions**	**Start Date**	**Due Date**	**Estimated Remediation Costs**
Product Development	New product security risks	ERM & IT	Corrective action plan			
Product Development	India computer system operations	ERM	Review			
Product Development	Key documentation controls	ERM & IA	Corrective action plan			
Finance	Vendor agreements	ERM	Review			
Finance	Staff risk management training	ERM & HR	Implement			

EXHIBIT 5.4 ANNUAL RISK ACTION PLAN EXAMPLE

Although planning approaches can vary, this sample plan shows where the risk management group is planning a formal risk assessment review in some areas, where it is planning on helping to install some improvements elsewhere, where it is coordinating a review with internal audit, and where it is just monitoring an area. Because the latter also takes time and resources, monitoring-only activities should be planned as well.

Risk assessment corrective action plans are somewhat different from many other enterprise events because they must be based, in part, on the actions to be taken in the event of an unanticipated risk occurance. An explosion at a nearby but unrelated different company production facility could hamper operations at a company-owned facility. However, that explosion is an entirely unknown and unanticipated event. The risk management team would have to spring into action to help get the company facility back in operation in the event of such an unexpected event. That action would certainly interrupt the annual risk action plan, but also would provide a priority type of list showing where adjustments should be made.

The financial accounting rules of establishing allowances for doubtful accounts can help in planning for these unknown risks. When selling goods, an enterprise typically ships them and sends the customer an invoice for payment expected at some later period. The transaction is initially recorded as

an accounts receivable due from the customer, with the final sale recorded when cash is received. However, no matter how good their credit screening process, there will always be some customers that just do not pay or pay only partially after protracted disputes. Based on the overall payment history of all of its customers, the enterprise will establish an accounting reserve allowance for doubtful accounts to offset and estimate that a certain but hopefully small number of customers will never pay. An ERM function should use this type of approach when planning its risk management monitoring activities. Although it will typically not have any history or advanced knowledge regarding risk events, it is prudent to develop the risk management plan with the allowance that there may be some level of unanticipated risk events during the period.

When developing these scope assessments and risk action plans, the CRO and the risk assessment team should always allow for and consider the broad objectives of COSO ERM. That is, plans should be on an enterprise-wide basis with an application across every level and unit. This says that there must be a strong level of communication, collaboration, and risk planning across the overall enterprise. This requires a much more expanded view than traditional business risk management approaches but is an approach that should enhance and protect the value of the overall enterprise.

Risk Management Policies, Standards, and Strategies

COSO ERM has moved the risk management function from a more traditional risk-by-risk approach to a perspective that covers the entire enterprise on a continuous monitoring approach. To achieve that scope, however, the risk management function must encompass all units and levels. It cannot just be run or managed by a CRO with a small staff at headquarters, but must be managed and communicated to a wide group of responsible persons throughout the enterprise. In addition, the ERM function, under leadership by the CRO, needs to develop some risk management policies and standards that are followed by units in the enterprise, following a consistent strategy. Designated managers throughout the enterprise should be trained on these risk management policies and then charged with their implementation.

Our point here is that while enterprise risk should be managed and directed by a central CRO-led function, direct responsibilities and tasks need to pushed down and across the enterprise by building a risk-sensitive culture throughout the enterprise. Stakeholders at all levels need to be aware of some of the risks that the enterprise is facing, the consequences of

those risk exposures, and some of the steps they can put in place to limit those risks. The following list outlines some of these steps for managing risks throughout the enterprise:

- *Building a risk-awareness culture.* As part of building an effective ethical culture in an enterprise, the "tone at the top" words of senior executives to others in the enterprise are very important. This is an element of the COSO internal controls framework that was discussed in Chapter 1. When a CEO addresses key employees about the importance of having an ethical culture and strongly endorses and supports the enterprise's code of business conduct, others will typically pay attention. The same concept holds true for risk awareness, although this can sometimes be a little different. Due to the wide variety of internal and external risks that an enterprise faces at all levels, it is difficult if not impossible to build a comprehensive risk-oriented principles document that is circulated throughout. However, an enterprise can develop and circulate some risk awareness documents that either target certain functions in the business or external threat risks. As an example, Exhibit 5.5 outlines some of the information security protection and content-related risks that can put a single unit as well as the overall enterprise in jeopardy. Copying a description of a corporate financial plan through an e-mail cut-and-paste process and then sending the plan out could create an enterprise-wide trade-secrets loss risk. Chapter 11 includes discussions of other IT enterprise security risks.

  The enterprise should focus on multiple internal risks, such as information security protection, and develop and circulate this type of guidance to its various organization levels. This is the type of information that can be communicated through messages on intranet home pages, employee newsletters, or comments at management meetings. The whole idea is to communicate the concept that the enterprise always faces certain risks but those risk exposures can often be limited by awareness and participation in the ERM program. These types of efforts will launch a risk awareness program and hopefully initiate a risk awareness culture.

- *Creating the enterprise-wide risk management enterprise.* We have discussed the importance of raising any existing ERM department to what has been described as a "C-level" function headed by a CRO. In addition to just one individual with a CRO title, it is important to build an effective ERM staff or set of resources to support that CRO.

Information Security Content Risks. There are multiple areas where an enterprise might have numerous levels of unprotected information assets such as source code, product plans, engineering drawings, product formulations and patent materials, and database lists of customers and vendors. There is a need to understand and document these various types of information assets and the current control procedures in place and to look at all identified data assets and decide which are the most vulnerable. These should then receive priority for content protection controls. Special scrutiny should be given to content stored in document management or content management systems since these are likely to be of high value. Since the organization may not be able to establish content protection controls over all data assets, there should be a formal, documented record outlining why one set of content assets are at a higher, more immediate corrective action level than others.

Establishing Content Compliance. Content protection policies and procedures need to be clearly stated to all stakeholders—employees, vendors, and others, similar to employee Code of Conduct rules. These rules as to what types of content are sensitive and how they can be copied or captured should be defined as clearly as possible. All stakeholders should be asked to acknowledge that they have read and understand these content protection rules and they agree to abide by them.

Content Protection Technology. Sensitive content leakage incidents can occur at many levels including accidentally posting sensitive information on a public Web site or e-mailing sensitive information to a personal Web mail account. Traditional IT control procedures such as identity management and access control lists are necessary, and specialized software content monitoring and filtering tools should be considered. Typically, these tools register or "fingerprint" sensitive content stored in the file system or in content management repositories. Installed at the Internet gateway, such tools should be selected to monitor all of the content flowing out of the organization and detect attempts to transmit sensitive information. Policy actions need to be established to include alerting, logging, and the actual blocking of the attempted transmissions.

EXHIBIT 5.5 RISK AWARENESS GUIDELINES: INFORMATION SECURITY CONTENT MANAGEMENT

As suggested through these chapters, an effective enterprise risk group or department often will be somewhat of a hybrid between a traditional internal audit group and the old insurance department that once was called risk management. It will also be a more active group that both monitors events and sometimes initiates its own program of corrective actions. An effective risk group should cover all aspects of the enterprise, in terms of specialized facilities and locations of operations. While the specialties can vary, it is often very effective to have specialists in three areas: accounting and finance risks, all aspects of IT service support and delivery, and risks impacting the enterprise's areas of operations. For example, if the enterprise is a provider of health care–related insurance claims processing, its risk coverage

over areas of operations might include a strong knowledge of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) health-related security law. HIPAA is a complex U.S.-based security-related law with multiple risk management provisions.

Those three specialties should be covered by staff professionals with a good understanding of the risks impacting the particular enterprise as well as techniques for limiting risk exposures. This might involve expertise within the risk management group, contacts with specialized help when needed, or close coordination with other functions within the enterprise. For example, risk issues over IT disaster recovery and continuity planning are discussed in Chapter 11. Risk-related issues here might be covered by specialists within the IT enterprise. However, the ERM group should establish close communication and coordination links with specialists in IT.

In addition to these core specialized areas, the enterprise risk group should provide coverage to the entire enterprise on a worldwide basis. There is little value for a Houston-based CRO and the supporting risk management group to only provide guidance that covers Texas or even the total U.S. operation if that guidance does not extend to some of its operations in Argentina. There must be communication and coverage throughout the total, global enterprise. While establishment of risk management staff functions worldwide may not be cost effective, strong training and procedures can build some dotted-line relationships with other groups outside of the home country to create a local "eyes and ears" risk monitoring process at all locations as needed.

Enterprises are organized in many different sizes and shapes, and there is no one best risk management enterprise approach. However, there should be some CRO-led central or corporate risk management function to communicate risk-related objectives and plans to senior management. Based on our sample company's background description in Exhibit 3.5, Exhibit 5.6 shows the ERM enterprise chart for Global Computer Products. It suggests a corporate enterprise risk management function based at its Chicago area headquarters as well as a small risk management function at the Belgian distribution center. This latter group would be responsible for monitoring European Union (EU) risk-related legal and regulatory issues, as well as risks associated with the distribution operations there. Global's internal audit function has a branch or field facility nearby the computer security facility in San Jose, and the corporate enterprise risk function has

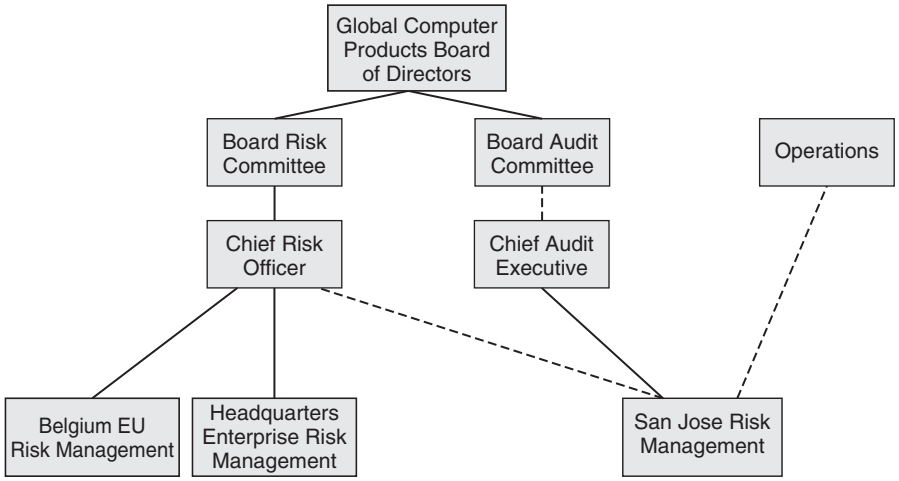

EXHIBIT 5.6 GLOBAL COMPUTER PRODUCTIONS ENTERPRISE RISK MANAGEMENT ORGANIZATION CHART

established a strong dotted-line relationship for risk management with that group. Through policies, procedures, and training, risk management activities at other Global locations are handled through coordination and communication to assess risk issues at those facilities.

- *Enterprise risk management policies and standards.* In addition to building an effective enterprise risk management group or function along with messages to help foster a risk-sensitive culture in the enterprise, a series of risk management policies and standards should be developed and communicated throughout the enterprise. While the headquarters' CRO-led risk management team should be constantly assessing and reviewing higher-level risks, there will be many risk-related decisions that must be made at all levels, such as a selection of a new vendor, the purchase of some new asset, or any of many other, often smaller-scale transactions. Risk assessment policies and standards should be developed that call for all members of the enterprise to consider risk management concerns and considerations.

  An effective method to introduce risk awareness throughout the enterprise is to develop and distribute a risk assessment guideline signoff form that stakeholders are asked to consider whenever making a decision for the enterprise that involves more than some

Global Computer Products

Risk Assessment Acknowledgment.

Operating Unit _____ Responsible Manager _____ Date ____

Activity Description _____ Asset Value _____ Cntl # ___

If activity or asset value are above guidelines, was Activity sent to Enterprise Risk for review? _____

For qualifying other Activities, were risks reviewed by Operating Unit? _____

I have **assessed the operational and financial risks associated with the activity and have** taken appropriate actions per Risk Guidelines.

Risk Acknowledgment Signature _____

EXHIBIT 5.7 RISK ASSESSMENT SIGN-OFF ACKNOWLEDGMENT FORM

assigned level of X dollars, where X is a number to be determined depending on the location. Distributed similar to a code of conduct, the risk assessment guideline signoff form should be included with all cash-type transactions such as a new material purchase requisition. Exhibit 5.7 is an example of the types of words that might be included in such guidelines. The idea is to request that all front-line managers, including smaller units or at a foreign location, personally acknowledge that they have considered relative risks when signing off or approving a designated level of financial transaction.

The purpose of this risk assessment guideline form is not to "get" the employee who signed the form for some financial transaction that resulted in a risk-related failure, but to encourage all stakeholders to acknowledge that they have considered potential risks when authorizing and approving any financial transaction above some designated value. That value, of course, should vary depending on the business. For a chain of fast-food restaurants, as an example, a procurement manager with responsibility for the entire chain might be asked to acknowledge consideration of risks for all supply purchases over $25,000, while a unit manager in that same chain would be asked to acknowledge his or her consideration of risks for transactions over $500. At appropriate levels, all members of the enterprise should be asked to evaluate relative risks when making financial-based decisions.

This guideline form only asked stakeholders to specifically acknowledge that they have considered risks above a designated monetary level. This type of form does not cover such matters as legal risks, market risks, or IT-related risks. However, it can be a method to encourage stakeholders to consider appropriate risks when making any transaction-based decisions in their area of responsibility. To encourage this type of thinking even further, an enterprise should deliver some overall risk awareness training to all levels of the enterprise. Examples of risk management training will be introduced in Chapter 12. The idea is to encourage all levels to remember that there are risks involved with any transaction and that the enterprise, by policy, should not enter into a transaction that is above the enterprise's risk tolerance level.

Business, IT, and Risk Transfer Processes

The next and very important level to building an effective ERM program is to understand the risks directly impacting the enterprise and then to develop general remedial procedures covering them. These direct impact risks have been grouped into three general risk areas of business, IT, and transfer-related processes. While these categories are broad and arbitrary, transfer processes cover the insurance types of protections that are external to or beyond the regular control of enterprise managers. These also provide insurance coverage for a potential production plant fire, the risk that a governmental unit will impose some unexpected regulation, or the risks of general geopolitical changes in some area of operations. The category of IT risks covers both what auditors call general controls areas as well as business application specific risks. These general controls areas include risks such as IT continuity or disaster recovery planning as well as concerns regarding a malicious attack on the IT network (both are discussed in Chapter 11). The remaining risks are classified as business-related risks and include a wide variety of concerns.

Timing can be a major consideration in assigning business risks to these areas of business operations. IT-related risks are a good example of this timing consideration. The risk of a virus attack on a computer system's network is a very immediate type of concern. The risk event could occur with little warning, and the response to that risk should be immediate. The business risks associated with a financial accounting error are more or less an immediate type of concern tied to periodic financial reporting cycles, and technical process risks are often longer-term types of risk events.

While it is sometimes difficult to easily split all risks into these three broad areas, this suggested split provides a good starting basis for assigning all risks to appropriate people or functions in the enterprise. For example, while IT systems and related technologies really cover all aspects of business operations, their technical nature and the need for specialized knowledge makes it convenient to assign them to an IT risk category "bucket." Similarly, what we have called technical and transfer-related risk controls are those best monitored and controlled by persons outside business operations. These might include the law department for legislative rule matters, facility operations for fire control issues, and specialists in insurance coverage. Although the number of enterprise risk categories can be expanded, the idea is to somewhat divide up responsibilities for enterprise risks at a very high level.

General Business Operations Risks. The majority of enterprise risks discussed throughout this book should be considered as business operations risks. These are the wide range of financial, competition-related, and business operations risks that are major enterprise concerns. Prior to COSO ERM, these risk areas were generally considered in the following manner or order:

- *Risk management focus.* Emphasis was on financial risks associated with breakdowns in internal accounting controls.
- *Business operations scope and risk objectives.* Protecting enterprise value, with an emphasis on treasury and insurance.
- *Risk management emphasis.* Financial and other business operations covering only limited risk areas, operations, and processes.

COSO ERM has broadened these traditional risk factors and moved to an overall entity-level set of considerations. Following the description of the enterprise-wide risk framework discussed in this chapter, a component of the risk management function should establish communication links and monitor risk events and activities throughout the enterprise. This is the portion of an effective risk management function that should identify significant risk areas in all levels and dimension of the enterprise and should take steps to both review the levels of exposures to those risks and initiate corrective actions.

IT General and Application-Specific Risks. While Chapter 11 provides more details on the types and nature of IT risks, it is usually convenient to classify IT-related risks in the same manner that we classify IT internal

controls—general and application-specific controls. General controls are the pervasive factors or control considerations covering all IT operations such as a password security or software change control processes. This control type covers all IT operations and is not specific to any one application. Many IT-related risks also can be considered general IT risks. The risk that IT may not be able to continue operations in the event of some massive electrical outage will impact all IT operations and all of the applications running in that computer network.

The two unique aspects to this area are the need for ongoing and real-time monitoring of the risk environment as well as both requirements for technical skills and tools to respond and react. A major area of concern is the risks surrounding the telecommunications network that supports many of today's enterprises. Whether it be an e-mail network that is necessary for enterprise-wide communications or many applications, all operations should be operating and communicating with one another and to the Web. Whether a malicious virus attack on the network, the internal controls failure of some key application, or just extended delays due to heavy legitimate traffic, these IT networks are exposed to a wide variety of risks. There is a need to continuously monitor these risk events and to respond at once. This IT risk monitoring requires a wide range of specialized tools and techniques that are discussed in Chapter 11.

An effective enterprise risk management needs to establish specialized personnel and tools to monitor and respond to IT-related risks. Some of this activity might be assigned to the IT function and its ongoing IT operations and security monitoring and technical remediation activities. In many respects these activities are part of overall IT service support and service delivery ongoing activities. We do not consider the process of assigning IT network access passwords and monitoring password violations as a risk-related activity but as just good IT operations management. IT would be expected to assign effective control procedures and recognize the risks if they are poor.

Alternative Risk Transfer and Facility-Related Risks. As discussed previously, many enterprises prior to COSO ERM thought of their risk management operations in terms of insurance coverage and physical asset protection mechanisms. While we now should be thinking of risks on a broader, strategy-setting level, the risk-based concerns about having appropriate insurance coverage or physical perimeter protections still have not gone away. There will continue to be a need to monitor those risk areas and to establish appropriate control processes. The term *risk transfer* is really

the process of securing and purchasing insurance. An enterprise may face a risk that one of its facilities may incur a major fire. While there is not a significant chance that there will be a fire, the repair and recovery costs could be very expensive to the enterprise. Rather than setting up a fund to cover any fire losses or just hoping against hope that the enterprise will not have to incur the losses associated with such a major fire, that risk is generally transferred to an insurance carrier. Such an insurance carrier will offer similar insurance to many other enterprises and will bet that while there may be risks of fires at one or another enterprise production plant, they will not incur such losses at all of them. Thus, they can cover the costs of an enterprise's plant fire risk lower than if the enterprise were self-insured.

In addition to risk transfers through insurance, there are many alternative financial risk transfer mechanisms through the general investment or financial-related products called derivatives. A broad and complex field, financial derivatives are financial tools to cover or hedge against financial losses. A simple example here—and one that is still not that simple for many people—is the process of selling a stock or investment "short." If some security seems to be priced high today, and the investor feels that it may go down in price soon, the investor can sell that stock short even if the investor does not own the stock today. The investor borrows money for the stock and then sells it today's high price. If—and hopefully when—the stock goes down in price, the investor covers the loan of borrowed stock by buying more stock at the current lower price. The investor must pay interest for the loan on the borrowed stock but can profit greatly on the transaction if all works well.

Although a short sale is not considered to be a true financial derivative, it illustrates the concept of a financial risk protection mechanism. There are many other types of derivative transactions that an enterprise can use to hedge or transfer its financial risks. However, while a CRO and the ERM function may have some understanding of hedging financial risks through the use of derivatives, the ERM function may need to seek specialized financial help if it seeks to structure any financial derivative transactions. Making some very wrong bets or developing a poorly structured derivative transaction could result in massive costs to the enterprise.

There is still a variety of other facility-related or broad risk categories that belong in this category of an effective ERM program. These include, but are certainly not limited to:

- *Building and facilities security.* This category can include all security beyond IT facility and network security and include plant

perimeter security controls, employee badges, and many other related matters. Other specialized people in the enterprise typically manage these risks, but the ERM group should have a good understanding of them and should monitor risk events in these areas.

- *Legal and regulatory risks.* Whether it is litigation actions against the enterprise or new laws being considered by legislative bodies, an enterprise should have a good understanding of the legal and regulatory developments and issues in their area of operations. The CRO or some designated member of the enterprise risk function should maintain close ties with legal counsel or other sources. In many respects, this area of risk management primarily involves understanding and appropriately communicating risk-related matters to others in the enterprise.

The preceding examples could be expanded to other issues as well. The point is that an effective ERM function should install continuous monitoring processes to review, understand, and take appropriate actions on all risks that may impact them. An enterprise group, reporting to a strong CRO, should be able to introduce effective ERM programs.

Although it has been suggested that one person should be designated as CRO to manage the ERM function and that it should consist of three basic functions, we have not suggested the size for such group. Much will depend on its planned activities, if the enterprise risk group is performing some direct risk assessment reviews and if it is also helping to install preventive controls in other areas. The size of an ERM function should often be about the size of their total internal audit group.

Exhibit 3.5 described the size and activities of our Global Computer Products example company. With the assumption that the CRO has a mandate to establish an effective worldwide ERM function with active coordination with internal audit and other supporting functions, this would be the type of enterprise risk function that would directly perform some its own risk assessment reviews but would rely on some specialized technical help in such areas as IT network control risks.

Risk Assessment Reviews and Corrective Action Practices

As discussed, an effective ERM group will often operate in a manner that is very similar to internal auditors. Much of their work involves monitoring ongoing issues and either providing recommendations to improve controls or providing consulting-type guidance. However, as was emphasized in Chapter 3, the ERM group should identify and focus on significant areas in the

enterprise with high levels of likelihood of occurrence. In those situations, the ERM function should not just sit back and wait for the risk event to occur. Rather, this is an appropriate time for the ERM group to review the risk area and make appropriate recommendations to lessen the risk and improve surrounding internal controls. Risk management review reports can be a major responsibility of the risk management function, and this chapter introduces a new review approach, called risk assessment review (RAR).

While not every higher-risk area identified will be subject to such a review, the enterprise risk function should borrow some techniques from their internal auditors and perform appropriate reviews of higher risk areas. ERM function–led RARs will report on risk-related examinations in key enterprise areas and will make recommendations for both improving internal controls and reducing risk likelihood.

This RAR approach places enterprise risk activities in an almost parallel path with traditional internal audit activities. However, with some advance communication and coordination, these reviews are not designed to compete with internal audit activities but will enhance and support similar internal audit internal controls-related reviews. We can see how this process works by reviewing the Global Computer Products sample company. As part of an overall discussion covering this area, Exhibit 9.1 identified Global's San Jose Auditable Entities receiving and inventory controls processes as a significant risk area requiring audit or internal controls review attention. If the ERM group sees significant exposures in this area and if internal audit has no planned reviews here, the ERM group should schedule an RAR of this area.

The RAR is a new type of review, and the risk management group should communicate their review plans and procedures with senior management, internal audit, and the board audit committee. This type of review is not designed to compete with internal audit review activities but to improve on the risk environment and enhance internal controls. Exhibit 5.8 shows this comparison between the functions and objectives of this new RAR risk-related review and a traditional internal audit report. A new type of compliance reporting, risk management should review its plans for RAR reports with senior management, internal audit, and more important, the audit committee.

The RAR process should proceed in a manner similar to the process of planning, performing and reporting the results of internal audits.[3] The key difference here is that the RAR reviewers would emphasize a wide range of identified risks in the area selected and then would suggest approaches to eliminate or minimize these risks. Although there can be many variations

due to the nature of the initially identified risks, the enterprise risk reviewers should form a standard set of review steps to review the identified area. Exhibit 5.9 shows the risk review steps that might be used to review risks embedded in the Global Computer Products' San Jose receiving and inventory controls area.

Risk Assessment Report Characteristics	Internal Audit Report Characteristics
Report Objectives	
Evaluate operational and other risks based on established plan or risk-related events. The report will make suggestions for corrective actions or will report on the progress of remediation efforts.	Evaluate the adequacy of financial, operational, or IT controls following audit plan approved by the audit committee. The report will make recommendations for improvement as appropriate.
Responsibility for Completing Work	
Enterprise risk management staff with support from IT, internal audit, and other subject management experts	Internal audit.
Review Evaluation Process	
Review of documentation, observations, and testing as appropriate.	Review of documentation, observations, and testing as appropriate.
Standards Governing Reviews	
Currently no professional organization standards	IIA Standards for the Practice of Internal Auditing.
Report Final Recipient	
Board audit committee, if established, or else senior management such as CEO or CFO	Audit committee of the board
Reporting Process Responsibility	
Chief risk officer	Chief auditor executive
Report Corrective Actions Responsibility	
Risk management reports findings and may review recommendation follow-up status and may become actively involved in implementing corrective actions.	Internal audit reports findings and may review recommendation follow-up status but generally has no responsibility for implementing recommendations.

EXHIBIT 5.8 RISK ASSESSMENT REVIEW AND INTERNAL AUDIT REPORT COMPARISON

The following outlines the steps necessary to perform a risk assessment review (RAR) in compliance with the COSO ERM framework:

1. Schedule review based on long-range risk assessment plans, management request, or unanticipated risk event.
2. Develop preliminary objectives for the RAR:
   a. Review current risk status for management reporting.
   b. Risk-related assessment in conjunction with internal audit or other group.
   c. Perceived enterprise risk exposure to be reviewed.
3. Review supporting data to gain an understanding of the nature of the risk, its severity, occurrence probability, and alternatives for risk mitigation.
   a. Review supporting data or perform tests of data to better understand the nature of deviations or further risks of occurrence.
   b. Reconcile results of reviews with preliminary risk assessment objectives.
4. Develop cost-based alternative risk mitigation strategies, such as risk substitution or risk acceptance.
   a. Review mitigation strategies with responsible management to assess feasibilities.
   b. Develop best approaches for risk mitigation.
   c. When practicable, test proposed mitigation strategies.
5. Develop exit strategy for the RAR.
   a. Recommendations for immediate corrective action to be performed by operating unit.
   b. Corrective actions to be performed through a planned scheduled project.
   c. Corrective remediation performed by the ERM team.
   d. Documented avoidance of risk.
6. Publish RAR with copies to responsible management, the risk committee, and a request for RAR wrap-up actions at a designated date.

EXHIBIT 5.9 SAMPLE RISK ASSESSMENT REVIEW GUIDANCE

An example might better explain this RAR process. We will go back to our same Global Computer Products example and to potential risks in the area of San Jose operations receiving and inventory controls. Given this hypothetical risk situation, assume that the ERM team has decided to implement an RAR process in this area. Risk management would perform a review similar to an internal audit review and should develop what internal auditors call a program of set procedures to perform the review. This type

of review guidance can be developed through discussions with internal audit on how they would perform reviews in this area as well as on the ERM group's knowledge of the special concerns in this area. Exhibit 5.9 is an example of the review approach that the risk management specialists would follow when reviewing risk management concerns in this area of our sample company's San Jose operations.

As a result of such a review, the ERM group would prepare and release a RAR report, similar to an internal audit report including audit findings and recommendations. Exhibit 5.10 is an example of such a report for this area

Global Computer Products

ENTERPRISE RISK MANAGEMENT

RISK ASSESSMENT REVIEW

San Jose Receiving and Inventory Risk Assessment Review December 15, 2007

The corporate enterprise risk management (ERM) group performed a risk assessment review of the San Jose operations receiving and inventory operations at the San Jose facility. The review was performed with members of the internal audit team who are based at San Jose and, in conjunction with ERM, provide support for ongoing risk-assessment activities. The review was initiated on September 15 with the following risk-based objectives:

1. Documentation supporting certain input shipments may not be properly checked for certain import compliance rules, placing company at risk of trade violation rules.
2. Quality control testing of input shipment electronic may be insufficient, causing the company to approve and pay for bad incoming products and ultimately producing inferior finished products.

Our review included detailed reviews of receiving documentation over the third quarter of 2007 as well as observation and testing of these processes. The results of our review activities and detailed observations are described in the addendum to this report. However, in summary, the review team found:

- The receiving department is not properly reviewing import documentation with regard to trading partner rules. Proposed procedures to improve these processes and to limit our risks of potential compliance violations are described on the pages following this report.
- We generally found the incoming goods quality control testing to be adequate, limiting the risk of inferior product components.

EXHIBIT 5.10 RISK ASSESSMENT REPORT SAMPLE: SAN JOSE RECEIVING AND INVENTORY

of San Jose operations. The idea here is that the ERM function should operate in a manner similar to internal audit but concentrate the review on significant enterprise risks. This type of exercise should not compete with internal audit but should enhance an enterprise's review and understanding of significant risks.

The concept of launching RAR reviews and their resultant reports will require coordination with senior management, internal audit, appropriate board committees, and others. The concept here is that RARs should not be viewed as competition or a distraction from internal audits efforts but a special and unique set of reviews concentrating on significant enterprise risks. The concept of RAR reports is a somewhat new and different activity for risk management groups but represents an area that will promote the effective implementation of COSO ERM.

ERM COMMUNICATIONS APPROACHES

While an effective ERM function will perform many behind the scenes protective functions for an enterprise, strong communication procedures are essential for the function's success! Beyond the regular communications of an enterprise risk specialist talking with IT regarding some suggested risk actions or the CRO communicating with the general counsel regarding the status of some litigation action, the ERM function should communicate its concerns, and activities to appropriate levels throughout the overall enterprise. These communications should include making senior management and the board aware of enterprise risk concerns, describing the enterprise risk review process through a series of RAR reviews, and awareness on overall enterprise risks. Considerations and approaches for launching an effective RAR process include:

- *Board or senior management risk concerns.* Boards of director audit committees have always been aware of the importance of internal audit, and SOx with its legislative requirements has very much strengthened that relationship. Because of their history as more of an insurance department, a lower-level function, enterprise risk management has not had that level of attention from corporate boards. This will change! As discussed in Chapter 8, boards of directors are becoming increasingly aware of the enterprise risk concerns defined in COSO ERM. The enterprise CEO should introduce the CRO to the board with arrangements established for regular reports to the board on higher risk areas in the enterprise.

- *RAR reporting processes.* While similar to traditional internal audit reports, RAR's focus on *enterprise risk* concerns limited but specialized areas. They will almost always contain recommendations to improve the risk environment in some area. However, they will sometimes be an account of an area where the enterprise risk group has identified the risk area and assisted in installing processes to eliminate the risk concern.
- *Enterprise risk awareness programs.* An effective ERM group should develop communication processes to make all members of the enterprise aware of the enterprise's risk management approach. This may be as simple as a company newsletter article, but it should provide some information on the current risk environment as well as some guidance for employee decision making in this area. As discussed previously and particularly in Chapter 3, every enterprise should somewhat define and understand its appetite for risk. A newsletter or other communication can help deliver that message through the enterprise. Again using our Global Computer Products company, Exhibit 5.11 provides an example of an enterprise-wide

Global Computer Products

RISK AWARENESS NEWSLETTER

ENTERPRISE RISK MANAGEMENT NEWSLETTER V1.2

This is the second issue of the enterprise risk management group's employee newsletter to remind all stakeholders of the risks facing Global Computer Products and the steps we all can take in minimizing and controlling risks.

Risks and Sarbanes-Oxley. Many of our operating units have been asked to review and update the internal control documentation that was prepared in the prior period for our Sarbanes-Oxley 404 requirements. When you go through this review of determining if there have been any changes to your documented internal control processes in the last period, please complete that review with a risk awareness perspective. All employees should have received COSO ERM risk training over this past period. That training asked you to evaluate risks impacting us at all levels and to both report these concerns and to take steps to help minimize those risks.

… Ongoing Newsletter Discussion Follows …

EXHIBIT 5.11 RISK AWARENESS NEWSLETTER EXAMPLE

risk awareness communication. More suggestions on ERM communications and education programs are discussed in Chapter 12.

CRO AND AN EFFECTIVE ENTERPRISE RISK MANAGEMENT FUNCTION

Both the position of a CRO and a supporting formal ERM function are new to many enterprises today. However, to implement this very important function or concept of COSO ERM, an enterprise should establish both of these concepts. An effective ERM group will improve the overall enterprise controls environment and will improve many of the procedures discussed throughout this book. While the enterprise risk function, as discussed, can operate similar to an internal audit function with its own RAR reviews, it is important to remember that the CRO and the designated risk management function have a significant overall responsibility for helping to launch and manage the overall COSO ERM framework as described in Exhibit 3.1. That three-dimensional framework included eight levels of risk management such as risk assessments and control activities in one dimension, with considerations given to all levels of the enterprise in a second dimension. The third dimension covered the compliance, reporting, operations, and strategic elements of risk management covering those other two dimensions or perspectives.

Will a single CRO or even a relatively small ERM group be able to effectively manage all aspects of such a complex COSO ERM framework? This is not just a job that can be handled by one person or group. Effective team and responsibility structures and linkages must be built. The CEO of a corporation is certainly not responsible for every activity that takes place on a day-to-day basis, but should have control and reporting processes in place to make certain the overall processes are performed as defined and that problems are communicated at appropriate levels, with that CEO and the board having final responsibility in "the buck stops here" sense.

The CRO and the ERM function should have broad oversight responsibilities in monitoring and establishing processes to manage the overall ERM function. This will require considerable communication and education such that staff at all levels can be better aware of the risks surrounding their areas of activities and can accept or reject those risks with a risk appetite that is consistent with overall enterprise high-level guidelines.

This chapter has described an ERM function—following the COSO ERM framework—that is, a somewhat new function to most enterprises today. This new function is closer to internal audit than the traditional risk-related

insurance functions, but it cannot be just another function that is part of an internal audit group. An effective ERM department, led by a strong CRO with high-level reporting responsibilities should become an important component in many major enterprise organizations going forward.

NOTES

1. *See* Robert R. Moeller, *Brink's Modern Internal Auditing,* 6th ed., Chapter 12, "Internal Audit Professional Standards." Hoboken, NJ: John Wiley & Sons, 2005.
2. For a better understanding of these internal audit processes, see Moeller, *Brink's Modern Internal Auditing,* 6th ed.
3. *See* note 1.

6

INTEGRATING ERM WITH COSO INTERNAL CONTROLS

Often confused by their similar names and the same sponsors, the Committee of Sponsoring Organizations (COSO) internal controls and their enterprise risk management (ERM) framework represent two different approaches to understanding internal controls and risk-related processes in today's enterprise. While much of this book has discussed COSO ERM, this chapter will look at the COSO internal controls framework and its risk-related relationships with COSO ERM. Professionals need to recognize that these are two rather different frameworks or models. All too often and almost up to the present, many have referred to the COSO internal controls framework as just "COSO" or "COSO #1" with the similarly named but different COSO ERM framework sometimes called "COSO #2".

This chapter looks at the components and objectives of the COSO internal control framework as well as some background on its origins. Since the COSO internal controls framework has a risk component, we will discuss its relationship to COSO ERM. An overall objective of

this chapter will be to describe how managers can use and apply effective ERM practices when building strong COSO internal control practices.

COSO INTERNAL CONTROLS: BACKGROUND AND EARLIER LEGISLATION

The concept of internal control has been used by business professionals since the very early days of auditing to define the process of how management mechanisms work. Internal control descriptions and definitions were first developed by the American Institute of Certified Public Accountants (AICPA) in the United States and were then used by the Securities and Exchange Commission (SEC) in the United States to help develop the Securities Exchange Act of 1934. Although there have been changes over the years, the AICPA's first standards were codified and called the Statement on Auditing Standards (SAS No. 1[1]). This standard was a key component defining the practice of financial statement auditing in the United States for many years and was also similar to definitions used by the Canadian Institute of Chartered Accountants (CICA). SAS No. 1 used the following definition to describe internal control:

> Internal control comprises the plan of enterprise and all of the coordinate methods and measures adopted with a business to safeguard its assets, check the accuracy and reliability of its accounting data, promote operational efficiency, and encourage adherence to prescribed managerial policies.

The original AICPA SAS No. 1 was further modified to add the concepts of administrative controls and accounting controls to its basic internal control definition. These two definitions are:

> Administrative control: "includes, but is not limited to, the plan of enterprise and the procedures and records that are concerned with the decision processes leading to management's authorization of transactions. Such authorization is a management function directly associated with the responsibility for achieving the objectives of the enterprise and is the starting point for establishing accounting control of transactions."
>
> Accounting control: "comprises the plan of enterprise and the procedures and records that are concerned with the safeguarding of assets and the reliability of financial records and consequently are designed to provide reasonable assurance that:
>
> a. Transactions are executed in accordance with management's general or specific authorization.

b. Transactions are recorded as necessary (1) to permit preparation of financial statements in conformity with generally accepted accounting principles or any other criteria applicable to such statements and (2) to maintain accountability for assets.
c. Access to assets is permitted only in accordance with management's authorization.
d. The recorded accountability for assets is compared with the existing assets at reasonable intervals and appropriate action is taken with respect to any differences."

These overlapping relationships of the two types of internal controls were then further discussed in pre-1988 AICPA standards:

> The foregoing definitions are not necessarily mutually exclusive because some of the procedures and records comprehended in accounting control may also be involved in administrative control. For example, sales and cost records classified by products may be used for accounting control purposes and also in making management decisions concerning unit prices or other aspects of operations. Such multiple uses of procedures or records, however, are not critical for the purposes of this section because it is concerned primarily with clarifying the outer boundary of accounting control. Examples of records used solely for administrative control are those pertaining to customers contacted by salesmen and to defective work by production employees maintained only for evaluating personnel performance.

The point here is that the definition of internal control, as then defined by the AICPA, had been subject to changes and reinterpretations over the years. However, these earlier AICPA standards stress that the system of internal control extends beyond just matters relating directly to accounting and financial statements. Over this period through the 1970s, there were many internal controls guidelines published by the SEC and AICPA as well as voluminous interpretations and guidelines developed by major CPA firms. These early and very general definitions led up to some of the following various legislative actions that are predecessors to today's Sarbanes-Oxley Act (SOx).

Foreign Corrupt Practices Act of 1977

Just as the scandals at Enron and others in the early years of this century brought us SOx, the United States experienced a similar situation some 30 years earlier. The period of 1974 through 1977 was a time of extreme social and political turmoil in the United States. The 1972 presidential election was surrounded by allegations of a series of illegal and questionable acts that eventually led to President Nixon's resignation. The events were first precipitated by a burglary of the Democrat party headquarters, then located

in a building complex known as Watergate. The resulting scandal and related investigations became known as the Watergate affair, and investigators found, among other matters, that various bribes and other questionable practices had occurred. All of these seemed questionable but were not covered by then existing legislation.

In 1976, the SEC submitted to the U.S. Senate a report on its Watergate-related investigations into these various questionable or potentially illegal corporate payments and practices. (The phrase *potentially illegal* is used because many legal statutes in place at the time were somewhat vague regarding these activities.) As federal legislation to prohibit such bribes and other questionable payments, the Foreign Corrupt Practices Act (FCPA) was enacted in December 1977. In addition to some strong antibribery rules, the Act contained provisions requiring the maintenance of accurate books and records and the implementation of systems of internal accounting controls. The FCPA provisions apply to virtually all U.S. companies with SEC-registered securities. Using terminology taken directly from the Act, SEC-regulated enterprises must:

- Make and keep books, records, and accounts, which, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the issuers,
- Devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that:
  - Transactions are executed in accordance with management's general or specific authorization,
  - Transactions are recorded as necessary both to permit the preparation of financial statements in conformity with generally accepted accounting principles (GAAP) or any other criteria applicable to such statements, and also to maintain accountability for assets,
- Access to assets is permitted only in accordance with management's general or specific authorization, and
- The recorded accountability for assets is compared with the existing assets at reasonable intervals, and appropriate action is taken with respect to any differences.

The special significance of FCPA requirements was that, for the first time, management was made responsible for maintaining an adequate system of internal accounting control. The Act required enterprises to "make and keep books, records, and accounts, which in reasonable detail, accurately and

fairly reflect the transactions and dispositions of the assets of the issuer." Similar to today's SOx, the FCPA record-keeping requirements applied to all public corporations registered with the SEC.

In addition, the FCPA required that enterprises keep records that accurately reflect their transactions "in reasonable detail." While there was no exact definition here, the intent of the rule was that records should reflect transactions in conformity with accepted methods of recording economic events, preventing off-the-books "slush funds" and payments of bribes. The FCPA also required that companies with registered securities maintain a system of internal accounting controls, sufficient to provide reasonable assurances that transactions are authorized and recorded to permit preparation of financial statements in conformity with GAAP. The FCPA also states that accountability is to be maintained for assets, access to assets is permitted only as authorized, and recorded assets are to be physically inventoried periodically, with any significant differences analyzed.

The main reason for the FCPA, the bribery provisions, are applicable to both SEC registered corporations and all other U.S. domestic concerns. The Act prohibits bribes to foreign officials to influence or assist an enterprise in obtaining business, with the offer or gift intended to induce the recipient to misuse an official position, such as to direct business to the payer or a client. Excluded from the definition of foreign official are government employees whose functions are clerical or ministerial in nature. Thus, so-called grease payments to minor officials to get their help in expediting some process are permissible. Passed over 25 years ago, the FCPA introduced a strong set of governance rules to U.S. corporations; because of the FCPA, many companies' boards of directors and their audit committees began to take an active part in directing reviews of internal controls.

The FCPA Aftermath: What Happened?

When enacted, the FCPA resulted in a flurry of activity among major U.S. corporations. Many enterprises then initiated major efforts to assess and document their systems of internal control. However, there was no clear and consistent definition at that time regarding what was meant by the term "internal controls." Enterprises that had never formally documented procedures, despite a long chain of internal audit reports pointing out that weakness, now embarked on major documentation efforts. This responsibility for FCPA documentation was often given to internal audit departments who used their best efforts to comply with the internal control provisions of the Act. The reader should recall that this was in the late 1970s and very early

1980s when most automated systems were mainframe batch oriented, and graphics tools were often little more than plastic flowchart templates and number 2 pencils.

Considerable efforts were expended in establishing compliance with the FCPA, and many consultants and seminar presenters became wealthier in the process. One of the major public accounting firms at that time ran a series of advertisements in major business publications showing a small flowchart template with a message that this firm could use these templates to help client enterprises solve their FCPA problems. Of course, much more was needed than a flowchart template. Even though systems and processes change relatively often, many large enterprises developed extensive sets of paper-based systems documentation with no provisions, once they had been completed, to update them. As a result of the FCPA, many enterprises also strengthened their internal audit departments significantly.

Many anticipated a wave of additional regulations or legal initiatives following the enactment of the FCPA. However, this did not occur. Legal actions were essentially nonexistent, no government auditors or regulators came to inspect the files of assembled documentation, and today the FCPA has dropped off of the list of current ''hot'' legislative concerns. The FCPA is still very much in force, but is more recognized as an anticorruption, antibribery law. An FCPA-related search on the Web today will yield few if any references to the Act's internal control provisions. The law was amended in the early 1990s but only to strengthen and improve its anticorruption provisions.

When enacted in 1977, the FCPA emphasized the importance of effective internal controls for many U.S. corporations. Although there was no consistent definition at the time, the law heightened the importance of internal controls in the corporation. Its antibribery provisions are and continue to be important. It was an important first step for helping enterprises to establish effective internal controls. Although it dates back to an era of minimal automation and many manual processes, it provided a good precursor to today's SOx requirements. Perhaps if there had been more efforts in achieving FCPA internal controls compliance years ago, we would never have had some of the issues that led to today's SOx.

Efforts Leading to the Treadway Commission

With all of the various published approaches for documenting internal controls, it soon became obvious to many, including auditors and business financial managers, that there was no clear and consistent understanding of

what was meant by the term "internal control." As an example, external auditors thought in terms of "internal accounting control," while internal auditors had their broader definitions that included both financial and operational controls. Concurrent with these internal control definition friendly debates, the financial press and others in the United States began to call for external auditors to express an opinion on the adequacy of an enterprise's internal controls as part of their audits of financial statements. We are now well into the twenty-first century and these events happened in the late 1980s. Nevertheless, these events lead to why we have COSO internal control today.

In those late 1970s times, external auditors reported only that an enterprise's financial statements were "fairly presented." There was no mention of the adequacy of internal control procedures supporting those audited financial statements. The FCPA legislation had a requirement for enterprises to document their internal controls but did not ask external auditors to attest to whether an enterprise under audit was in compliance with these internal control reporting requirements. The SEC subsequently began a series of studies and reports over about a ten-year period to better define both the meaning of internal control and the external auditor's responsibility for reporting on the adequacy of those controls.

AICPA and CICA Commissions on Auditor Responsibilities. The AICPA had formed a high-level commission on auditors' responsibilities in 1974 to study the external auditor's responsibility for reporting on internal controls. This group, better known then as the Cohen Commission, released its report in 1978, recommending that corporate management be required to present a statement on the condition of their company's internal controls along with the financial statements. These Cohen Commission initiatives were taking place concurrently with the development and initial publication of the FCPA. At about the same time, the CICA's Commission on Auditor Expectations released a report in 1978 with similar conclusions.

In the United States, the Cohen Commission's report initially ran into a torrent of criticism. In particular, the report's recommendations were not precise on what was meant by "reporting on internal controls," and external auditors strongly expressed concerns about their roles in this process. Many external auditors were concerned about potential liabilities if their reports on internal control gave inconsistent signals due to a lack of understanding over what were internal control standards. Although auditors were accustomed to attesting to the fairness of financial statements, the Cohen Commission report suggested that they should express an audit opinion on

the fairness of the management control assertions in the proposed financial statement internal control letter. The issue was again raised that management did not have a consistent definition of internal control. Different enterprises might use the same terms regarding the quality of their internal controls, with each meaning something a little different. If an enterprise reported that its controls were "adequate" and if its auditors "blessed" these assertions in their internal controls report, the external auditor could later be criticized or even suffer potential litigation if some significant control problems appeared later.

The Financial Executives Institute (FEI) then got involved in this internal controls reporting controversy. Just as the Institute of Internal Auditors (IIA) is the professional enterprise for internal auditors and the AICPA or CICA represents the public accountants in the United States and Canada, respectively, the FEI represents senior financial officers in enterprises. The FEI endorsed the Cohen Commission's recommendations on internal control reports and suggested that publicly held enterprises should report on the status of their internal accounting controls. With all of this late 1970s activity, publicly held corporations began to discuss the adequacy of their internal controls as part of their annual report management letters. These internal control letters were entirely voluntary and typically included comments stating that management, often through its internal auditors, had periodically assessed the quality of its internal controls. The same letters sometimes included "negative assurance" comments indicating that nothing was found to indicate that there might be an internal control problem in operations.

The term *negative assurance* will return again in this discussion of internal controls. Because an external auditor cannot detect all problems and because of the risk of potential litigation, their reports often have been stated in terms of a negative assurance. That is, rather than saying that they "found no problems" in an area under review, an external auditor would state that they did not find anything that would lead them to believe that there was a problem. This is a subtle but important difference.

SEC 1979 Internal Control Reporting Proposal. Using both the Cohen Commission's and FEI's recommendations, the SEC subsequently issued proposed rules calling for *mandatory* management reports on an entity's internal accounting control system. The SEC stated that information on the effectiveness of an entity's internal control system was necessary to allow investors to better evaluate both management's performance and the integrity of published financial reports. This SEC proposal raised a storm of

controversy. First, many CEOs and CFOs felt that this was an onerous requirement on top of the newly enacted FCPA regulations.

Questions were once again raised from many directions regarding the definition of internal accounting control, and while enterprises might agree to voluntary reporting, they did not want to subject themselves to the civil and legal penalties associated with a violation of SEC regulations. The SEC soon dropped this 1979 internal control reporting proposal, but promised to re-release the regulations at a later date. The SEC proposal was important, however, in that it emphasized the need for a separate management report on internal accounting controls as part of the annual report to shareholders and the required SEC filings. This tentative regulation caused larger public companies to begin to issue voluntary internal control comments or letters in their annual reports. Moving more to the present, these then controversial regulatory requirements are similar to today's SOx Section 404 rules, as summarized in Chapter 7.

Minahan Committee and Financial Executives Research Foundation. In parallel with the SEC's proposed rules on internal control reporting, the AICPA formed yet another committee, the Special Advisory Committee on Internal Control (the Minahan Committee). Their 1979 report pointed out the lack of management guidance on internal control procedures and acknowledged that most of the published guidance on internal controls was found only in the accounting and auditing literature. This guidance would not necessarily come to the attention of or be completely relevant to a business manager in other areas of an enterprise, such as operations, who had a need to understand internal control concepts.

At about the same time, the FEI Research Foundation (FEIRF) researched published literature and considered definitions used for the characteristics, conditions, practices, and procedures that define internal control systems. One of these reports[2] pointed out the vast differences in the definitions of various professional standards-setting groups in what constitutes an effective system of internal control. The FEIRF also released a related research study in 1980[3] that attempted to define the broad, conceptual criteria for evaluating internal control.

These two efforts pointed out the need to find a better and more consistent meaning of internal controls. A regulatory group such as the SEC could not then realistically draft requirements for reporting for internal control unless both the enterprises developing those reports and the investors who read them all had a consistent understanding of the concept.

Earlier AICPA Auditing Standards: SAS No. 55. Prior to SOx, the AICPA was responsible for external audit standards through what was called Statements on Auditing Standards (SASs) that were released from time to time and were codified in an overall set of professional standards. As discussed previously regarding SAS No. 1, these standards were once almost engraved in stone, with few changes from year to year. They formed the basis of the external auditor's review and evaluation of financial statements. During this same period of the 1970s and 1980s, the public accounting profession, in general, and the AICPA were criticized that their standards did not provide adequate guidance to either external auditors or the users of these reports. This problem was called the "expectations gap," or that the public accounting standards did not meet the expectations of investors.

To answer this need, the AICPA released a series of new SASs on internal control-related auditing standards during the period of 1980 to 1985. These standards were viewed by critics of the public accounting profession as being too little and too late. For example, SAS No. 48, *The Effects of Computer Processing on the Examination of Financial Statements,* was issued in 1984 and provided guidance on the need to review both the computer systems applications controls and such general controls as physical security. Although there had been massive technological changes in the way computer systems were constructed, at the time SAS No. 48 was issued, external auditors were still using guidance from the early 1970s.

The AICPA subsequently released a whole new series of auditing standards that better defined many problem areas facing external auditors. One of these, SAS No. 55, defined internal control from the perspective of the external auditor and defined internal control in terms of three elements:

1. The control environment
2. The accounting system
3. The control procedures

SAS No. 55 presented a somewhat different approach to understanding internal controls than had been used by the AICPA in the past, or by other standards setting groups, such as the IIA.

An enterprise generally has other internal control structure policies and procedures that are not relevant to a financial statement audit and therefore are not considered by the external auditors. Examples include policies and procedures concerning the effectiveness, economy, and efficiency of certain management decision-making processes, such as setting of an appropriate price for products or deciding whether to make expenditures for

certain research and development activities. Although these processes are certainly important to the enterprise, they do not ordinarily relate to the external auditor's financial statement audit.

SAS No. 55 defined internal control in much broader scope than had been traditionally taken by external auditors and provided a basis for the COSO's definition of internal control. The interests of internal auditors extend beyond internal accounting control to the effectiveness of the total system of internal control, and that internal accounting control is part of a larger system. SAS No. 55 became effective in 1990 and represented a major stride toward providing an appropriate definition of internal control.

Treadway Commission Report. In addition to the previously discussed events that led to the FCPA, the later 1970s and early 1980s were a period of many major enterprise failures in the United States caused by high inflation rates, the resultant high interest rates, and high energy costs due to excessive government regulation. During this time period, it was not unusual for an enterprise to report adequate earnings in its published financial reports, with external auditors attesting that these same financial reports were fairly stated, only to have the enterprise suffer a financial collapse shortly after the release of such favorable audited financial reports. Some of these failures were caused by fraudulent financial reporting, although many others were caused by high inflation or other factors causing the overall instability. At that time, congressional legislation was proposed to "correct" these potential business and audit failures, but no legislation was passed.

After much public debate and as a response to these concerns, the National Commission on Fraudulent Financial Reporting was formed. Five professional enterprises sponsored the Commission: the IIA, the AICPA, and the FEI, all discussed previously, as well as the American Accounting Association (AAA) and the Institute of Management Accountants (IMA). The AAA is the academic professional accountants' enterprise. The IMA is the professional enterprise for managerial or cost accountants. This enterprise, formerly called the National Association of Accountants, sponsors the Certificate in Management Accounting (CMA).

The National Commission on Fraudulent Reporting (the Treadway Commission, named after its chairperson) had as its major objectives the identification of the causal factors that allowed fraudulent financial reporting and the making of recommendations to reduce their incidence. The Treadway Commission's final report was issued in 1987[4] and included recommendations to management, boards of directors, the public accounting profession,

and others. The Treadway Commission report again called for management reports on the effectiveness of their internal control systems and emphasized key elements in what it felt should be an effective system of internal control, including a strong control environment, codes of conduct, a competent and involved audit committee, and a strong internal audit function. The Treadway Commission report again pointed out the lack of a consistent definition of internal control, suggesting further work was needed. The same Committee of Sponsoring Enterprises (COSO) that had managed the Treadway report, subsequently contracted with outside specialists and embarked on a new project to define internal control. Although it established no standards, the Treadway report was important as it raised the level of concern and attention regarding reporting on internal control.

The internal control–reporting efforts discussed here are presented as if they were a series of sequential events. In reality, many of the internal control–related efforts took place in almost a parallel fashion. This massive effort over nearly a 20-year period redefined internal control, a basic concept for all managers and auditors; it increased the responsibility of many other participants in an enterprise's control structure. The result has been the COSO internal control framework, discussed in the sections following and elsewhere in this book.

COSO INTERNAL CONTROL FRAMEWORK

As mentioned, the acronym COSO stands for the five sponsoring professional auditing and accounting organizations that developed this internal control report; its official title is *Internal Control—Integrated Framework* (COSO internal control report). The sponsoring enterprises contracted with a public accounting firm, used a large number of volunteers to research and develop the report, and then released a draft in 1990 for public exposure and comment. More than 40,000 copies of the COSO draft version were sent for comment to corporate officers, internal and external auditors, legislators, academics, and other interested parties. Formal comments regarding this draft were requested and the internal control review procedures portion of the study, discussed in the sections following, were field-tested by five public accounting firms.

The final COSO internal controls report was released in September 1992.[5] The report proposed a common framework for the definition of internal control, as well as procedures to evaluate those controls. In a very short number of years, the COSO framework has become the recognized

framework or standard for understanding and establishing effective internal controls in virtually all U.S. business enterprises.

COSO Internal Controls Framework Model

COSO internal controls are defined through a framework that looks very similar to the COSO ERM framework described in Chapter 3. In fact, because COSO internal controls came first, it can be inferred that the ERM framework followed internal controls, where virtually every public corporation has a complex control procedures structure. Following the description of a classic enterprise chart, there are levels of senior and middle management in its multiple operating units or within different activities. In addition, control procedures may be somewhat different at each of these levels and components. For example, one operating unit may operate in a regulated business environment where control processes are very structured, while another unit may be an entrepreneurial start-up operation with a less formal structure. Different levels of management in these enterprises will have different control concern perspectives. The question ''How do you describe your system of internal controls?'' might receive different answers from persons in different levels in each of these enterprise components.

This COSO report provides an excellent description of this multidimensional concept of internal controls. It defines internal control as follows:

> Internal control is a process, affected 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 definition should be very familiar to internal auditors. It follows the same theme that Vic Brink used as a definition of internal auditing in his first 1943 edition of *Modern Internal Auditing* and all subsequent editions. He defined internal auditing as follows:

> Internal auditing is an independent appraisal function established within an enterprise to examine and evaluate its activities as a service to the enterprise.[6]

While COSO focuses on financial reporting controls, Brink used the broader definition of service to management to define what the new profession of internal auditing was then. That definition is still important today.

Using this very general definition of internal control, COSO uses a three-dimensional model to describe an internal control system in an enterprise similar to the COSO enterprise risk management model presented in Chapter 3. Exhibit 1.1 defines the COSO model of internal control as a cube structure with five horizontal layered or interconnected components in one dimension. In the second dimension, the model is sliced between the three major components of internal controls: effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations. The model has a component for the separate entities and activities in an enterprise. The COSO internal control model will be discussed in more detail in the sections following.

While the COSO ERM model has eight horizontal layers or components–going from the monitoring component at its base to the internal environment on top, the COSO internal controls framework has five layers or components. Some of the names of each are the same—both models have a monitoring component—but the concepts somewhat differ. Some of these similarly named concepts provide different images. For example, the internal controls environment is depicted at the base or foundation for COSO internal controls while a similarly named component is at the head or top of the stack for ERM. Based on the elements described in Exhibit 1.1, we will discuss each of these COSO internal control components and how they relate to the COSO ERM framework introduced in Chapter 3.

COSO Internal Control Elements: The Control Environment. The COSO internal control framework has a base or foundation in an element called the *internal control environment*. The COSO internal control framework emphasizes that this internal control foundation has a pervasive influence on how business activities are structured and risks are assessed in any enterprise. The control environment serves as a foundation for all other components of internal control and has an influence on each of the three objectives and all activities. The control environment reflects the overall attitude, awareness, and actions by the board of directors, management, and others concerning the importance of internal control in the enterprise. Perhaps more of an issue of philosophy, COSO ERM calls this element the control environment and puts this element at the top of the stack of ERM elements. This ERM view makes its foundation component more of a keystone component, keeping supporting components together.

For many organizations, history and culture often play a major role in forming this control environment. If an enterprise historically has had a strong management emphasis on producing error-free products and if

senior management continues to emphasize the importance of high-quality products, this message will be communicated to all levels and becomes a major control environment factor for the enterprise. However, if senior management has had a reputation of "looking the other way" at policy violations, this message will be similarly communicated to other levels in the enterprise. A positive "tone at the top" by senior management will establish the control environment for the enterprise.

The following sections outline other major elements of the COSO control environment component of internal control. While some of these are defined through formal policies and procedures in larger organizations, similar factors will be more informal in smaller enterprises. Factors such as integrity and ethical values have the same names and are very different concepts between the internal controls and the ERM frameworks. In other cases, they are essentially the same.

Integrity and Ethical Values

The collective integrity and ethical values of an enterprise are essential elements of its internal controls environment. These factors are often defined through ''tone at the top'' messages communicated by senior management. If the enterprise has developed a strong code of conduct that emphasizes integrity and ethical values, and if all stakeholders appear to follow that code, internal audit will have assurances that the enterprise has a good set of integrity and ethical values.

A code of ethics or conduct is an important component of enterprise governance, but these principles can often be violated through employee ignorance in addition to deliberate malfeasance. In many instances, employees may not know that they are doing something wrong or may erroneously believe that their actions are in the enterprise's best interests. This ignorance is often caused by poor moral guidance by senior management rather than by any employee intent to deceive. An enterprise's policies and values must be communicated to all levels of the enterprise. While there can always be ''bad apples'' in any enterprise, a strong moral message will encourage everyone to act correctly. When performing a review in a given area, the internal auditor should always ask questions to determine if appropriate messages or signals have been transmitted throughout the enterprise. The enterprise's code of conduct and how it is applied throughout the enterprise is important. If the code is out of date, if it does not appear to address important ethical issues facing an enterprise, or if management does not appear to be communicating the code to all stakeholders on a recurring basis, this internal control environment will be weakened.

While the code of conduct describes the rules for ethical behavior in an enterprise and while senior members of management should transmit a proper ethical message throughout their enterprise, other incentives and temptations can erode this overall control environment. Individuals in the enterprise may engage in dishonest, illegal, or unethical acts if their enterprise gives them strong incentives or temptations to do so. For example, an enterprise may establish very high, unrealistic performance targets for sales or production quotas. If there are strong rewards for the achievement of these performance goals—or worse, strong threats for any missed targets—employees may be encouraged to engage in fraudulent or questionable practices to achieve those goals. The kinds of temptations that encourage stakeholders to engage in improper accounting or similar acts include:

- Nonexistent or ineffective controls, such as poor segregation of duties in sensitive areas, that offer temptations to steal or to conceal poor performance
- High decentralization that leaves top management unaware of actions taken at lower enterprise levels and thereby reduces the chances of getting caught
- A weak internal audit function that has neither the ability nor the authority to detect and report improper behavior
- Penalties for improper behavior that are insignificant or unpublicized and thus lose their value as deterrents

There is a strong message here both for enterprise managers and internal auditors performing internal control of the enterprise. These control environment factors should always be considered when assessing this environment. A reviewer, such as an internal auditor, should always be skeptical and perform appropriate levels of tests when reviewing various areas of operations. When things look ''too good,'' the auditor or management reviewer might want to look a bit harder.

A strong internal audit function also should be a major component of the COSO control environment. If internal audit finds that management is placing constraints on its internal control review activities, internal audit should remind management of the importance of their function as part of the enterprise's overall internal control structure and should communicate these concerns to the audit committee to achieve corrective action.

Commitment to Competence

An enterprise's control environment can be seriously eroded if a significant number of positions are filled with persons lacking required job skills.

Because all humans have different levels of skills and abilities, adequate supervision and training should be available to help until proper skills are acquired.

An enterprise needs to specify the required competence levels for its various job tasks and to translate those requirements into necessary levels of knowledge and skill. By placing the proper people in appropriate jobs and giving adequate training when required, an enterprise is making an overall *commitment to competence*, an important element in the enterprise's overall control environment. This area is called human resource standards in COSO ERM where it does not receive the same level of emphasis as in COSO internal controls.

Board of Directors and Audit Committee

The COSO internal control environment is very much influenced by the actions of an enterprise's board of directors and its audit committee. In the years prior to SOx, boards and their audit committees often were dominated by senior management, with only limited, minority representation from outside members. This created situations wherein the boards were not totally independent of management. Company officers sat on the board and were, in effect, managing themselves, often with less concern for the outside investors. SOx has changed all of that, and boards now have a more important corporate governance role, with audit committees now required to be truly independent.

An active and independent board is an essential component of both an enterprise's internal control environment under both COSO internal controls and ERM. By setting high-level policies and reviewing overall enterprise conduct, the board and its audit committee have the ultimate responsibility for setting this ''tone at the top.''

Management's Philosophy and Operating Style

Words that are not found in COSO ERM, the philosophy and operating style of top management, have a considerable influence over an enterprise's control environment. Some top-level managers frequently take significant enterprise risks in their new business or product ventures, while others are very cautious or conservative. Some managers seem to operate by the "seat of the pants," while others insist that everything must be properly approved and documented. Still others take very aggressive approaches in their interpretations of tax and financial-reporting rules while some go strictly by the book. These comments do not necessarily mean that one approach is

always good and the other bad. A small, entrepreneurial enterprise may be forced to take certain business risks to remain competitive while one in a highly regulated industry would be risk averse. Called an enterprise's appetite for risk, this concept—a key component of COSO ERM—was discussed in Chapter 3.

These management philosophy and operational style considerations are all part of an enterprise's control environment. Internal auditors and others responsible for assessing internal controls, such as the ERM group introduced in Chapter 5, should understand these factors and take them into consideration when evaluating the effectiveness of internal controls. While no one set of styles and philosophies is always the best for all enterprises, these factors are important when considering the other components of internal control in an enterprise.

Enterprise Structure

The enterprise structure component of COSO internal controls provides a framework for planning, executing, controlling, and monitoring activities for achieving overall objectives. This is an aspect of the control environment——also found in COSO ERM—that relates to the way various functions are managed and organized, following the classic enterprise chart. Some enterprises are highly centralized, while others are decentralized by product, geography, or other factors. Still others are organized in a matrix manner with no single direct lines of reporting. Enterprise structure is a very important aspect of the enterprise's control environment. No one structure provides a preferred environment for internal controls.

An enterprise can be described as the way individual work efforts are both assigned and subsequently integrated for the achievement of overall goals. While in a sense this concept could be applied to the manner in which a single individual organizes efforts, it is more applicable when a number of people are involved in a group effort. For a large modern corporation, a strong plan of organizational control is an important component of the system of internal control. Individuals and subgroups must have an understanding of the total goals and objectives of the group or entity of which they are a part. Without such an understanding, there can be significant control weaknesses.

Every enterprise or entity—whether a business, government, philanthrop, or other type of unit—needs an effective plan of enterprise. The internal auditor needs to have a good understanding of this organizational structure and the resultant reporting relationships, whether a functional, decentralized, or matrix enterprise structure. Often, a weakness in enterprise

controls can have a pervasive effect throughout the total control environment. Despite clear lines of authority, enterprises sometimes have built-in inefficiencies that become greater as they expand in size. These inefficiencies can often cause control procedures to break down, and the auditor should be aware of them when evaluating the control environment in the functional enterprise.

Assignment of Authority and Responsibility

The COSO guidance for internal controls here is essentially the same as found in COSO ERM, and previously discussed in Chapter 3. An enterprise's structure defines the assignment, integration, and duties of the total work effort. The assignment of authority is essentially the way responsibilities are defined in terms of job descriptions and structured in terms of organization charts. Although job assignments can never fully escape some overlapping or joint responsibilities, the more precisely they can be stated and formally defined, the better. Unclear or poorly documented guidance on how job responsibilities will be assigned is often a cause of confusion and conflict between individual and group work efforts.

Enterprises of all types and sizes today have pushed their decision-making authority downward and closer to the front-line personnel. The idea is that these front-line employees should have the knowledge and power to make important decisions in their own area of operations rather than be required to pass the request for a decision up through enterprise channels. The critical challenge that goes with this delegation or empowerment is that although it can delegate some authority in order to achieve its objectives, senior management is ultimately responsible for any decisions made by those subordinates. A key component here is that those decisions will involve the understanding and acceptance of various risks at several levels. An enterprise can place itself at risk if too many decisions involving higher-level objectives are assigned at inappropriately lower levels without adequate management review. In addition, each person in the enterprise must have a good understanding of the enterprise's overall objectives as well as how individual actions interrelate to achieve those objectives. The framework section of the COSO internal control report describes this very important area of the control environment as follows:

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

This same paragraph exists in COSO ERM controls with only two small differences. ERM talks about the "internal environment" rather than the control environment—perhaps a difference in semantics. More importantly, ERM references "*the chief executive, who with board oversight, has …"* This really says that COSO ERM better recognizes the expanded responsibility of the board in these processes.

Human Resources Policies and Practices

Again the same general concepts as found in COSO ERM, human resource practices cover such areas as hiring, orientation, training, evaluating, counseling, promoting, compensating, and taking appropriate remedial actions. While the human resources function should have adequate published policies in these areas, their actual practice areas send strong messages to employees regarding their expected levels of ethical behavior and competence. The higher-level employee who openly abuses a human resources policy, such as a violation of plant floor dress codes, quickly sends a message to other levels in the enterprise. The message grows even louder when a lower-level employee is disciplined for the same unauthorized violation while everyone looks the other way at the higher-level violator.

The COSO internal control framework gives more attention to human resources than does ERM. This may be because human resource-related problems present a greater challenge to effective internal controls than enterprise-wide risks. Areas where internal control human resources policies and practices are particularly important include:

- *Recruitment and hiring.* The enterprise should take steps to hire the best, most qualified candidates. Potential employees should be checked to verify their educational backgrounds and prior work experiences. Interviews should be well organized and in-depth. They should also transmit a message to the prospective candidate about the enterprise's values, culture, and operating style.
- *New employee orientation.* A clear signal should be given to new employees regarding the enterprise's value system and the consequences of noncompliance. This is when new employees are introduced to the code of conduct and asked to formally acknowledge acceptance of that code. Without these messages, new employees may join the enterprise lacking an appropriate understanding of its values.
- *Evaluation, promotion, and compensation.* There should be a fair performance-evaluation program in place that is not subject to an

excessive amount of managerial discretion. Because issues such as evaluation and compensation can violate employee confidentiality, the overall system should be established in a manner that appears to be fair to all.

- *Disciplinary actions.* There should be consistent and well-understood policies for disciplinary actions. All employees should know that if they violate certain rules, they will be subject to a progression of disciplinary actions leading up to dismissal. The enterprise should take care to ensure that no double standard exists for disciplinary actions—or, if any such double standard does exist, that higher-level employees are subject to even more severe disciplinary actions.

Effective human resource policies and procedures are a critical component in the overall control environment. Messages from the top of strong enterprise structures will accomplish little if the enterprise does not have strong human resource policies and procedures in place. Internal audit should always consider this element of the control environment when performing reviews of other elements of the internal control framework.

COSO Internal Control Environment in Perspective

In the internal controls framework, this component is placed at the lowest or foundation level of the framework. Just as a strong foundation is essential for a multistory building, the control environment provides the foundation for the other components of internal control. An enterprise that is building a strong internal control structure should give special attention to placing solid foundation bricks in this control environment foundation. The ERM framework places this very similar framework at the head of a stack of other ERM components. The placement of internal environment factors above all other components gives COSO ERM internal environment factors a "tone at the top" type of message.

Risk Assessment. In the Exhibit 1.1 COSO internal control framework description, the next level or layer above the control foundation is risk assessment. The focus under COSO internal controls is that an enterprise's ability to achieve its objectives can be at risk due to a variety of internal and external factors. An enterprise should have a process in place to evaluate the potential risks that may impact attainment of its various objectives. The internal controls component here is called risk assessment, while ERM talks about risk response. Similar names but differences that will be discussed in this section.

While this type of risk assessment process does not need to be a formal quantitative risk assessment exercise, as was discussed in Chapter 2, there should be a minimal understanding of the risk assessment process for an entity. Internal control–related risk assessments should be a forward-looking processes performed at all levels and for virtually all activities within the enterprise—essentially the same as COSO ERM. The internal control framework describes risk assessment as a three-step process:

1. Estimate the significance of the risk.
2. Assess the likelihood or frequency of the risk's occurring.
3. Consider how the risk should be managed and assess what actions must be taken.

The COSO internal control framework risk assessment process places a responsibility on management to go through the steps to assess whether a risk is significant and then, if so, to take appropriate actions. COSO, here, emphasizes that risk analysis is not a theoretical process, but often can be critical to an entity's overall success. As part of its overall assessment of internal control, management should take steps to assess these risks that may impact the overall enterprise, as well as the risks over various enterprise activities or entities. A variety of risks, caused by either internal or external sources, are included in the COSO internal control framework as follows:

- *Risks due to external factors.* Technological developments can affect the nature and timing of research and development or lead to changes in procurement processes. Other external factor risks include changing customer needs or expectations that can affect product development, production, pricing, or warranties or new product competition that can alter marketing or service activities. New legislation or regulations can force changes in operating policies or strategies, and catastrophes, such as the World Trade Center 9/11 terrorist attack, can lead to changes in operations and highlight the need for contingency planning.
- *Risks due to internal factors.* A disruption in the enterprise's information systems processing facility can adversely affect the entity's overall operations. Also, the quality of personnel hired and methods of training and motivation can influence the level of control consciousness within the entity, and the extent of employee accessibility to assets can contribute to misappropriation of resources.
- *Specific activity-level risks.* In addition to enterprise-wide risks, specific risk areas should also be considered at each significant business

unit and key activity, such as marketing or information systems. This is very similar to the ERM framework, where risks are to be considered on a business unit and smaller subunit level.

The risk assessment element of the COSO internal controls framework is an area where there has been some misunderstanding and confusion. COSO ERM was released after the COSO internal control framework, but the COSO-released guidance material has not done as much as might be expected in explaining their differences. In addition, as was summarized in Chapter 1, the AICPA's Auditing Standards Board (ASB) recently announced a new series of auditing standards based on risk.[7] However, these new ASB auditing standards really only apply to smaller, nonpublic organizations since the Public Company Accounting Oversight Board (PCAOB) is responsible for determining auditing standards for most larger corporations. The key point here is that evaluating, assessing, and working through risks is very important, whether within specific enterprise functions or throughout the overall enterprise.

Control Activities. The next layer up in the COSO internal controls framework is called control activities. The COSO ERM framework, as was discussed in Chapter 3, has a component with the same name and with similar internal control considerations. Control activities are the policies and procedures that help ensure that actions identified to address risks are carried out. This internal control component includes a wide range of activities and procedures, from establishing enterprise standards with appropriate segregation of duties to reviewing and approving key operation reports properly. Control activities should exist at all levels within the enterprise, and in many cases they may overlap one another.

The concept of control activities should be familiar to managers or internal auditors who develop procedures such as to test whether invoice records from an account payable (AP) system were properly coded and discounts properly calculated. Each would use different item-checking processes, but there should be specific control-related process in place to determine accuracy.

Control activities should be closely related to the identified risks discussed previously as part of the COSO internal controls risk assessment component. Internal control is a process, and appropriate control activities should be installed to address identified risks. Control activities should not be installed just because they seem to be the ''right thing to do'' if management has identified no significant risks in an area where some control activity would be installed. All too often, management may still have control

activities or procedures in place that perhaps once served some control-risk concern, although the concerns have largely gone away. A control activity procedure should not be discarded because there have not been control violation incidents in recent years, but management needs to periodically reevaluate the relative risks. All control activities should contribute to the overall control structure.

The preceding comments refer to what might be called ''dumb'' control activities that once had a purpose but over subsequent years accomplished little. Parking lots once gave receipts for attendant-parked cars, stating—in very fine print and with lots of legalistic terms—that the parking lot assumed no responsibility for much of anything regarding the parked car. Legal rulings have proved that the lot owner does have that responsibility, and the published rules on a parking lot ticket have little meaning today. While some controls will cease in their relative importance, other basic controls, such as the importance of strong separation of duties over incompatible functions, should always remain in effect.

The need for control activities, ranging from top-level reviews to basic segregation of duties controls, are essentially the same, whether installing them within the enterprise, for internal control purposes, or for the entire enterprise. These ERM control activities were summarized in Chapter 3, and the COSO internal control framework has control activities very similar to the ERM framework.

Communications and Information. Earlier COSO descriptions of the internal controls framework describe this component not as a horizontal layer but a component that spans across the other components. Both important portions of the internal control framework, information and communications, are related but are really very distinct internal control components. Appropriate information, supported by automated systems, must be communicated up and down in a manner and time frame that allow people to carry out their responsibilities. In addition to formal and informal communication systems, there should be effective procedures in place to communicate with internal and external parties. As part of any evaluation of internal controls, there is a need to have a good understanding of the information and communication flows or processes in the organization.

Relationship of Information and Internal Control

Various types of information are needed at all levels of the enterprise in order to achieve operational, financial reporting, and compliance objectives. The enterprise needs proper information to prepare the financial

reports that are communicated to outside investors. It also needs both internal cost information and external market preference information to make correct marketing decisions. This information must flow from the top levels of the enterprise on down to lower levels. COSO internal controls take a broad approach to the concept of an information system; it recognizes the importance of automated systems but makes the point that information systems can be manual, automated, or conceptual. Any of these information systems can be either formal or informal. Regular conversations with customers or suppliers can be highly important sources of information and are an informal type of information system. The effective enterprise should have information systems in place to listen to customer requests or complaints and to forward that customer-initiated information to appropriate personnel.

The COSO internal control framework also emphasizes the importance of keeping information and supporting systems consistent with overall enterprise needs. Information systems adapt to support changes on many levels. Although its application controls may be good, the information system may not support the current needs of the enterprise. The COSO internal control framework takes a broad view of information systems, both automated and manual, and points to the need to understand both manual systems processes and automated systems technologies.

Strategic and Integrated Systems. Accounting and financial processes were once the first automated systems in most enterprises, starting with the unit record or ''IBM card'' accounting machines in the 1950s and then moving to the earliest computer systems. While enterprises have upgraded their automated systems over time, their basic mix of supporting automated applications may not have changed significantly. An enterprise will have its general ledger, payroll, inventory, accounts receivable, accounts payable, and related financial-based processes as core information systems, without too much else. Both the COSO internal control and ERM frameworks suggest that the effective enterprise should go a step further and implement both strategic and integrated information systems.

By a strategic system, both frameworks suggest that management should consider the planning, design, and implementation of its information systems as part of its overall enterprise strategy. These strategic systems then support the enterprise's business and help it to carry out its overall business missions. There have been many examples of companies that developed strategic information systems to support their business strategies—systems that moved them even further forward. Examples here range from American

Airlines, which developed its SABRE automated reservation system back in the 1960s, greatly enhancing its ability to sell tickets and make more effective use of its resources, to Amazon.com, with its fairly recent one-click order fulfillment system for customer Internet orders. Not every enterprise has the resources to develop systems of the nature or scale of SABRE or Amazon; however, even smaller systems should be designed and developed to support the enterprise's strategies. These strategic systems allow enterprises to understand and to respond better to changes in their marketplaces and control environments.

COSO internal controls also emphasizes the importance of integrating automated information systems with other operations. Examples include a fully automated manufacturing system that controls both production machines and equipment inventories or a highly automated distribution system that controls inventory and schedules shipments. These comments about strategic information systems are a step forward or into the future when contrasted with the information systems–related comments from earlier internal control standards. The COSO internal control framework makes the point, however, that it is a mistake to assume that just because a system is new, it will provide better controls. Older systems have presumably been tried and tested through use, while the new system can have unknown or untested control weaknesses.

Quality of Information. Both COSO internal controls and ERM have sections on the importance of the quality of information. Poor-quality information systems, filled with errors and omissions, affect management's ability to make appropriate decisions. Reports should contain enough data and information to support effective control activities. The quality of information includes ascertaining whether:

- The content of reported information is appropriate.
- The information is timely and available when required.
- The information is current or at least the latest available.
- The data and information are correct.
- The information is accessible to appropriate parties.

These points all circle back to today's SOx requirements. While the COSO framework holds up these quality-of-information points as objectives, SOx effectively makes them requirements.

Communications Aspect of Internal Control

Communications is defined as a separate internal control element in COSO's internal control framework. Communication channels provide the

details to individuals to carry out their financial reporting, operational, and compliance responsibilities. COSO emphasizes that communication must take place in a broader sense in dealing with various individuals and groups and their expectations. The existence of appropriate channels of communication is an important element in the overall framework of both ERM and internal control. An enterprise needs to establish these communication channels throughout its various activities and between the enterprise and various interested outsiders. Although communication channels can have many dimensions, COSO highlights the separate components of internal and external communications.

Communications: Internal Components. According to the COSO internal control framework, perhaps the most important component of communication is that all stakeholders should periodically receive messages from senior management reminding them that their internal control responsibilities must be taken seriously. The clarity of this message is important to ensure that the overall enterprise follows effective internal control principles. This message is part of the ''tone at the top,'' discussed earlier as part of the control environment, and it should be communicated throughout the enterprise.

All stakeholders need to know limits and boundaries and when their activities may become unethical, illegal, or otherwise improper. People also need to know how to respond to errors or other unexpected events in the course of performing their duties. They typically require communication in terms of messages from management, procedure documentation, and adequate training. Communication must flow in two directions, and COSO internal controls emphasizes that stakeholders must have a mechanism to report matters upward throughout the enterprise. This upward communication has two components: communication through normal channels and special, confidential reporting. Normal reporting refers to the process in which members of the enterprises are expected to report status information, errors, or problems up through their supervisors. This communication should be freely encouraged, and the enterprise should avoid "shooting the messenger" when bad news is reported. Otherwise, it will be understood that employees should report only good news, and managers may not become aware of significant problems. Because personnel may sometimes be reluctant to report matters to their immediate supervisors, whistleblower programs are essential. This section of COSO internal controls concludes with the importance of communication channels between top management and the board of directors. Per the COSO internal control framework, now

in place for over 25 years, management should take care to inform the board of major developments, risks, and occurrences. The board, in turn, must independently review operations and communicate their concerns and decisions to management. These were recommendations as part of the COSO internal control framework that did not receive sufficient attention until SOx.

External Communications. Enterprises need to establish appropriate communication channels with interested outside parties, including customers, suppliers, shareholders, bankers, regulators, and others. This communication should go beyond the public relations type of function that large enterprises often establish to talk about themselves. Similar to internal communication channels, external information must flow in two directions. The information provided to outside parties should be relevant to their needs so they can better understand an enterprise and the challenges it faces. The enterprise that sends out highly optimistic reports to outsiders when many inside the enterprise realize there are problems is also giving an inappropriate message to its own employees. This is what was occurring in the events leading up to the passage of SOx when some enterprises were reporting overly optimistic if not fraudulent results.

External communications can also be a very important way to identify potential control problems. Customer complaints, involving such matters as service, billings, or product quality, often can point out significant operating and control problems. Independent mechanisms should be established to receive these messages and to appropriately act on them. This form of communication should be investigated and corrective action taken when necessary.

Management also should establish appropriate communication channels with outside parties such as financial analysts or even regulators. Open and frank two-way communications may alert the enterprise to potential communication problems or allow it to discuss and solve any problems in advance of adverse publicity.

Means and Methods of Communication. There is no one correct means of communicating internal control information within the enterprise. The modern enterprise can communicate its messages through many vehicles, including bulletin board announcements, procedure manuals, webcasts, videotaped presentation, or speeches by members of management. Often, however, the action taken by the communicator either before or after the message will give a stronger signal to the recipients of that communication. Both COSO frameworks summarize this internal control element as follows:

> An entity with a long and rich history of operating with integrity, and whose culture is well understood by people through the organization, will

likely find little difficulty in communicating its message. An entity without such a tradition will likely need to put more into the way the messages are communicated.

COSO Internal Control Elements: Monitoring. The capstone of the COSO internal control framework model is the monitoring component. While internal control systems will work effectively with proper support from management, control procedures, and both information and communication linkages, a process must be in place to monitor these activities. Monitoring activities have long been the role of financial managers and internal auditors, who perform reviews to assess compliance with established procedures.

The COSO internal control framework recognizes that control procedures and other systems change over time. What appeared to be effective when it was first installed may not be that effective in the future due to changing external conditions, new personnel, new systems and procedures, and other factors. A process should be in place to assess the effectiveness of established internal control components and to take corrective action when appropriate. An enterprise needs to establish a variety of monitoring activities to measure the effectiveness of its internal controls.

Monitoring can be accomplished through a series of separate evaluations as well as through ongoing activities. Both COSO internal controls and ERM contain some of the same general specific factors. These ongoing activities refer to processes that monitor performance and make corrective action when required.

Ongoing Monitor Activities

Many routine business functions can be characterized as monitoring activities. Although auditors and financial managers often do not always think of these in that sense, COSO internal controls gives the following examples of the ongoing monitoring component of internal control.

- *Operating management normal functions.* Normal management reviews over operations and financial reports constitute an important ongoing monitoring activity. However, special attention should be given to reported exceptions and potential internal control deviations. Internal control is enhanced if reports are reviewed on a regular basis and corrective action initiated for any reported exceptions.
- *Communications from external parties.* This element of monitoring is closely related to the component of communication from external

parties discussed earlier. External communication–measuring monitors, such as a customer complaint telephone number, are important; however, the enterprise needs to closely monitor these calls and then initiate corrective action when appropriate.

- *Enterprise structure and supervisory activities.* While more senior management should review summary reports and take corrective action, the first level of supervision and the related enterprise structure often plays an even more significant role in monitoring. Direct supervision of clerical activities, for example, should routinely review and correct lower-level errors and assure improved clerical employee performance. This review is also an area in which the importance of an adequate separation of duties is emphasized by COSO. Dividing duties among employees allows them to serve as a monitoring check on one another.
- *Physical inventories and asset reconciliation***.** Periodic physical inventories, whether of storeroom stocks or negotiable securities, are an important monitoring activity. An annual inventory in a retail store, for example, may indicate a significant merchandise loss. A possible reason for this loss could be theft, pointing to the need for better security controls.

These are examples from a longer list in the COSO internal control report. They illustrate procedures that are often in place in enterprises but are not thought of as ongoing monitoring activities. Any activity that reviews enterprise activities on a regular basis and then suggests potential corrective actions can be thought of as a monitoring activity. The COSO ERM framework lists very similar monitoring activities here.

Separate Internal Control Evaluation

While COSO internal controls points out the importance of ongoing monitoring activities to support the internal control framework, COSO also suggests that ''it may be useful to take a fresh look from time to time'' at the effectiveness of internal controls through separate evaluations. The frequency and nature of these separate special reviews will greatly depend on the nature of the enterprise and the significance of the risks it must control. While management may want to periodically initiate an evaluation of its entire internal control system, most reviews should be initiated to assess a specific area of control. These reviews may often be initiated when there has been an acquisition, a change in business strategy, or some other significant activity.

COSO internal controls also emphasizes that these evaluations can be performed by direct line management through self-assessment types of reviews. A function such as internal audit is not required to perform the review unless requested by senior management; the scheduling of these will be dependent on internal audit's risk assessment process and the resources available to schedule and perform reviews. Considerable time may pass before internal audit may have scheduled a normal review in a given area of operations. However, responsible management in that area should consider scheduling and performing its own self-assessments on a more regular basis. The internally generated self-assessment review can point out potential control problems and cause operating management to implement corrective action.

Internal Control Evaluation Process. COSO internal controls talk about the evaluation process for reviewing a system of internal controls. The controls self-assessor should first develop an understanding of the system design, identify its controls, test those controls, and then develop conclusions on the basis of the test results. This is really the internal audit process. COSO here also mentions another approach for evaluation called *benchmarking,* an approach that is occasionally performed by internal auditors and quality assurance professionals. Benchmarking is the process of comparing an enterprise's processes, control procedures, and other activities with those of peer enterprises. Comparisons may be made with specific similar enterprises or against published statistics from similar industry groups. This approach is convenient for some types of measures but filled with dangers for others. For example, it is fairly easy to benchmark the enterprise size, staffing levels, and average compensations of a sales function against comparable enterprises in the same general industry; however, the evaluator may encounter difficulties in trying to compare other factors due to the many small differences that make all enterprises unique.

Evaluation Action Plans. COSO internal controls discuss the importance of control documentation, particularly when statements about controls are made to outside parties. However, COSO recognizes that not all control procedures lend themselves to formal documentation. Many are informal and undocumented, although they may be regularly performed and highly effective. The COSO internal control framework makes the point that these undocumented controls should be tested and evaluated in the same manner as documented ones. While an appropriate level of documentation makes any evaluation of internal control more efficient and facilitates employees' understanding of how the process works, that documentation is not always essential.

Reporting Internal Control Deficiencies

Whether internal control deficiencies are identified through processes in the internal control system itself, through monitoring activities, or through other external events, these internal control deficiencies should be reported to appropriate levels of enterprise management. The key question for the control evaluator is to determine what should be reported given the large body of details that may be encountered, and to whom the reports should be directed. COSO internal controls state that "all internal control deficiencies that can affect the entity's attaining its objectives should be reported to those who can take necessary action." While this statement initially makes sense, the experienced professional, such as an internal auditor, will realize that this directive is difficult to implement. The modern enterprise, no matter how well organized, can be guilty of a variety of internal control errors or omissions. COSO suggests that all of these should be identified and reported, and that even the most minor of errors should be investigated to understand if they were caused by any overall control deficiencies. Both the COSO internal controls and ERM reports use the example of an employee taking a few dollars from the petty cash fund.

While the amount may not be significant, COSO urges that the matter be investigated rather than ignored, since "such apparent condoning personal use of the entity's money might send an unintended message to employees." Prior to SOx, external auditors regularly applied the concept of materiality when performing their reviews. That is, they often decided that some errors and irregularities are so small that they are not material to the overall conclusion that the external auditor will reach. While the operational efficiency of administrative control is of prime importance, materiality should also be considered when evaluating internal controls in general. SOx does not really discuss materiality issues, but it certainly will be a major factor in any enforcement actions. In the first years of SOx 404 reviews, many external auditors ignored materiality and raised issues on some really minor exceptions. After massive industry complaints, the SEC is changing their guidance to concentrate on more major, material internal controls issues and exceptions.

COSO internal controls conclude by discussing to whom to report internal control deficiencies in the enterprise. In one paragraph, COSO provides guidance that is useful for evaluations:

> Findings on internal control deficiencies usually should be reported not only to the individual responsible for the function or activity involved, who is in the position to take corrective action, but also to at least one level of management

above the directly responsible person. This process enables that individual to provide needed support or oversight for taking corrective action, and to communicate with others in the enterprise whose activities may be affected. Where findings cut across enterprise boundaries, the reporting should cross over as well and be directed to a sufficiently high level to ensure appropriate action.

SOx has tightened up this COSO internal control reporting guidance. Matters that appear to be of a material nature become an almost immediate CFO and audit committee reporting issue. The enterprise should also develop reporting procedures such that all internal financial control deficiencies, whether encountered through an SOx Section 404 review or through internal audit reviews of ongoing operations, are reported to appropriate levels of the enterprise. Management reporting and monitoring is a highly important aspect of internal control.

COSO INTERNAL CONTROLS AND COSO ERM COMPARED

Although the two frameworks are slightly different and the number of components are different, COSO Internal Controls and COSO ERM are very similar framework guides for achieving effective controls, whether within the enterprise or over a broader scope. With its guidance in areas such as risk responses and risk assessments, COSO ERM certainly takes a different and much broader scope. In many other areas, such as objective setting, the two frameworks are essentially identical. A major difference between the two frameworks is the second—top of the cube—dimension where COSO internal controls emphasizes the major components of internal control including operations, financial reporting, and compliance with laws and regulations. As discussed in Chapter 3, this dimension of COSO ERM also has a strategic component.

These two COSO frameworks are similar but have some different objectives and components. The guidance in each is important for today's enterprise. It may not be appropriate for an enterprise to try to build processes to comply with both frameworks, but the emphasis today should be more focused on ERM. This is particularly important to the previously discussed change in AICPA-sponsored auditing standards with their increased emphasis on risk.

NOTES

1. American Institute of Certified Public Accountants, *Statement on Auditing Standards No. 1*. New York: AICPA.

2. Kenneth A. Merchant, *Fraudulent and Questionable Financial Reporting: A Corporate Perspective.* Morristown, NJ: Financial Executives Research Foundation, 1980.
3. R. K. Mautz and J. Winjum, *Criteria for Management Control Systems.* Morristown, NJ: Financial Executives Research Foundation, 1981.
4. Report of the National Commission on Fraudulent Financial Reporting. National Commission on Fraudulent Financial Reporting, 1987.
5. Committee of Sponsoring Enterprises of the Treadway Committee, Jersey City, NJ: AICPA, 1992.
6. Robert Moeller, *Brink's Modern Internal Auditing,* 6th ed., John Wiley & Sons, 2005, p. 70.
7. American Institute of Certified Public Accountants, *Statement on Auditing Standards No. 107* ("Audit Risk and Materiality in Conducting an Audit"). New York: AICPA, 2006.

7

SARBANES-OXLEY AND COSO ERM

Since becoming a U.S. law in 2002, the Sarbanes-Oxley Act (SOx) has had a major impact on worldwide enterprises and particularly those with securities registered through the Securities and Exchange Commission (SEC). SOx has changed the public accounting regulatory landscape from one of self-regulation by external audit firms to quasi-governmental rules for public accounting firms. More important, SOx now requires business managers to take personal responsibility for the documentation, review, and testing of their enterprise's internal controls. Although the Act requires enterprises to follow Committee of Sponsoring Organizations (COSO) internal control rules, the COSO enterprise risk management (ERM) was released after SOx that is not specifically mentioned in the legislation.

Nevertheless, both SOx and COSO ERM have some important dependencies on one another, and today's enterprise manager must have a general understanding of both. This chapter provides a general background on SOx and describes some of its enterprise risk-related attributes.[1]

SARBANES-OXLEY BACKGROUND

The five or so years starting in the mid-1990s were an investment boom time for the United States and elsewhere. The Internet and networked information systems technology, although ubiquitous today, were just coming of age. Stock markets were booming worldwide, new technology start-up companies were being sprouted like so many seeds of grass, and some credible-sounding writers were even predicting that there would never be another recession[2] because of these new technology changes.

That bright future did not last forever, and the stock market boom of late 1990s—often called the dot-com bubble—soon collapsed. During this entire period, some corporations improperly tried to stretch accounting rules to keep their reported earnings high while others, it was later found, had been "cooking their books" all along. Perhaps what has been depicted as the most egregious of these was the Houston, Texas–based corporation, Enron. Starting as an oil and gas pipeline operator, Enron soon expanded into a wide range of operations including broadband telecommunications, video-on-demand Internet services, worldwide power plant construction, water purification, and much more. Enron quickly became a very large corporation and really got the attention of investors. Its business approach was aggressive but appeared to be profitable. Then, in late 2001, it was discovered that Enron was not telling investors the true story about its financial condition. It was found to be using off-balance-sheet accounting to hide some major debt balances. They had been transferring significant financial transactions to the books of unaffiliated partnership enterprises that did not have to be consolidated in Enron's financial statements. Even worse, these off-balance-sheet entities were paper-shuffling transactions orchestrated by Enron's chief financial officer (CFO) who made massive personal profits from these bogus transactions. Such personal transactions had been prohibited by Enron's code of conduct, but that same CFO requested the Enron board to formally exempt him from code violations. Blessed by their external auditors, the board had then approved these dicey off-balance-sheet transactions. Once publicly discovered, Enron was forced to roll these side transactions back into Enron's consolidated financial statements, making its numbers look very bad, and forcing a restatement of earnings. Certain key lines of credit and other banking transactions also were based on Enron's pledge to maintain certain financial health ratios. The restated earnings put Enron in violation of these agreements. What once had looked like a strong, healthy corporation was soon forced to declare bankruptcy.

Because Enron was a prominent company, there were many "How could this have happened?" questions raised in the press and by government authorities. Another major question was, "Where were the auditors?" Commentators felt that someone should have seen this catastrophe coming if they only had only looked harder. The press at the time was filled with articles about Enron's fraudulent accounting, the poor governance practices of Enron's board, and the failure of its auditors. The firm Arthur Andersen—once a very prominent public accounting firm—had served as Enron's external auditors and had also assumed their internal audit function through outsourcing. With a notice that the SEC would soon be on the way to investigate the evolving mess at Enron, Andersen directed its offices responsible for the Enron audit to "clean up" all records from that audit. The result was a massive paper-shredding exercise, giving the appearance of pure evidence destruction.

The federal government moved quickly to indict Andersen for obstruction of justice because of this document shredding, and in June 2002, Andersen was convicted of a felony by a Texas jury, fined $500,000, and sentenced to five years' probation. Although Andersen eventually won on appeal, that felony charge caused it to lose all public and professional trust, and it soon ceased to exist.

Enron was not alone. At about that same time, the telecommunications firm WorldCom disclosed that it had inflated its reported profits by at least $9 billion during the previous three years, forcing WorldCom to declare bankruptcy. Another telecommunications company, Global Crossing, also failed during that same time period when its shaky accounting became public. Then, the cable television company, Adelphia, failed when it was revealed that its top management, the founding family, was using company funds as sort of a personal piggy bank, and soon thereafter the CEO of the major conglomerate Tyco was indicted, fired, and subsequently went to prison because of major questionable financial transactions. Only a few examples from 2001 are mentioned here; and through the following year 2002, many other large corporations were accused of fraud, poor corporate governance policies, or sloppy accounting procedures. The press, the SEC, and members of the U.S. Congress all declared that auditing and corporate governance practices needed to be fixed.

The major outcome here was the passage of SOx in 2002. Although there are many other provisions, SOx established major new regulatory rules for public accounting firms, financial auditing standards, and corporate governance. Through SOx, the public accounting profession was transformed, the American Institute of Certified Public Accountants' (AICPA's)

Auditing Standards Board lost its responsibility for setting public corporation auditing standards, and the rules soon changed for corporate senior executives, boards of directors, and their audit committees. A new entity, the Public Company Accounting Oversight Board (PCAOB), was established under the SEC to set financial reporting and auditing standards as well as to oversee individual public accounting firms. Although not directly covered in that legislation, SOx also has very much impacted enterprise risk management as well.

Political and economic events often drive legislation, and those laws and rules often stay with us for a long time after the underlying problems have been corrected. The great depression in the United States in the early 1930s, for example, caused the United States to enact some very strict regulations covering banks. Although financial institutions have changed considerably and many older problems are no longer concerns, much of this 1930s legislation stayed "on the books" until only very recently. With that thinking, SOx will be with all business professionals for a long time into the future.

SOX LEGISLATION OVERVIEW

This section discusses this very significant public accounting standards-setting and corporate governance legislation, SOx, with an emphasis on its aspects that are most important for enterprise risk management. SOx and the PCAOB represent the major changes to public accounting, financial reporting, and corporate governance rules since the SEC was launched in the 1930s. Just for the record, the official name for this August 2002 U.S. federal legislative act to regulate the accounting and auditing practices of publicly traded companies is the "Public Accounting Reform and Investor Protection Act." The law's title being a bit long, business professionals generally refer to it as the Sarbanes-Oxley Act, using the names of its congressional principal sponsors; some call it SOX, SOA, others use SarBox, and we refer to it as SOx throughout this book.

U.S. federal laws are organized and issued as separate sections of legislation called "titles", with numbered sections and subsections under each. Much of the actual SOx text only mandates rules to be issued by the responsible agency, the SEC. That is, SOx states that a rule should be established, and the SEC sets the rules later. These upcoming specific SOx rules to be developed by the SEC may or may not be significant to most. Exhibit 7.1 summarizes the major titles of SOx and those that appear to be

Section	Subject	Rule or Requirement
101	Establishment of PCAOB	Overall rule for the establishment of PCAOB, including membership requirements.
104	Accounting Firm Inspections	Schedule for registered firm inspections.
108	Auditing Standards	The PCAOB will accept current ASB standards but will issue new standards.
201	Out-of-Scope Practices	Outlines prohibited practices such as internal audit outsourcing, bookkeeping, and financial systems design.
203	Audit Partner Rotations	The audit partner and the reviewing partner must rotate off an assignment every five years.
301	Audit Committee Independence	All audit committee members must be independent directors.
302	Corporate Responsibility for Financial Reports	The CEO and CFO must certify the periodic financial reports.
305	Officer and Director Bars	If received as part of fraudulent/illegal accounting the officers or director is required to personally reimburse funds received.
404	Internal Control Reports	Management is responsible for an annual assessment of internal controls.
407	Financial Expert	One audit committee director must be a designated financial expert.
409	Real-Time Disclosure	Financial reports must be distributed in a rapid and current manner.
1105	Officer or Director Prohibitions	The SEC may prohibit an officer or director from serving in another public company if guilty of a violation.

EXHIBIT 7.1 SARBANES-OXLEY ACT KEY PROVISIONS SUMMARY

more significant to risk managers and internal auditors. The following sections provide descriptions of key portions of SOx important to enterprise risk management. SOx is the most important financial legislation passed in the United States since the early 1930s, and it has caused changes for financial managers, internal auditors, external auditors, and corporate governance administrators in all corporations. While SOx is directed at corporations with SEC registered securities, its concepts, if not actual rules

and processes, encompass a wider swath of worldwide enterprises. In addition, while SOx is directed at financial reporting practices and both the management and external auditors responsible for those audited financial reports, the overall SOx rules are very important to all parties involved with implementing and effective ERM program in their enterprise.

Setting the Rules: The Public Company Accounting Oversight Board

As discussed, much of SOx concerns a public corporation's financial reporting. While management, board members, internal auditors, and others are, or should be, very aware of this overall process, some of these rules and concerns may appear to be in "another world" to some readers involved in formal risk management or many areas of information technology (IT) today. However, all concerned should have a general understanding of this process—what it was and how SOx has changed some of the rules. These include both the SEC-mandated annual and quarterly financial reports (called 10Q and 10K) and activities of the external auditors who reviewed and certified those reported results.

For many years, the AICPA had review responsibility for public accounting firms through their administration of the certified public accountant (CPA) test and the restriction of AICPA membership then only to CPAs. State boards of accountancy actually licensed CPAs, but the AICPA had overall responsibility for the profession. Auditing standards for new issues or concerns were set by the AICPA's Auditing Standards Board (ASB) through a process that involved member task forces to develop the proposed standards or changes, extensive individual member and firm reviews of those new draft standards, and the eventual issuance of the new or revised financial audit standards. Auditing standards were based on what was called generally accepted auditing standards (GAAS) along with a series of specific numbered auditing standards called Statements of Auditing Standards (SAS). GAAS rules govern auditing, while generally accepted accounting principles (GAAP) define the accounting rules. Much of GAAS was just good financial auditing practices, such as the understanding that certain transactions must be backed by appropriate documentation. The SASs covered more specific areas requiring better definition. SAS No. 79, for example, defined internal control standards, or SAS No. 99, *Consideration of Fraud in a Financial Statement Audit,* outlines the review standards that external auditors should follow when reviewing for the possibility of fraud.

The post-Enron-era financial failures introduced some major changes to what had been well-established financial auditing standards and practices. Government regulators as well as the investment community began to question and then reform the financial auditing standards-setting process and a wide range of public accounting firm practices. Many enterprise CEOs and CFOs were characterized by the press and others as being more interested in personal gain rather than serving their shareholders. Audit committees were often characterized as not being sufficiently involved in enterprise transactions, and external auditors and the AICPA received major levels of criticism. Outsourced internal auditors caught much criticism as well; they were viewed as being tied too closely to their external audit firm owners. Many other previously accepted practices, such as the self-regulation of public accounting firms, were seriously questioned. By self-regulation, we refer to the AICPA's peer review process where public accounting firm A would be given the responsibility to review the standards and practices in place at firm B. Knowing that firm B might be assigned to come back and review A a few years into the future, no firm ever had many critical things to say about its peers.

SOx has brought many changes to the auditing standards-setting process. The AICPA's Auditing Standards Board has lost its responsibility for setting auditing standards, and the rules have changed for corporate senior executives, boards of directors, and their audit committees. A new entity, the Public Company Accounting Oversight Board (PCAOB but sometimes call "Peek-a-Boo") has been established, as part of SOx and under the SEC to set public accounting auditing standards and to oversee individual public accounting firms. SOx and the PCAOB represent the most major changes to public accounting, financial reporting, and corporate governance rules since the SEC was launched in the 1930s. SOx represents the most important set of new rules for auditing and internal auditing today. The effective internal auditor and risk manager should have a good understanding of these new rules and how they apply to today's practice of auditing and financial reporting.

The PCAOB is now the independent entity that governs and regulates the public accounting industry and establishes financial auditing standards. While they have released a general auditing standard on internal control, called Auditing Standard No. 2 (AS/2), many other auditing standards will almost certainly be forthcoming in the future.[3] While the pre-2002 auditing standards are generally still in place, the PCAOB is in the process of releasing its own auditing standards over time. SOx has totally changed the rules for financial auditing, corporate governance, and the role of external audit firms, among

other matters. SOx also has had a major impact on all internal auditors, whether working in the United States or elsewhere for essentially any form of enterprise. The following sections discuss the major sections of SOx that have the greatest impact on ERM. They have not been listed in numerical order, and we have summarized the areas that are most important to the ERM process.

Section 404: Management's Assessment of Internal Controls

As mentioned previously, many aspects of the SOx rules cover the preparation of annual 10K reports that all enterprises with SEC-registered securities must prepare. This covers virtually all U.S. public corporations as well as many non-U.S. enterprises with securities traded on U.S. exchanges. There is a variety of exceptions and waivers here, but virtually all U.S. public corporations, at least, are required to comply. SOx Section 404 requires that each SEC annual report filing must contain an internal control report that states management's responsibility for establishing and maintaining an adequate system of internal controls as well as management's assessment, as of that fiscal year ending date, of the effectiveness of those installed internal control procedures. The external auditors are to attest to and report on the internal control assessments made by management. This is a major step in corporate governance that should be of particular interest to internal auditors with their ongoing internal control–related review work.

With SOx taking effect for many in 2004, the first effective year was difficult for many enterprises! SOx Section 404 requires that all impacted enterprises must document and describe their key internal controls and then must test those controls to determine if they are operating effectively as defined and also must identify any material weaknesses in those internal controls. Enterprise management then provides this formal assessment of internal controls to their external auditors who review the work, perform additional tests themselves as they may feel necessary, and use this overall assessment of internal controls to provide their audited opinion on the fairness of the published financial statements. This is a major element of SOx, and management also is required to formally assert that their internal controls are adequate. Provisions of SOx even include personal criminal penalties for fraudulent misstatements. Once an enterprise has gotten itself through its first Section 404 review, it is required to establish processes for a continuous monitoring, evaluation, and controls improvement. Going forward, the enterprise needs to monitor its key systems, determine if there were any changes in subsequent periods, and design

internal control procedures to correct any control weaknesses or otherwise fill control gaps. After that first year, an enterprise's Section 404 documentation standards and materials need to be reviewed and updated on a regular basis. Systems and processes change and acquisitions or enterprises may modify various aspects of their operating environment.

Simply put, management is now required to report on the quality of *their* internal controls, and the public accounting firm responsible for the financial statement audit must attest to the adequacy and accuracy of that management-prepared internal accounting controls report. Management has always been responsible for preparing their periodic financial reports, and their external auditors previously only reviewed those financial numbers and certified that they were fairly stated as part of their audit. Now with SOx Section 404, management is responsible for documenting and testing their internal financial controls in order to prepare a report on their effectiveness. The external auditors now review the supporting materials leading up to that internal financial controls report to assert that the report is an accurate description of that internal control environment.

To the nonauditor, this might appear to be an obscure or almost trivial requirement. Even some internal auditors that primarily specialize in operational audit reviews may wonder about the nuances in this process. However, audit reports on the status of internal controls have been an ongoing and simmering issue among the public accounting community, the SEC, and other interested parties going back to 1974. As discussed in Chapter 6 on integrating COSO with ERM internal controls, much of the debate, going through the 1980s, was that there was no recognized definition for what is meant by internal controls. The release of the COSO internal control framework in 1992 established a common definition or understanding for internal controls that has become today's accepted standard. Under SOx, management is now required to report on their internal controls, with the public accounting firm attesting to those internal control reports.

In the following section, we will discuss the process of launching a Section 404 review of key applications. There are many similarities between a SOx 404 review and understanding process risks as part of COSO ERM, and we will attempt to describe these as well.

Launching the Section 404 Compliance Review: Identifying Key Processes. Whether they are financial, operational, or IT related, every enterprise uses multiple processes to conduct its normal business activities. Some of these may be automated systems, others are primarily manual procedures that are performed on a regular basis, while still others are a

combination of automated and manual. The monthly financial accounting close is an example of the latter. Automated accounting systems, including an enterprise's general ledger system, support a large portion of this financial close process. For most enterprises, there is a major manual component here as well, and they should be thought of as the process of the monthly financial reporting close.

Whether understanding internal controls or significant risks, a very early step is for an enterprise to define and describe their major processes, including making certain all parties have a clear understanding of what is meant by this closing process. This concept can cause confusion to some when a Web search for "process definition" will yield a long list of sites from software firms and others who each have a different interpretation of what is meant by a process. We would define a process as a particular course of action intended to achieve a result, such as the procedure of obtaining a driver's license. A process is a series of actions that have clearly defined starting points, consistent operational steps, and defined output points. The process results in a usable set of defined steps to be followed, along with supporting documentation that can be followed consistently throughout the enterprise.

Internal audit or the risk management function can be a major help here in assisting an enterprise in defining its key processes. For many enterprises, internal audit has already defined their key processes through their annual internal audit planning process, as discussed in Chapter 9. A process is much more than just one automated application and includes all of the beginning and ending steps to allow an enterprise to form some business function. For a payroll application, for example, this process would include all aspects of the systems and procedures necessary to compensate employees, ranging from the preparation of timesheets to the automated payroll calculation system to the steps necessary to distribute compensation remittance notices and pay taxes, benefits, and much more. It will also include the numerous clerical and administrative steps that are necessary. The concept here is to think about processes in a big-picture sense, covering all basic business activities in an enterprise. Such a process view or understanding will form a basis or starting point for future internal control reviews. Enterprise processes should be summarized in a comprehensive enterprise process list that will become a basis for understanding basic accounting flows and for launching a stream of internal control and risk assessment reviews for the enterprise.

Launching the Section 404 Review: Organizing the Internal Control Review. Compliance with SOx Section 404 places a major challenge on SEC-registered enterprises. While some enterprise managers had previously taken a hard look at their COSO internal control framework, described in Chapter 6, and evaluated their internal controls using that framework prior to SOx requirements, many others may not have gone through this exercise. The enterprises staff that has evaluated their own internal controls in a COSO context will almost certainly have some work ahead, but at least should have gained an understanding of their internal control environment. A second pre-SOx group may have relied on their pre-SOx external auditors, who issued favorable financial reports with only limited internal control work. They may also have relied on their internal auditors, who had been reviewing internal controls in various selected areas but never in any consistency or totality. This second group faces a potentially major challenge in completing their assessment of internal controls under SOx Section 404 requirements. A third group often are smaller enterprises, that have given little attention to documenting their internal controls in the past and often have a small, understaffed internal audit functions as well and no risk management function. The latter have faced major challenges in establishing Section 404 compliance, and the SEC has given them a series of time extensions to complete this work.

An effective internal audit function can play a very major role in helping an enterprise get ready for SOx Section 404 compliance. The external auditors that once did some internal financial control assessment work as part of their annual audits are no longer directly responsible for these reviews. As discussed, those external auditors will review and attest to management's internal financial control assessment report but cannot do the work themselves. An internal audit function, another management team, or outside consultants should begin their Section 404 compliance review process by launching a formal, special project along the lines of project management processes discussed in Chapter 10. While details may vary, the project could be launched following these steps:

1. *Organize the Section 404 compliance project approach.* Assign a project team to lead the effort. A senior executive such as the CFO should act as the project sponsor with a team of both internal and external (but not external audit!) resources to participate in the effort. Roles, responsibilities, and resource requirements should be estimated as well. Internal audit will often assume major responsibilities here.

2. *Develop a project plan.* The internal financial control compliance project should be well planned and in process prior to the enterprise's financial year end. While the existing plan can be updated in subsequent years, there will be a major challenge and "time crunch" for earlier years. The plan should focus on significant areas of enterprise operations with coverage over all significant business units. Although there can be many variations here for developing such a plan, Exhibit 7.2 shows some of the major work steps—a work breakdown structure—that must be considered when planning a Section 404 compliance review project. Although the work steps described here are at a fairly high level, these steps can be used to develop a more detailed plan document to begin the internal financial controls review.
3. *Select key processes for review.* Every enterprise uses or depends on a wide range of financial and operational processes. We have used the term *process* here as opposed to *system* because the latter is often used only to refer to some automated processes. For most enterprises, the payroll system, for example, is a set of automated routines that take time and attendance data and produce payroll checks or transfers in employee checking accounts. The payroll process is much larger, including the steps necessary to add a new employee, to process a pay increase, and to communicate with accounting and benefit systems. There can be numerous transaction flows in this overall process.

   The Section 404 compliance team needs to review all enterprise processes and select the ones that are financially significant. This key process selection should focus on processes in which the risk of failure could cause a major loss or expense to the enterprise, and consideration should be given to processes in all enterprise entities, not just headquarter systems. The processes should then be ranked by the size of assets controlled, their materiality in terms of the overall financial resources of the enterprise, or other measures. Rather than just considering the size of assets managed, Exhibit 7.3 contains some process review selection guidelines. The focus on these guidelines is more on information systems–related considerations, but they exhibit some of the factors to consider. For example, in raising the question of whether the application software was purchased or built in-house, the enterprise might—and probably should—decide that purchased software often has a lower risk. Internal audit or risk

1. Assemble a review team. This may be led by internal audit, risk management, or other internal or external consultants. (*Note*: This assumes internal audit will not be supporting their external auditors for these reviews.)
2. Agree on a consistent terminology for the review, including an understanding of financial assertions and risks.
3. Define project objectives:
   - Determine if review will cover just financial controls or efficiency and effectiveness areas as well.
   - Determine organizational units to be covered in review.
   - Review results from any previous Section 404, internal audit, or risk management reviews requiring follow-up.
   - Establish a project timeline that allows time for external audit review.
   - Review planned objectives with the CFO and audit committee.
4. Develop a detailed project plan covering processes to be reviewed.
5. Establish review approach for each process/system included in the review:
   - Identify the types and nature of key process controls and the risks associated with failure of those controls.
   - Define nature and types of possible errors and omissions.
   - Define nature, size, and composition of transactions to be reviewed.
   - Determine volume, size, complexity, and homogeneity of individual transactions processed.
   - Establish guidelines for materiality and error significance.
   - Understand process transaction susceptibility to error or omissions.
6. Review approach and timing with external auditors.
7. Establish standards for review documentation and project progress reporting.
8. Complete preliminary reviews for each identified process or system including new or updated supporting documentation.
9. Follow up and resolve any items requiring investigation.
10. Consolidate review work and prepare a preliminary section 404 report.
11. Review 404 report results with CFO and release report.

EXHIBIT 7.2 SECTION 404 COMPLIANCE REVIEW WORK BREAKDOWN STRUCTURE

management can assist in developing a documented procedure to justify why one process was more worthy or significant for detailed review than another. The professional reviewing selection criteria may ask for such justifications and may add their own insights into the processes they feel should be viewed as review candidates.

4. *Document selected process transaction flows.* The next step, and an important one, is to prepare transaction flow documentation for the key processes selected. This can be an easy step for some enterprises where

The following questions can serve as a guide for selecting key processes to review as part of an SOx Section 404 review exercise. While there is not a right or wrong answer to any, these should help a team selecting key processes to consider key factors.

I. Process or IT System Status

A. Nature of the process or system to be reviewed:

— Is this a new system or process developed in-house?
— Is it a newly purchased application package?
— Have there been major changes over the past period affecting functionality?
— Does the process use newer technologies?
— Have past changes been described as only minor changes?
— Is there adequate current documentation supporting the process?

B. Past history of process or system changes:

— Have there been significant changes over the past two years?
— Have any past changes caused problems requiring corrective actions?
— Has it been two years or more since the last change?
— Is this a new process or one with no recent changes?
— Is there an adequate document change control process in place?

C. Process or system development team:

— Is the process managed by an outside contractor for its development or management?
— Is an in-house group responsible for process development and management?
— Is the process a purchased packaged solution with only minor local changes?

D. Senior management interest in process or project:

— Is this an enterprise-level process mandated by senior management?
— Does system or process responsibility reside at an operating-unit level?
— Is this a process initiated by middle management?
— Individual user or department responsibility?

II. Audit and Control Significance

A. Type of system or process:

— Does the process support financial statement balances?
— Support major organizational operations?
— Primarily for logistical or administrative support?
— Is this a less critical statistical or research application?

B. Past internal audit or SOx review involvement:

— Has there been a prior SOx review including control improvement recommendations?
— Have prior reviews concluded with only limited recommendations?
— Have prior Section 404 test results found no significant internal control problems?
— If control improvement recommendations have been made in prior reviews, do these matters appear to have been corrected?
— Is this a process that was never formally reviewed?

EXHIBIT 7.3 PROCESS REVIEW SELECTION GUIDELINES

C. System or process control procedures:
- — Are there process-generated internal controls?
- — Are there run-to-run controls with other systems or processes?
- — Is the process primarily operating in a batch mode or with manual controls?

III. Enterprise Risk Concerns

A. Have process risks been evaluated?

B. Does the process represent an area with significant failure probability?

C. Is there a high likelihood that identified risks could occur?

IV. Impact of Process Failure

A. Impact of incorrect reported results. Would a process failure result in:
- — Potential legal liability?
- — Financial statement impact?
- — Potential for incorrect management decisions?
- — Limited decision support risks?

B. Impact of application failure on personnel. Would a process failure result in:
- — Need for extra management analysis time?
- — Need for extra user clerical time?
- — Need for a wide range of specialized resources?

EXHIBIT 7.3 PROCESS REVIEW SELECTION GUIDELINES

there has been a COSO internal control review with key documentation prepared previously. Then, the existing documentation should be reviewed to determine that it is still accurate and updated as required. Process documentation is much more of a challenge if the enterprise has never previously documented its processes or if the documentation it has just represents old automated system transaction flows.

There is a variety of accepted documentation protocols supported by various automated tools. Exhibit 7.4 is an example of a simple flowchart describing a payroll timecard process for a smaller enterprise. The goal for these types of flowcharts is to describe key processes at a very high level. These include the steps to initiate a process, actions such as recording a transaction at a very high level, and key decision points. The documentation should show key transaction flows and control points. The space below the chart would contain a detailed process description. Although a variety of flowchart styles can be used, this example chart has notations where transactions are initiated, the data is recorded, and the transaction is authorized, as well as where processing takes place. The number references here refer to process flowchart procedural steps.

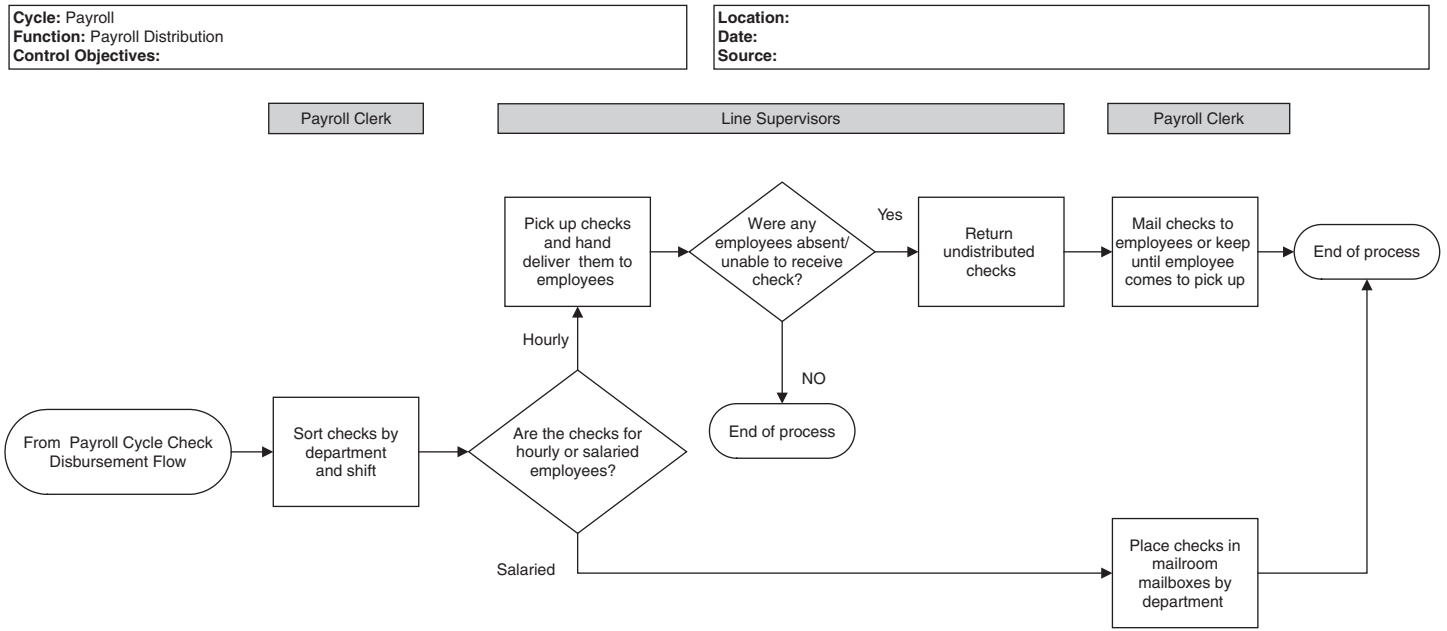

EXHIBIT 7.4 PAYROLL TIMECARD PROCESS

Source: Robert Moeller, *Brink's Modern Internal Auditing,* 6th ed. copyright © 2004, John Wiley & Sons. Reprinted with permission of John Wiley & Sons, Inc.

A key need for any documentation is its own supporting process to keep it updated. The traditional three-ring notebooks full of process documentation are of little value because they are almost never updated. Enterprises should establish procedures to ensure that all changes to previously documented systems are updated when required. Consideration should be given to installing one of the many automated documentation tools available today. The team that led the project to document SOx processes should be given the responsibility to maintain this documentation.

5. ***Identify, document, and test key internal controls***. This can be a major effort! Using some form of criticality analysis, key enterprise internal financial control processes should be identified and compliance tested, and the results documented. Documentation is very important here, because when the external auditors review these processes, they will need to examine this documentation in order to attest that controls are in place and operating. This is an area where internal audit can often play a key role in advising the internal financial controls project team. These steps will be discussed in greater detail in the paragraphs following.
6. *Assess selected process risks.* Once an enterprise has defined and documented its key processes, the next step is to assess risks to determine the significance and likelihood of those risks. Here, the team that first identified key-process areas and then documented them should go through a detailed "What could go wrong?" type of analysis following the risk management fundamentals discussed in Chapter 2. For example, in an accounts payable process, what is the likelihood that someone could gain access to the system and then arrange to cut themselves an unauthorized check? Are system controls sufficiently weak that multiple payments might be generated to the same authorized vendor? There could be numerous risks of this sort. A management team should go through each of the selected processes and highlight potential risks in such an open-ended set of questions and then focus on the expected supporting controls. Based on background, this is very much the type of analysis where internal audit can play a valuable role. Exhibit 7.5 is an example of this type of review for an accounts payable process and points to a review approach that should be developed for any key process. We have selected accounts payable (AP) as an example process, as it is fairly easy to understand in most circumstances. In many cases, existing

1	Are accounts payable staff independent from purchasing and receiving functions?
2	Are debit memos, adjustments, and other noncash debits to accounts payable approved and regularly reviewed by supervisory personnel?
3	Are there defined cutoff procedures at month end that are continually monitored by appropriate managers?
4	Are month-end accruals and other credit accounts payable estimates and adjustments reviewed and approved by appropriate managers?
5	Are all accounts payable vouchers and debit memos prenumbered through either manual or automated procedures?
6	Are all vendor invoices date and time stamped in sequential order, with the sequence periodically reviewed for missing/duplicate items?
7	Are all unused forms and related documents controlled?
8	Are records maintained for all voided forms?
9	Is the accounts payable subledger maintenance separate from general ledger maintenance?
10	Are accounts payable trial balances and general ledger control accounts periodically reconciled and reviewed by appropriate managers?
11	Are approved reconciliations of monthly vendor account statements made against unmatched open purchase orders and receiving reports?
12	Is a receipt of vendor account statements performed by someone other than accounts payable accounting staff?
13	Are accounts payable risks reviewed regularly, with corrective actions taken to limit those risks?
14	Have all control gaps from recent Section 404 reviews and internal audits been corrected?

EXHIBIT 7.5 ACCOUNTS PAYABLE PROCESS REVIEW PROCEDURES

internal audit programs or prior risk management analysis work can solve this need.

7. *Assess control effectiveness through appropriate test procedures.* System controls are of little value if they are not working effectively. We can sometimes determine that appropriate controls do not appear to be in place or are ineffective. In that case, the conclusions from the assessment should be documented, discussed with the process owners, and an action plan developed to take corrective actions to improve the controls. If the reviewer asks about the approval process necessary to generate an AP check and is effectively told there is no process beyond initial approval of the invoice, the reviewer may

determine that this an obvious internal control weakness that should be documented and discussed for planned corrective action.

In most instances, the reviewer's initial assessment of controls will require testing. Even well before SOx, audit testing has been a common process for both internal and external auditors in their reviews of controls. For financial audits, these audit tests were once extremely extensive, with large attribute and variable sample transactions taken and sample results evaluated. Attribute sampling is used for evaluating internal controls and variables sampling is used for estimating financial balances. Evaluation of the results of these samples allowed an internal or external auditor to draw conclusions regarding whether financial results were fairly stated or internal controls appeared to be working. A powerful tool, statistically based audit sampling is less common today based on difficulties with the computational process for many and pressures for audit efficiencies. Attribute sampling also can be a powerful tool to assess internal controls and to state with some measure of statistical confidence whether the internal control tested is working.[4]

Whether a statistical-based sample or not, the SOx process reviewer should virtually always use one or more sample transactions to test a process. If a complex but largely paper-based process with many people-based approval steps, the SOx reviewer might borrow from another classic internal audit technique and try a "walk-through" type of test. The idea here is to take a single transaction—such as a vendor invoice requiring approval before the AP check is generated—and individually "walk" that transaction through each of the processing steps prior to cutting that check. Again, this is a test to assess the internal controls over a process. If the results of the test are positive, the reviewer could determine if the process appears to be working correctly and with adequate internal controls. This is an exercise familiar to all internal auditors but is less common for risk managers.

8. *Identify any control gaps.* The review and documentation of enterprise processes as well as the subsequent testing of those processes may identify areas where one or another internal control is not working as described or has just been installed poorly. These items are often called "control gaps," areas where corrective actions are needed to improve or build internal controls. They should be documented and added to a list of future planned corrective actions.

9. *Review compliance results with key stakeholders.* Senior financial and executive management will ultimately be responsible for their final Section 404 report. The project team should review their progress with senior management on a periodic basis, highlighting their review approaches, any control gaps identified, and short-term corrective actions initiated. Similarly, since they must formally attest to the results of this internal financial control review, the external auditors should be kept informed of progress and any outstanding issues in process of resolution. Although often not part of the process prior to COSO ERM, the risk management function and the chief risk officer (CRO), should be included here.
10. *Complete report on the effectiveness of the internal control structure.* This is the final step to Section 404 compliance. Since this is not a one-time exercise, all work should be documented for follow-up reviews. The documentation process here is similar to a financial audit process where results are documented in audit work papers for ongoing periods. This is the report, along with the external auditor's attest work, that will be filed with the SEC as part of the enterprise's 10K annual report. Not a detailed report, there should be summary statements that internal controls have either been found and tested to be adequate or that control weaknesses—some potentially material—exist within the enterprise's internal control structure.

When the rules for Section 404 reviews were released as part of the SOx legislation in 2003, they were viewed as a major undertaking and certainly continue to require considerably more time and effort than is expressed in the limited number of work steps described above. Today, all larger SEC-registered U.S. public corporations have gone through the initial years of this documentation process and are now in the ongoing maintenance mode. However, as of this publication date, there are still many smaller or non-U.S., foreign enterprises that will still need to achieve Section 404 compliance. The SEC and the PCAOB have relaxed some rules, however, to make them a little less strenuous to smaller or foreign corporations.

In their first year and with ongoing maintenance, Section 404 internal control compliance reviews were major projects for many enterprises, although the level of work required depended on the amount of internal control work that has previously been performed in the enterprise. Many, if not most, larger major corporations in the United States have embraced the COSO or Control Objectives for Information Technology (CobiT)[5] internal control frameworks and have many strong internal audit functions in place

as well as audit reviews of those installed internal controls. Often through the leadership of internal audit, these enterprises have reviewed, tested, and documented their internal controls following the COSO framework standard. Such enterprises have had an easier task in achieving Section 404 compliance on a continuing basis.

At the present time in these still early years of SOx, there are still smaller, private, or non-U.S. enterprises that have not fully adopted the COSO internal control framework, as discussed in Chapter 6. There are many SEC-registered corporations today whose internal audit functions have performed some internal control reviews but have not otherwise embraced a COSO-like internal control framework throughout the enterprise. These are often enterprises wherein the internal audit and the ERM functions are relatively small, with activities focused on operational efficiency–related reviews or financial internal audit work in support of their external auditors. There are still many enterprises with no formal or even informal risk management processes in place. The SEC has frequently extended compliance deadlines for smaller U.S. companies and for foreign registrants and, in addition, has announced that some of these rules will be simplified and made less onerous. As we move to future years, SOx Section 404 rules will be changing.

Enterprise Risk Management and SOx Section 404 Reviews. Properly executed, Section 404 reviews and many elements of COSO ERM have some very common objectives. The SOx 404 review of key processes and their internal controls will have identified, documented, and confirmed through testing any control weaknesses in place—what are often called *control gaps.* Plans for corrective action should be constructed for these gaps and they should be split between what external auditors call "material" or "nonmaterial." control weaknesses. Material weaknesses, in particular, can have significant financial impacts on an enterprise. This concept of what is meant by the term *material* is discussed in the following paragraphs. At the extreme, external auditors may determine that, for a given entity, there may be so many control weaknesses in place that they cannot rely on the accuracy of the enterprise's published financial reports. Rather than an audited financial report, external auditors then will defer their opinion on the accuracy and fairness of the enterprise's financial statements due to these significant material weaknesses. This is a "kiss of death" that can have severe consequences on an enterprise.

COSO ERM often follows the same internal control assessment paths and has some similar implications. As discussed in Chapter 5, the ERM

function in an enterprise has a responsibility to review risks at all levels and to communicate those risks to the appropriate parties. The internal control gaps identified in a Section 404 review may represent those types of risks. For example, the Section 404 review may determine that a unit of the enterprise does not have an effective IT disaster recovery/business continuity plan in place for some or even all of its areas of operations. However, PCAOB rules do not require that the status of disaster recovery plans should be part of an enterprise's Section 404 review. With guidance that is surprising and contrary to the thinking of many internal auditors and risk managers, PCAOB Audit Standards[6] state:

> Management's plans that could potentially affect financial reporting in future periods are not controls. For example, a company's business continuity planning has no effect on the company's current abilities to initiate, authorize, record, process or report financial data. Therefore, a company's business continuity planning is not part of internal control over financial reporting.

While many in enterprise management will question why the lack of an effective continuity or disaster recovery plan is not a material weakness, the PCAOB today sets the rule for external auditors.

While there can be many other issues as well, this IT business continuity/disaster recovery example is a good illustration of an area where ERM and the SOx Section 404 reviewers often have very different perspectives and must coordinate their efforts and concerns. The lack of an effective plan to restore IT systems back in operation after some unexpected event would represent a major risk to almost any enterprise. The ERM team should coordinate with the Section 404 review effort to ensure that there is some coordination between SOx-identified gaps and ERM significant risks. Some Section 404 identified gaps may also not translate to ERM concerns. The Section 404 process is often more involved with accounting-related internal control issues and not with some of the operational or IT enterprise risks described in other Chapter 11. For example, the Section 404 review team may identify the lack of some timely account reconciliation as a significant control gap while ERM may not see that great a risk. An ERM team needs to understand the risk-related implications of that failure to reconcile accounts on a timely basis.

SOx Section 404 reviews require that management review and test its significant internal financial controls and then identify and report on any significant weaknesses. These internal control gaps should be listed on some form of "to-do" list for subsequent corrective actions. The ERM team will have similar responsibilities to identify significant risks over the enterprise and to

take corrective actions where necessary. There are many similarities between these two activities, and a level of ongoing dialogue is needed.

Section 302: Corporate Responsibility for Financial Reports

Prior to SOx, enterprises filed their annual 10K and quarterly 10Q financial statements with the SEC and published the results for investors, but the responsible corporate officers authorizing those reports were not personally responsible. If an enterprise was subsequently caught filing financial reports with fraudulent numbers, the CEO might say, "Its not my fault, my CFO gave me those numbers," and the CFO could say he only relied on the numbers supplied by his accounting staff and was not responsible either. Effectively, "no one" was responsible as matters were pushed down the ladder. The bar has now been raised, and the CEO, CFO, or other senior enterprise officers performing similar functions must certify for each annual and quarterly report filed that:

- The signing officer has reviewed the report.
- Based on that signing officer's knowledge, the financial statements do not contain any materially untrue or misleading information.
- Again based on the signing officer's knowledge, the financial statements fairly represent the financial conditions and results of operations of the enterprise.
- The signing officers are responsible for:
  - Establishing and maintaining internal controls.
  - Designing these internal controls to ensure that material information about the enterprise and its subsidiaries is made known to the signing officers during the period when the reports are prepared.
  - Evaluating the enterprise's internal controls within 90 days prior to the release of the report.
  - Presenting in these financial reports the signing officer's evaluation of the effectiveness of these internal controls as of that report date.
- Signing officers have disclosed to the external auditors, audit committee, and other directors:
  - All significant deficiencies in the design and operation of internal controls that could affect the reliability of the reported financial data and, further, have disclosed these material control weaknesses to the enterprise's auditors.

  - Any fraud, whether or not material, that involves management or other employees who have a significant role in the enterprise's internal controls.
- The signing officers have indicated in the report whether there were internal controls or other changes that could significantly impact those controls, including corrective actions, subsequent to the date of the internal control evaluation.

Given that SOx imposes criminal penalties of fines or jail time on individual violators, these signer requirements place a heavy burden on responsible corporate officers, who must take all reasonable steps to make certain that they are in compliance.

This personal sign-off requirement has raised major concerns for CEOs and CFOs and causes a significant amount of additional work for the accounting and finance staffs preparing these financial reports. This is very much a risk monitoring and reporting process! An enterprise needs to set up a detailed stream of paper-trail procedures such that the signing officers are comfortable that effective processes have been used and the calculations to build the report numbers are all well documented. The enterprise may want to consider using an extended sign-off process where staff members submitting the financial reports sign off on what they are submitting to the next level up the chain of authority. The ERM function can often act as an internal consultant and help senior officers establish effective processes here. Exhibit 7.6 provides an example of a Section 302 officer disclosure signoff statement that officers would be requested to sign. This is not an official PCAOB form, but is based on an SEC documentation approach, showing the types of things an officer will be asked to certify. We have highlighted a couple of phrases in the exhibit in ***bold italics*** to emphasize important points. Under SOx, the CEO or CFO is asked to personally assert to these types of representations, and they could be held criminally liable if incorrect. While the officer is at risk, the support staff—including internal audit and risk management—should take every precaution possible to make certain the package presented to the signing or authorizing officer is correct.

In the first years of SOx, starting perhaps in 2004 or 2005, the SEC has taken some strong investigatory and legal actions against corporate officers when a level of wrongdoing was suspected. For example, there were more SEC legal actions filed by the SEC in 2004 than had been filed in all of the years of the SEC's history going back to 1933! The CRO and chief audit executive (CAE)—the head of internal audit—should recognize this legal

GLOBAL COMPUTER PRODUCTS, INC.
CERTIFICATE OF OFFICER/EMPLOYEE REGARDING
SARBANES-OXLEY COMPLIANCE

Certification: Understanding that we intend to rely upon these statements, the undersigned hereby certifies, represents, and warrants to each of them and to the Company as follows:

1. I have read those portions of the accompanying draft of the covered filing that relate directly to the scope of my responsibilities as an employee of the Company (the "certified information").
2. Based on my knowledge, the certified information, as of the end of the period covered by such filing, did ***not contain an untrue statement of a material fact*** or omit to state a material fact necessary to make the statements therein, in light of the circumstances under which they were made, not misleading.
3. Based on my knowledge, to the extent of the scope of the certified information, the certified information fairly presents, in all material respects, the financial condition, results of operations and cash flows of the Company as of the close of and for the period presented in the covered filing.
4. I am not aware of any deficiencies in the effectiveness of the Company's disclosure controls and procedures that could adversely affect the Company's ability to record, process, summarize, and report information required to be disclosed in the covered filing.
5. I ***am not aware of any significant deficiencies or material weaknesses*** in the design or operation of the Company's internal controls that could adversely affect the Company's ability to record, process, summarize, and report financial data.
6. I ***am not aware of any fraud, whether or not material***, that involves the Company's management or other employees who have a significant role in the Company's internal controls.

Signature: _____.

Dated this _____ day of _____, 20__.

Print Name:

Title:

EXHIBIT 7.6 OFFICER DISCLOSURE SIGNOFF EXAMPLE

action risk and take appropriate efforts to work with corporate managers to expand and improve internal controls and the like so that the senior officer signing such reports can honestly attest that the financial statement filing "did not make any untrue statement of a material fact" as referenced in point 2 of the sample form (see Exhibit 7.6). To establish such an environment,

the risk management and internal audit functions must place a strong emphasis on performing reviews surrounding significant internal control areas. This can be done through a detailed risk assessment of the internal control environments, discussions of these assessments with senior corporate officers, and then a detailed plan documenting how these internal control systems will be reviewed.

Risk managers and internal auditors should take particular care, given SOx rules, on the nature and description of any findings encountered during the course of their audits or risk assessment reviews, on follow-up reporting regarding the status of corrective actions taken, and on the distributions of these audit reports. Many risk assessment or internal audit reports may identify significant weaknesses in areas of the enterprise that are not material to overall operations. A breakdown in the invoicing process at one regional sales office may be a significant risk for that sales region, but will not be a materially significant internal control weakness if the matter is local and does not reflect a wider, pervasive problem, and if it was corrected after being discovered. There is always a need for good communications links with key financial officers in the enterprise such that they are aware of internal reviews performed, key findings, and corrective actions taken. Internal audit should also provide some guidance as to whether reported audit findings are material to the enterprise's overall system of internal control.

Although much of the emphasis on SOx since its enactment has been on Section 404 internal control assessment, Section 302 with its management attestations is equally as important. A SOx review team can review its internal controls and can identify control gaps or significant weaknesses in internal controls, but senior management has the responsibility to "go public" on such matters. ERM can play a significant role here in counseling senior managers on the potential risks associated with material internal control weaknesses. As discussed below, the term *material* is very significant here. There is no need to publish a long laundry list of identified internal control gaps, but only the ones that are significant to the enterprise. Too long a public list of not very important matters will send improper messages to others. However, if a corporate officer does not disclose key internal control weaknesses, he or she may face criminal actions.

The question of how much or what is "material" for SOx-related reporting continues to be an open question among professionals. Prior to SOx, public accounting firms used guidelines along the lines that only if an error or internal control failure altered reported earnings per share by some fraction of a cent, the matter would be considered "material" for purposes of

financial reporting. All other errors were considered nonmaterial. This meant that, in past years, the auditors for a large corporation could discover a very large value error in a transaction—perhaps several tens of millions of dollars—but would not investigate the reasons for that error or make some further adjustments because they considered it "nonmaterial" for an enterprise with accounts valued in the hundreds of millions. Prior to SOx, this decision to define a transaction as material was really an external auditor's judgment call.Of course, the error that was considered to be nonmaterial to the external auditors might often be considered much more material or significant to the internal auditors and other members of management.

With SOx, the SEC has indicated that *their* existing legal standards for materiality will now apply. That is, information is now generally considered to be material if:

- There is a substantial likelihood that a "reasonable investor" would consider it unimportant in making an investment decision, and
- There is a substantial likelihood that that the information would be viewed by the reasonable investor as having significantly altered the total mix of available information.

The SEC has taken a further position that quantitatively small accounting errors may still be considered material under certain circumstances and that simple percentage thresholds for determining are not appropriate.

This really says that all involved parties in an internal accounting controls and financial audit process need to have a consistent understanding on what is a material error. An internal control error causing an accounting error that is reported in an internal audit report but ignored by the external auditors could cause trouble for the corporation's officers signing the final financial reports if they are unaware or ignore the reported error. Given the era in which SOX was enacted, all parties would probably benefit from lowering their thresholds for materiality such that more potential errors are viewed as material. The SEC and PCAOB announced future changes are moving in that direction to better rationalize matters here.

Internal audit and ERM needs to work closely with senior management and the audit committee to ensure that there is a consistent definition of materiality when reporting errors or omissions. There is no need for a situation where external audit has ignored some internal controls that a recently issued internal audit or risk assessment review report has identified as "serious." Such a discrepancy places the senior officers signing off on these report in a potentially difficult situation.

Financial Officer Codes of Ethics

SOx requires that corporations must adopt a code of ethics for their senior financial officers, including the CEO and principal financial officers, and disclose their compliance with the code to the SEC as part of the annual financial reporting. Employee codes of ethics or conduct have been in place in some enterprises for many years. They evolved from formal ethics initiatives in many larger corporations in the early 1990s, but were often established with staff and first-line supervisory employees in mind rather than the senior managers and officers. These codes defined a set of rules or policies that were designed to apply for all employees and covered such matters as policies on the protection of company records or on gifts and other benefit issues.

SOx brings enterprise codes of conduct to new levels. Since the mid-1990s, this area has become very important for many enterprises. With a growing public concern about the needs for strong ethical practices, many enterprises have appointed an ethics officer to launch such an initiative with a code of conduct as a first step. However, while that code of conduct received senior officer endorsement, it was often directed at the overall population of employees, not the endorsing senior officers themselves.

SOx does not address the content of these enterprise-wide codes of ethics, but focuses on the need for the same standards for senior officers as for all employees in the enterprise. SOx specifically requires that an enterprise's code of ethics or conduct for senior officers must reasonably promote:

- Honest and ethical conduct, including the ethical handling of actual or apparent conflicts of interest between personal and professional relationships.
- Full, fair, accurate, timely, and understandable disclosure in the enterprise financial reports.
- Compliance with applicable governmental rules and regulations.

Many larger enterprises today have established ethics-type functions, but smaller ones often have not. If an ethics function is not in place, management should launch such an initiative for all members of the enterprise, board members, officers, and employees. Efforts should be made to ensure that this code applies to all members of the enterprise and is consistent with SOx rules. The key issue here is that the code of conduct should have been communicated to senior management, and that these officers have agreed to comply with it. While others in the enterprise can make certain that the

existing code of conduct is consistent with SOx, the CAE is a key person to communicate that information the audit committee.

An enterprise faces a greater challenge here if they have no formal ethics function, no code of conduct, or just a code that has not been effectively communicated throughout the enterprise. While SOx compliance processes can be established just for the senior officers enumerated in SOx, this is the ideal time to launch an ethics function throughout the enterprise that applies to senior management and to all employees as well.

A strong ethics function should be promoted throughout the enterprise and not just as an SOx legal requirement. A strong set of ethical standards can get an enterprise through a crisis situation and help it to not accept unnecessary risks. A motivation for SOx and its strong provisions in these areas was the perception that certain corporate officers were operating on the basis of personal greed with no consideration for strong ethical values, as evidenced by correct and accurate financial reporting. However, a code of conduct outlining a strong set of ethical standards will encourage an enterprise to operate with better internal controls and encourage taking only appropriate risks.

Sarbanes-Oxley: The Other Sections

SOx is a major set of legislation with rules and provisions covering many areas of both corporate and external auditing related rules. From the perspective of ERM, we have briefly discussed Section 404 on reviews of internal controls and Section 302 on management's formal responsibility to report those controls, and on codes of conduct for corporate officers. These are areas that are particularly important to an effective ERM program. Other areas of SOx cover corporate audit committees, external audit firm prohibitions and responsibilities, and securities analyst conflicts of interest. The Act really tried to cover and provide rules for a wide variety of then "hot" problems that all seemed to come together in about the same time period as the fall of Enron and the collapse of the dot-com bubble. While not an all-inclusive list and in addition to Sections 302 and 404, SOx also establishes other important rules in the following areas:

- *Corporate audit committees.* These important board committees now must take a much more active role in their reviews of the audit functions in their organizations as well as reviews of financial transactions. At least one member of the audit committee must be a designated "financial expert." In addition, all members of the audit

committee must be outside directors, not members of the management team. Some of the SOx-initiated rules for audit committees are discussed in Chapter 8.

- *Boards of directors.* In addition to just the SOx audit committee enhanced procedures, full boards of directors can no longer accept consulting contracts from management and must operate with a variety of proscribed better governance rules.
- *External auditors and the auditing profession.* As mentioned, the AICPA no longer sets new auditing rules for SOx-registered corporations. The PCAOB is responsible for issuing external auditing standards. In addition, external audit firms can no longer establish outsourced internal audit functions and financial consulting practices for the enterprises they audit.
- *Financial reporting rules.* Corporations can no longer use what were called "pro-forma" rules for reporting financial results. They previously reported results on the basis of expected but not actual events. GAAP now must always be used.
- *Securities analyst conflicts of interest.* Very much an issue when SOx was being drafted, some securities analysts were looking at the same investment situation and giving conflicting messages to investors and to their own investment banker clients. There were numerous situations where an analyst said "Buy, Buy" to investors but told internal cohorts the same stock was "junk." SOx rules have been established here.

The preceding bullet points highlight a few of the other important aspects of SOx, and there are many other rules as well.[7] Many of these rules are particularly important for managers involved with elements of corporate governance. Professionals involved with ERM should focus on both the important Sections 302 and 404 as well as how compliance with other provisions in other elements of SOx will be consistent with the risk management program for an enterprise.

SOX AND COSO ERM

Although two separate enterprise initiatives, there are some close relationships between the SOx regulatory rules and the COSO ERM framework. While the chapters of this book generally focus on establishing an effective ERM process in an organization, following the COSO ERM framework,

compliance with SOx rules is even more important—it is the law. There are some broad differences between the two as well as many common threads and requirements. A major difference, of course, is that SOx primarily focuses on accurate financial reporting and related corporate governance issues. COSO ERM takes a broader view of things and covers all risks surrounding an enterprise. An enthusiastic and dedicated CRO or other member of the risk management function might argue that COSO ERM is even more important than SOx, as it covers such a wide range of potential enterprise risks. However, an enterprise CFO who could do prison time due to some fouled-up financial reporting may view the risks of a SOx violation as far more significant than probabilistic estimates of a significant enterprise risk.

The implementation of an effective ERM program should be closely coordinated with efforts to establish effective SOx compliance. While SOx focuses primarily on financial reporting and ERM on a larger view of enterprise risks, the functions coordinating each should closely work together and coordinate their activities. An effective ERM program, as described in Chapter 5, should become very aware of the risks associated with SOx rules noncompliance and should communicate appropriate risk matters to senior corporate management for possible consideration in any Section 302 reporting.

NOTES

1. For a more detailed explanation of SOx, including a description of all aspects of this important legislation, see Robert Moeller, *Sarbanes-Oxley and the New Internal Auditing Rules,* New York: John Wiley & Sons, 2004.
2. Peter Schwartz and Peter Leyden, "The Long Boom: A History of the Future, 1980–2020," *Wired,* Issue 5.07, July 1997.
3. For more information on the PCAOB and its standards, see *www.pcaobus.gov*.
4. For an introduction to these audit sampling techniques, see Robert Moeller, *Brink's Modern Internal Auditing,* 6th ed., Chapter 16.
5. IT Control Objectives for Sarbanes-Oxley, 2nd edition, Information Systems Audit and Control Association (ISACA), Rolling Meadows, IL, 2006.
6. PCAOB Audit Standard N. 2, paragraph C5, pcaobus.org/standards
7. For a section-by-section overview of SOx, see Robert Moeller, *Sarbanes-Oxley and the New Internal Auditing Rules.* Hoboken, NJ: John Wiley & Sons, 2004.

8

IMPORTANCE OF ERM IN THE CORPORATE BOARD ROOM

A board of directors is the ultimate manager of all stockholder, investor-owned enterprises as well as for most large private organizations. Directors may be either elected from the existing stockholders, known as outside or nonemployee directors, or may be directors selected from the very senior members of management, called inside or employee directors. While their overall tenures in office and general responsibilities are based on established corporate charter and bylaw documents, boards of directors are charged with independently reviewing and approving all major decisions for the enterprises they manage. They are *th*e independent managing representatives for the stockholders, with a responsibility to make major decisions for the corporation based on their assessment of the risks and potential benefits presented to them. However, over the years and up until very recent times, the responsibility of the board of directors as an independent managing authority began to somewhat erode in many corporations. Until recent

years and before the Sarbanes-Oxley Act (SOx), it was common for the majority of a board to consist of inside directors—officers of the corporation itself and hardly independent managers. In addition, many of the outside or nonemployee directors were often friends of the chief executive officer (CEO). These friends-of-the-CEO directors were often very loyal and financially obligated to the CEO, who rewarded them with lush "consulting" fees and other benefits in addition to their board meeting attendance fees. All too often, many corporation board-of-director decisions prior to SOx were sometimes little more than "rubber stamp" actions affirming decisions or wishes of the CEO.

A combination of increased shareholder activism and some of the requirements of SOx have really changed things. Today, board audit committees must consist of only independent directors, SOx rules have abolished director consulting fee rewards, and poor board decisions may result in litigation against individual board members. The board is responsible for reviewing major activities throughout the corporation and for making major and often risk-based decisions. They are key players in a corporation to make truly enterprise-wide risk decisions. An effective implementation of the Committee of Sponsoring Organizations' enterprise risk management (COSO ERM) framework provides an important approach and methodology for the board of directors to assess risks and to make better decisions for an enterprise and its shareholder owners.

This chapter considers the role of corporate boards of directors in managing corporate risks and the importance of introducing COSO ERM to today's board. The chapter

will consider the organization and decision-making processes that are common in boards of directors and suggest approaches for effectively implementing COSO ERM both for overall organization decision-making guidance and as a process for helping the board make its decisions. In addition, the chapter will discuss the importance of establishing a board-level risk committee, operating in parallel with the audit committee. While managers at all levels can use COSO ERM to make better operational and various levels of strategic decisions, the broad organization-wide perspective of COSO ERM is an important tool for helping board members to better consider and evaluate the risks facing their organizations.

An organization's board of directors and its individual members are a level above enterprise senior management and somewhat beyond the organization charts and procedures that most employees encounter. Going well beyond the human resources (HR) function, members of the board are typically nominated by existing board members or major investors and are officially elected by the stockholders at an annual meeting. While major investors, bankers, and the CEO often have a role in recruiting board members, the board and a majority of the stockholders make essentially all major decisions for the enterprise, including terminating the CEO or making major risky decisions. Public corporation board governance procedures and other operating procedures are essential for assessing and dealing with risks. While this chapter is not intended to be guidance on "how to be a board member," it provides some background on board members and their audit and risk committee operations in light of COSO ERM. With the exception of senior corporate

officers and key members of the internal audit function, most corporation employees have little contact with their boards of directors beyond seeing a face in the annual report. It is important for all employees and managers to understand how their boards operate and manage the operations and risks that impact all employees and other stakeholders.

BOARD DECISIONS AND RISK MANAGEMENT

Although the typical employee works a 40-plus-hour regular workweek, nonemployee board members are usually not involved in daily, full-time workweek activities. Rather, boards operate on a part-time basis. A board may formally meet only once a month for several days or less. However, this is much more than the "part-time job" as we often think of that concept. Board members will serve on multiple committees beyond the formal full board meetings, often will have multiple telephone committee meetings during interim periods, and are responsible for reviewing and understanding often massive amounts of financial, operational, and other reports concerning the corporation they are managing. While this may be a "part-time job" for a given board member at a single corporation, that same individual may often serve on similar boards for other corporations. The CEO and a limited number of other corporate officers, such as the CFO, may also sit on the board in the role of inside or employee directors in addition to their regular job duties. While a board may formally meet for only a few days once a month, their service is hardly a part-time job!

Board decisions and the directions given to the corporation they govern, are based on actions taken in periodic board meetings. These decisions can have an important impact on the overall enterprise. For example, based on good financial results and a strong balance sheet, the board can declare an extra or increased dividend. This type of decision is usually based on prior recommendations and agreements with senior management, who will then be responsible for communicating the decision and making changes to supporting processes to initiate the action. This is the type of regular board decision that is made in the course of the normal business cycle. As a clarification here and throughout this chapter, references to "the board's" making a decision means that a majority of board members have agreed on

some action. A board of directors operates as a committee representing the stockholders. If a corporation has a nine-member board, for example, a majority of only five must agree on some action, and that majority rules.

The board can also make decisions that do not have management's full concurrence. The board may decide on a major reorganization, such as sale of a division to some other entity or acting on a merger proposal—either friendly or hostile—from another organization. Sometimes, these board decisions are made totally contrary to senior management wishes. For example, the board may decide to shut down an unprofitable business unit. The CEO may totally disagree with such a decision, but the CEO, even if serving as an employee director and chair of the board, has only one board vote. The CEO can make a case to keep and not dispose of the unprofitable unit in an open board meeting, but if the board's majority-rule decision goes against that CEO's wishes, management will have to shut down that unit, even though senior management or outside investment advisors disagree. Of course, for many—if not most—corporations, board decisions are generally collaborative, and boards are often tied very closely to the CEO and make many decisions based on that executive's recommendations. In addition, many CEO's are strong and powerful people with influence and persuasive powers that can heavily influence other board members. However, the board can overrule the CEO and can just as easily terminate the services of a CEO or some other senior officer and take actions to bring in someone new. Some corporations have both a separate CEO and a chair of the board, two powerful leaders who should work closely together for the greater good of the corporation. In many other cases, one leader holds joint chair of the board and CEO titles. The trend today is perhaps for two separate leaders here.

The understanding, evaluation, and acceptance of risk should be a major consideration in almost every board decision. Because of their most senior positions in organizations, board members are expected by many outside of the boardroom—investors, regulators, and others—to have a strong understanding of their corporation and the risks it faces. Just because of their very senior positions in the corporation, directors should generally have a good understanding of many of the specific risks that their companies face, such as risks associated with introducing a new product into a very competitive marketing environment or of committing capital into a volatile area with the possibility of high rewards. As part of good management practices, directors are expected to have a good understanding of managing a wide range of enterprise-level risks. While directors must comply with financial and accounting regulatory rules—such as Securities

and Exchange (SEC) rules in the United States—there are no specific rules or requirements for the director-level management and understanding of risks. COSO ERM has provided a framework for understanding these risks, but traditionally directors often have had no specific guidance or rules covering their acceptance and understanding of dealing with enterprise-level risks.

While directors have always realized that their decisions entailed risks, and that they should be making those risky decisions in the best interests of the corporations they were governing, there was no formal, recognized framework for board-level risk assessment prior to COSO ERM. Perhaps the most major concept of COSO ERM is this emphasis of *enterprise*-wide risk management, the very decision area that impacts a corporate director. A manager in a product manufacturing organization, for example, should think of risks associated with the operation of the equipment on the production floor, outside vendors supplying raw materials, and risks associated with the worldwide tastes and acceptance of the manufactured products. COSO ERM calls for the manager to think of and deal with risks on a larger, wider plane. Just as a manufacturing manager should think of enterprise risks on a wider horizon, a corporation director must always have this "big picture" concept of enterprise-wide risk in mind when making nearly all decisions. The COSO ERM framework provides an excellent model for many board-level decisions, and board members must always keep in mind that their decisions usually cover a wide spectrum. Closing a plant, for example, can present logistics risks in moving people and equipment to sustain operations, legal risks associated with various plant-closing notification risks, and public relations risks in appropriately communicating the closure plans. COSO ERM is a very important board of directors–level concept here.

While directors are expected to have a good understanding of their corporation, its issues, operations management problems, and many other surrounding rules, recent research indicates that many directors of major corporations today do not always have a good understanding of overall risk management and of the concepts of both ERM and the supporting COSO ERM standards. The Conference Board, a major corporate governance research group, recently surveyed over 125 major corporation board members, conducted direct interviews with a smaller group of them, and found that many of these directors do not appear to have a good understanding of many aspects of risk, including COSO ERM. In a June 2006 study,[1] it was found that U.S. corporate directors tend to approach the risks facing their organizations only on a case-by-case basis rather than looking at risks from

an overall ERM perspective. This is despite comments in past chapters here about the importance of looking at risks from an enterprise-wide perspective.

The Conference Board found that while corporate directors seem to have a high-level, top-down understanding of risk and that 89.5 percent reported that they understand the implications of their current corporate risk management strategies:

- Only 77.4 percent of the directors surveyed said they fully understand the risk/return trade-offs underlying that current corporate risk strategy. In addition, nearly one-third of major corporation directors, 33.6 percent, do not appear to understand that risks must be balanced against the potential rewards associated with those risks.
- Only 73.4 percent of directors feel that their companies fully manage risk. This says that these directors know there are risks in the corporations they govern, but they are not really sure if their senior managers are properly managing those risks.
- Only 59.3 percent of directors fully understand how business segments in their organizations interact in an overall risk portfolio. This finding says the concept of enterprise risk, as defined and discussed through COSO ERM, has really not been communicated to some 40 percent of the directors that are managing major U.S. corporations.
- Only 54.0 percent of directors have clearly defined risk tolerance levels. This finding is similar to the previous one that says directors do not understand how the corporations they manage can juggle the risks they face. This finding says that some 46 percent of directors do not have an established set of standards—risk tolerance levels—to help them to decide when to accept or reject some risk-related opportunity.
- Only 47.6 percent of the boards rank their key risks. While many of the chapters in this book have discussed the importance of ranking all risks from high to low, this finding says that only half of major U.S. corporations go through this process on an overall corporate board level. To some extent this finding is understandable because the board will, or should, expect groups, such as marketing or new-product development, to rank their risks before presenting the higher payback ones to the board. However, directors are or should be looking at risks and potential rewards on a worldwide basis and should be going through their own risk-ranking processes.

- Only 42.0 percent of the boards in the survey have formal practices and policies in place to address risks to the overall corporate reputations. A bad outcome in some area could massively damage the reputation of a corporation. However, this finding says that over half of the corporations surveyed do not have policies in place to consider risks that could damage the overall reputation of the corporation.

With COSO ERM now out and in front of corporate directors, these mid-2006 survey results should be viewed as troubling! The Conference Board is a highly respected organization in the corporate governance world, and directors of major corporations can be expected to give honest, forthright responses to such a survey or in face-to-face interviews. Still, the directors surveyed are reporting that they understand risk only in a general sense, but they often do not really have a good understanding of the risk environments in the corporations that they govern!

While previous chapters have discussed the importance of recognizing and managing risks at all levels, this understanding is particularly important for the most senior managers of an enterprise—its board of directors. Persons within an enterprise who have the most direct contact with board members, such as the CEO, CFO, legal counsel, chief risk officer (CRO), and chief audit executive (CAE), should work with their board members to ensure that there will be consistent management and understanding of the risks surrounding the enterprise and of COSO ERM. Understanding the board committee organization structure, governance responsibilities, and its key committees is essential for understanding board decision processes and how COSO ERM might be better incorporated in board decision processes.

BOARD ORGANIZATION AND GOVERNANCE RULES

Employees working for a corporation are accustomed to following a fairly structured set of organizational rules and procedures, regardless of their employment level or position in an organization. All are expected to follow corporate code-of-conduct guidelines, to generally tailor their work hours to normal operating procedures, and to follow corporate policies and procedures. These are organization-specific as well as legal rules. Other employee practice guidelines are also defined through various professional standards or labor-related bargaining unit agreements. An accountant, for example, should be following generally accepted accounting principles (GAAP) as part of his or her work, and internal auditors are expected to follow the standards published by their professional organization, the Institute of Internal Auditors (IIA). However, an employee or

even a supervisor on the shop floor will probably not be aware of these specific GAAP accounting or IIA auditing guidance procedures. Some of these rules or standards may apply to all employees, while others are very specific. Beyond legal and corporate policy rules, employees also are expected to follow a wide range of good practice guidelines.

Just as every employee has many rules and best practice guidelines to consider as part of day-to-day work activities, an elected board member also must follow a wide range of legal, ethical, and good business practice rules and procedures. In addition, because the board of directors is responsible for the overall governance of the corporation, the collective board and its individual members are responsible for ensuring compliance with virtually all of the rules and regulations that may impact the corporation and all of its employees. However, an individual board member and particularly an independent director is not subject to the same types of detailed rules that govern a typical employee. There often are no "employee handbooks" for a board member to provide guidance for ongoing decision-related activities. A board will have established a high-level corporate charter and bylaws that sets broad rules for all governance activities. In addition, past board resolutions and policies establish governance practices, but a board is an independent high-level committee that can set many of its own rules. They can rely on key employees, such as help from the CFO on finance question issues, and they will often bring in other inside or outside experts and other published guidance materials to provide help in many other areas. However, as the senior or ultimate decision makers in an organization, the board can really set many of its own rules beyond legal restrictions. While many, if not most, boards and their members exercise prudent care over the corporations they govern, there will always be boards of directors that make high-risk, bad, or even potentially criminal decisions. When this occurs, they can be subject to criticism or even legal action by stockholders or actions by regulatory authorities such as the SEC.

While COSO ERM will not prevent a board from making high-risk or bad decisions, it can provide some help and guidance for making better decisions on a board or board committee level. Because a board of directors is structured on a different level than a typical hierarchical business organization, we often forget that a board operates in a majority-rule committee structure. While the board chair—frequently, but not always, the CEO—may want the board to take some action for the corporation, a majority of board members may vote to take a different action. The following sections discuss this typical board-of-directors committee structure and

how individual board members should manage and understand enterprise-level risks.

Corporate Charters and the Board Committee Structure

A corporate charter is the authorizing document setting the high-level rules and procedures for a corporation. In the United States, corporations are registered through state registration authorities, with various governance and taxing rules different for each state. Based on this registration, every corporation should have a high-level registered charter as well as some detailed bylaws. These documents establish the basic governance rules for a corporation, such as the size of the board, terms of service of board members, and board meeting voting arrangements. The purpose of this chapter is not to discuss basic corporate board organization concepts or rules but to highlight the importance of COSO ERM in a board of directors' framework and to discuss how board committees should support this initiative. A basic book on corporate organization will provide this information. For a corporation, a charter and its bylaws are similar to a constitution for a country or political unit. They provide the high-level rules used to govern the corporation. Just as a political unit is empowered and governed by its franchised voters, who established that constitution and must vote to amend it, a corporate charter and its bylaws sets the high-level and broad rules of corporate governance and can be changed only by amendments through a majority vote of the stockholders. Among many other matters, the corporate charter and bylaws define the size and general organization of the board, any special board voting rules, and the terms in office for individual directors. For publicly held corporations, governmental securities regulators set another very important level of rules. In the United States, the SEC has released a large set of other corporate and board governance rules that are above the corporate charter and its bylaws For example, the SEC has regulations covering board audit committees—rules that became even more significant after SOx. The importance of the audit committee and other committees in the effective management of risks is discussed below.

Boards operate very much in a majority-rule type of committee structure, where the board chair conducts meetings but must abide by committee majority votes. As in any committee organization structure, many decisions and actions depend on the strengths, opinions, and persuasive powers of individual board members. The board chair may exercise a powerful influence over other board members but can be outvoted through a board member majority vote decision. To many corporate employees, whether on staff or

even fairly senior management, the board of directors' structure often seems remote and difficult to understand. Following their established meeting schedules, nonemployee director board members typically arrive at corporate headquarters or at an off-site location for their scheduled—often monthly—board meetings. Inside or employee directors, such as the CEO and CFO, will join these meetings, as will other invited persons, such as the general counsel, CAE, or the external audit partner. Under the leadership of the board chair, they will meet in what is usually an almost closed-door meeting. The point here is that regular board meetings are not open to the public, and the nonemployee directors may even ask the CEO to leave the room for some critical decision matters. Internal minutes are taken, and decisions are documented through meeting minutes and formal board resolutions. While some board activities, such as the release of financial results or plans to launch an acquisition, are communicated through press releases or other announcements, much of the board activity takes place in private in a confidential, closed-door environment. The exception here is the annual meeting, where stockholders are invited to attend an open session and to vote on nominated directors, changes to charter-based corporate rules, and shareholder proposals. The annual meeting is a forum where stockholder attendees can ask members of the board direct questions in an open forum. Otherwise, many board-meeting activities are relatively confidential.

Many of a board's activities take place through a series of specialized committees, such as the compensation or the audit committee. Board members typically will sit on one, two, or more of these board committees, which will meet either concurrently with regular board meetings or at other times. While many corporate functions have large support staffs, board members operate essentially as individuals. For example, a corporation may have a large finance and accounting staff, while only a small number of directors make many high-level decisions here, with the help and support of the CFO, external and internal auditors, and other consultants. The committees have their own organization charter documents, meet multiple times as necessary, keep minutes of their decisions, and report any recommendations for change to the full board for action.

As discussed, a board of directors and its committees often seem rather remote to a typical corporate employee. However, that same corporate employee might find the activities of a board organization and its supporting committees similar to operations found with many professional and civic organizations. A more junior member of a corporate internal audit staff may attend local chapter IIA meetings and will listen to the president of that specific area–based IIA chapter announce the meeting speaker and

discuss other planned upcoming activities. Although this direct comparison to a corporate board falls down for many reasons, that IIA chapter has its own board of directors who fund meeting speakers and authorize other activities. The chapter also has a set of bylaws to describe or limit its activities. Other chapter members, who are not necessarily board members, volunteer to take on other activities such as meeting registrations. While this analogy between an IIA chapter and a corporate board can be easily stretched too far, those IIA board members must consider some organizational risks as well. They can contract with an outside speaker and organize a special seminar for IIA chapter members on what they feel might be a topic of interest, such as understanding COSO ERM. Although certainly a pertinent topic, the chapter board faces a wide range of cost and logistic risks in launching their chapter activities.

The failure of local chapter IIA board in some activity, such as a poorly organized technical session, can be embarrassing to chapter members and may put a dent in the IIA chapter's voluntary finances. However, risks are often not that much greater. Activities and risks are very different for a corporate board and its individual board members. Board actions can be viewed as contrary to state securities regulations and, much more significantly, SEC reporting and governance rules. Violations can result in fines or legal or even criminal actions. Individual corporate board members can also be subject to legal actions, but corporations generally acquire what is called directors and officers (D&O) insurance to protect board members against civil legal actions.

A board of directors has many responsibilities in managing the overall operation of a corporation. Risk oversight and the management of risks are major components of those activities and board responsibilities. This was stated quite appropriately by the National Association of Corporate Directors in a 2002 report on a board's risk oversight responsibilities[2]:

> The board's role, quite simply, is to provide risk oversight. This means making sure that management has instituted processes to identify, and bring to the board's attention, the major risks the enterprise faces. It also means the continual reevaluation of these monitoring processes and the risks with the help of the board and its committees.

These are strong words, but they place a challenge on the individual members and the total board. Members must try to identify the potential risks facing the organization and then understand the potential implications and consequences of these various risks. This can be daunting for the board member who receives only supporting data about an upcoming potential risk-based decision; has an opportunity to ask further questions about the

matter, often during a tight agenda and limited-time board meeting; and then must vote to take appropriate actions regarding that risk. This type of activity is coupled with all of the other matters that may be of concern before the board.

Because board members and particularly nonemployee members operate as part-time participants with typically many other responsibilities, they usually face a huge number of items of concern with limited time to review and resolve the matters. This is a particular challenge because board members operate as individuals, without a supporting staff. To add some efficiency to board operations, committees are established to help with their decision processes. Some of these committees are required under SEC rules, while others will be established due to a board decision. Major board committees include:

- *Audit committee.* This SEC-mandated board committee is responsible for supervising the internal audit function, hiring and reviewing the work of external auditors, approving periodic financial reports, and many other activities. and their role in the risk management process are discussed in the next section.
- *Nominating committee.* This committee is responsible for helping to recruit new director candidates, when a need arises, and to place them on voting ballots at subsequent annual meetings.
- *Compensation committee.* Another SEC-required committee, the compensation committee makes officer- and bonus-related decisions for the corporation. Working closely with the corporation's human resources function, the compensation committee also reviews and approves stock option and other deferred-benefit programs.

Corporate boards may establish a wide range of other committees, depending on the type of issues surrounding the corporation. For example, a corporation involved in developing new technology-related products and acquiring other smaller companies to develop these lines of business may establish a board technology committee to review items of interest and make recommendations for action to the overall board. With ongoing interests in the area, many corporations today have established ethics and governance committees. The following sections discuss the roles and responsibilities of two important risk management–related board committees: audit committees and a newer, evolving corporate board committee, the risk committee.

AUDIT COMMITTEE AND MANAGING RISKS

With their responsibilities of supervising the internal and external audit functions and approving periodic financial reports, audit committees have had a high level of responsibility in corporate governance for an extended period of time. However, until the late 1980s, many audit committees too often were little more than "paper tigers," as they often did not really exercise that much of an independent audit authority. In those earlier years, there were no restrictions on which directors could serve on their audit committees. This sometimes resulted in employee directors, even the CFO, serving on the board audit committees and approving the financial results—a classic "fox guarding the chicken coop" situation and hardly a separation of duties! The rules for corporate audit committees began to change in the 1980s with first the New York Stock Exchange (NYSE) and then other security exchanges requiring that all members of an audit committee be independent, nonemployee directors. Then, in December 1999, the SEC issued audit committee rules covering such matters as director independence, qualifications, charters, and outside auditor involvement.

While suggested improved standards for audit committee members was a frequent topic in corporate governance literature, things really changed again after the fall of Enron and the passage of SOx. Legislative hearings at that time found out that the Enron audit committee was connectly composed of nonemployee directors. However, testimony and hearings also revealed that many members of that Enron audit committee could demonstrate no strong understanding of the complex financial transactions that caused, or at least helped, Enron to fail as fast as it did. In addition, that Enron audit committee spent only very limited amounts of time in reviewing and approving some very complex transactions. It did not help that the Enron audit committee relied on the advice of the then external auditors, Arthur Andersen, who turned out to be very close to designing many of these same complex financial transactions.

The world has changed, and today the audit committee has become the most high profile of all board-of-directors committees. Beyond decisions by the overall board and its chair, audit committees receive attention because of their financial and internal control review responsibilities. These audit committee board members review and act on often confidential audit findings as well as review and approve the enterprise's audited financial statements. Audit committees have come under extreme attention since the fall of Enron and the launching of SOx in 2002, and are now required to be a committee of nonemployee directors.

With some internal audit departments today changing their names or titles from just "internal audit" to the "risk assessment department," some boards have changed their names or titles from that of the "audit committee" to the "risk management" committee. However, these changed-name board committees often continue to focus on their traditional audit committee roles, such as an overview and approval of the internal and external audit functions, with perhaps less emphasis on overall enterprise risk issues. Audit committees define their roles and responsibilities through formal audit committee charters. While there are many examples of corporate audit committee charters that are published in corporate proxy statements, Exhibit 8.1 shows the audit committee charter for the major and very well-respected semiconductor manufacturer, Intel Corporation, as of March 29, 2005. Similar to other audit committee charters, this document outlines the major functions of the Intel audit committee in a fairly lengthy list including:

INTEL CORP. CHARTER OF THE AUDIT COMMITTEE AS AMENDED AND RESTATED, FEBRUARY 2, 2005

THE PURPOSE OF THE AUDIT COMMITTEE.

The purpose of the Audit Committee is to represent and assist the Board of Directors in its general oversight of the company's accounting and financial reporting processes, audits of the financial statements, and internal control and audit functions. Management is responsible for

- **a.** the preparation, presentation and integrity of the company's financial statements;
- **b.** accounting and financial reporting principles; and
- **c.** the company's internal controls and procedures designed to promote compliance with accounting standards and applicable laws and regulations. The company's independent auditing firm is responsible for performing an independent audit of the consolidated financial statements in accordance with generally accepted auditing standards.

The Audit Committee members are not professional accountants or auditors and their functions are not intended to duplicate or to certify the activities of management and the independent auditor, nor can the Committee certify that the independent auditor is "independent" under applicable rules. The Audit Committee serves a board level oversight role where it oversees the relationship with the independent auditor, as set forth in this charter, receives information and provides advice, counsel and general direction, as it deems appropriate, to management and the auditors, taking into account the information it receives, discussions with the auditor, and the experience of the Committee's members in business, financial and accounting matters.

EXHIBIT 8.1 INTEL CORPORATION AUDIT COMMITTEE CHARTER*

INTEL CORP. CHARTER OF THE AUDIT COMMITTEE AS AMENDED AND RESTATED, FEBRUARY 2, 2005

MEMBERSHIP AND STRUCTURE.

The Audit Committee is comprised of at least three directors determined by the Board of Directors to meet the director and audit committee member independence requirements and financial literacy requirements of The NASDAQ Stock Market, Inc. ("NASDAQ"). At least one member of the Committee must be financially sophisticated, as determined by the Board, and no Committee member may have participated in the preparation of the financial statements of the company or any of the company's current subsidiaries at any time during the past three years, each as required by NASDAQ listing standards. Appointment to the Committee, including the designation of the Chair of the Committee and the designation of any Committee members as "audit committee financial experts", shall be made on an annual basis by the full Board upon recommendation of the Nominating Committee. Meetings of the Audit Committee shall be held at such times and places as the Audit Committee shall determine, including by written consent. When necessary, the Committee shall meet in executive session outside of the presence of any senior executive officer of the company. The Chair of the Audit Committee shall report on activities of the Committee to the full Board. In fulfilling its responsibilities the Audit Committee shall have authority to delegate its authority to subcommittees, in each case to the extent permitted by applicable law.

RESPONSIBILITIES.

The Audit Committee:

- Is directly responsible for the appointment, replacement, compensation, and oversight of the work of the independent auditor. The independent auditor shall report directly to the Audit Committee.
- Obtains and reviews annually a report by the independent auditor describing the firm's internal quality-control procedures; any material issues raised by the most recent internal quality-control review or peer review or by any inquiry or investigation by governmental or professional authorities, within the preceding five years, respecting one or more independent audits carried out by the firm, and any steps taken to deal with any such issues.
- Reviews and discusses with the independent auditor the written statement from the independent auditor concerning any relationship between the auditor and the company or any other relationships that may adversely affect the independence of the auditor, and, based on such review, assesses the independence of the auditor.
- Establishes policies and procedures for the review and pre-approval by the Committee of all auditing services and permissible non-audit services (including the fees and terms thereof) to be performed by the independent auditor.

EXHIBIT 8.1 INTEL CORPORATION AUDIT COMMITTEE CHARTER* *(CONTINUED)*

INTEL CORP. CHARTER OF THE AUDIT COMMITTEE AS AMENDED AND RESTATED, FEBRUARY 2, 2005

- Reviews and discusses with the independent auditor:
  - **a.** its audit plans, and audit procedures, including the scope, fees and timing of the audit;
  - **b.** the results of the annual audit examination and accompanying management letters; and
  - **c.** the results of the independent auditor's procedures with respect to interim periods.
- Reviews and discusses reports from the independent auditors on
  - **a.** all critical accounting policies and practices used by the company,
  - **b.** alternative accounting treatments within GAAP related to material items that have been discussed with management, including the ramifications of the use of the alternative treatments and the treatment preferred by the independent auditor, and
  - **c.** other material written communications between the independent auditor and management.
- Reviews and discusses with the independent auditor the independent auditor's judgments as to the quality, not just the acceptability, of the company's accounting principles and such further matters as the independent auditors present the Committee under generally accepted auditing standards.
- Discusses with management and the independent auditor quarterly earnings press releases, including the interim financial information and Business Outlook included therein, reviews the year-end audited financial statements and "Management's Discussion and Analysis of Financial Condition and Results of Operations" and, if deemed appropriate, recommends to the Board of Directors that the audited financial statements be included in the Annual Report on Form 10-K for the year.
- Reviews and discusses with management and the independent auditor various topics and events that may have significant financial impact on the company or that are the subject of discussions between management and the independent auditor.
- Reviews and discusses with management the company's major financial risk exposures and the steps management has taken to monitor and control such exposures.
- Reviews and approves related-party transactions (as defined in the relevant NASDAQ requirements).
- Reviews and discusses with management, the independent auditor, and the company's chief audit executive (CAE):

EXHIBIT 8.1 INTEL CORPORATION AUDIT COMMITTEE CHARTER* *(CONTINUED)*

INTEL CORP. CHARTER OF THE AUDIT COMMITTEE AS AMENDED AND RESTATED, FEBRUARY 2, 2005

a. the adequacy and effectiveness of the company's internal controls (including any significant deficiencies and significant changes in internal controls reported to the Committee by the independent auditor or management;

b. the company's internal audit procedures; and

c. the adequacy and effectiveness of the company's disclosures controls and procedures, and management reports thereon.

- Reviews annually with the CAE the scope of the internal audit program, and reviews annually the performance of both the internal audit group and the independent auditor in executing their plans and meeting their objectives.
- Reviews and concurs in the appointment, replacement, reassignment, or dismissal of the CAE.
- Reviews the use of auditors other than the independent auditor in cases such as management's request for second opinions.
- Reviews matters related to the corporate compliance activities of the company, including the review of reports from the company's Ethics and Compliance Oversight Committee and other related groups.
- Establishes procedures for the receipt, retention and treatment of complaints received by the company regarding accounting, internal accounting controls, or auditing matters, and the confidential, anonymous submission by employees of concerns regarding questionable accounting or auditing matters.
- Establishes policies for the hiring of employees and former employees of the independent auditor.
- Publishes the report of the Committee required by the rules of the Securities and Exchange Commission to be included in the company's annual proxy statement.
- When appropriate, designates one or more of its members to perform certain of its duties on its behalf, subject to such reporting to or ratification by the Committee as the Committee shall direct.

The Audit Committee will engage in an annual self-assessment with the goal of continuing improvement, and will annually review and reassess the adequacy of its charter, and recommend any changes to the full Board.

The Audit Committee shall have the authority to engage independent legal, accounting and other advisers, as it determines necessary to carry out its duties. The Audit Committee shall have sole authority to approve related fees and retention terms.

EXHIBIT 8.1 INTEL CORPORATION AUDIT COMMITTEE CHARTER* *(CONTINUED)*

INTEL CORP. CHARTER OF THE AUDIT COMMITTEE AS AMENDED AND RESTATED, FEBRUARY 2, 2005

The Audit Committee shall meet at such times and places as the Audit Committee shall determine. The Audit Committee shall meet in executive session with the independent auditor, the CAE and management periodically. The Chairman of the Audit Committee shall report on Audit Committee activities to the full Board.

The Chairman of the Audit Committee is to be contacted directly by the CAE or the independent auditor (1) to review items of a sensitive nature that can impact the accuracy of financial reporting or (2) to discuss significant issues relative to the overall Board responsibility that have been communicated to management but, in their judgment, may warrant follow-up by the Audit Committee.

*Charter taken from Public Filing records as of 3/29/2005.

EXHIBIT 8.1 INTEL CORPORATION AUDIT COMMITTEE CHARTER* *(CONTINUED)*

Source: Used with permission of Intel Corporation

- Directly responsible for the appointment, replacement, compensation, and oversight of the work of the independent auditor, who reports directly to the audit committee.
- Reviews and discusses with management, the independent auditor, and the company's CAE:
  - The adequacy and effectiveness of the company's internal controls including any significant deficiencies and significant changes in internal controls reported to the committee by the independent auditor or management;
  - The company's internal audit procedures; and
  - The adequacy and effectiveness of the company's disclosures controls and procedures, and management reports thereon.
- Reviews annually with the CAE the scope of the internal audit program, and reviews annually the performance of both the internal audit group and the independent auditor in executing their plans and meeting their objectives.

The above are extracted from a lengthy list of Intel audit committee responsibilities. Another on that list is, “Reviews and discusses with management the company's major financial risk exposures and the steps management has taken to monitor and control such exposures.” This statement contains the only reference to *risk* in the entire audit committee charter, and the emphasis here is on financial risk and not overall enterprise risk. As of the time of this review, Intel does not have a separate, board-level risk committee.

Over time, we may expect to see much more emphasis on enterprise-level risks in corporate board audit committee charters and other supporting documentation. However, with the launch of COSO ERM and its emphasis on enterprise-wide risk, board-level risk management committees perhaps should be the ideal approach for a board to cover ERM issues rather than assigning them as an additional audit committee responsibility. This approach may serve to reduce the workload responsibilities of many board audit committees. Prior to SOx, a board seat on an audit committee was not a heavy time responsibility type of role. Although they also had a responsibility to supervise their internal audit functions and the CAE, pre-SOx audit committees were heavily weighted and tied to their external auditors. They provided regular updates of their audit activity progress, often made strong suggestions that the external audit firm engage in needed consulting activities, and managed many aspects of the financial audit process. SOx has really changed all of that, and corporate management and audit committee members now have a much more important role in managing and overseeing their audit and financial reporting processes. For many audit committees, what were once the often perfunctory-length meetings held each quarter before the regular board meetings have turned into once-a-month face-to-face sessions along with numerous telephone conferences during the interim. Audit committee members today are busy!

ESTABLISHING A BOARD-LEVEL RISK COMMITTEE

While boards are required to have audit, nominating, and compensation committees, other committees are established based on the overall business of the corporation and other issues. The risk committee is a relatively new committee for many corporate boards today. In past years, corporations involved with financial instruments, trading, or commodities sometimes established risk committees to monitor such matters as interest rate changes or trading gains and losses. Other corporations viewed many audit processes as the assessments of risks and renamed their audit committees to something like the audit and risk committee. However, these revised committee structures or nonconventional names did not necessarily change the practices of a board's management and assessment of risks.

With the growing attention given to many aspects of risk management at major corporations, many corporate boards have introduced chief risk officers (CROs), and especially with COSO ERM, a growing number of corporate boards are beginning to establish separate risk committees. These board-level committees directly supervise the activities of the CRO,

monitor risk issues at a very high level, coordinate closely with the audit committee, and communicate risk-related issues with the overall board. While senior management can establish an effective ERM function, as discussed in Chapter 5, and can create a CRO type or level of position, there is a need for high-level oversight of corporate ERM activities. A corporate risk committee can assess risk-related issues at this very high level; review and act on the risk assessment review (RAR) reports introduced in Chapter 5; and provide a message to stockholders, overall management, and others that the corporation is actively assessing and monitoring risks at a very high level.

Exhibit 8.2 is an example of a charter for a corporate board of directors' risk management committee, using the same Global Computer Products Corporation that has been used throughout these chapters. This document was based on several actual risk committee charters, but was modified to remove some of the legalese found in such actual documents. The charter clearly calls out the purpose of the committee, "to assist in overseeing, and receiving information regarding, the Corporation's policies, procedures, and practices relating to business, market, and operational risk." The sample charter calls for a risk management committee, with a separate committee chair, and with that committee reporting to the chairman of the board along with other key board committees such as audit. This charter outlines the responsibilities of a set of nonemployee directors, including:

Global Computer Products Corporation Board of Directors
CHARTER OF THE RISK COMMITTEE

I. Overview of Risk Management Governance.

The Board of Directors (the "Board") and management of **Global Computer Products Corporation** (the "Corporation") have established a corporate risk governance process that focuses on the major risks that are inherent to the Corporation, including emerging risks. Generally, these risks can be categorized in the following classifications—business strategy risk, reputation risk, liquidity risk, interest rate sensitivity risk, credit risk, market risk, and operational risk.

The Corporation has established various management committees to assess and manage the Corporation's exposure to the above risks. The Senior Risk Committee is the management committee responsible for monitoring the direction and trend of all major types of risks relative to business strategies and market conditions. It also reviews identified emerging risks to the Corporation and monitors activities to appropriately mitigate those risks.

EXHIBIT 8.2 BOARD RISK COMMITTEE CHARTER: GLOBAL COMPUTER PRODUCTS EXAMPLE

Global Computer Products Corporation Board of Directors
CHARTER OF THE RISK COMMITTEE

The Corporation's chief risk officer (CRO) reports to the chief executive officer (CEO) and is responsible for the oversight of the Corporation's risk-taking activities and risk governance processes. The CRO may appoint such other officers or establish such other management committees as may be necessary or advisable for the development, communication, implementation, and monitoring of the Corporation's risk management processes.

The Board, with the assistance of the Risk Committee and the Audit Committee, oversees the Corporation's corporate risk governance process.

II. Purpose of the Committee.

The Risk Committee (the "Committee") is appointed by the Board to assist in overseeing, and receiving information regarding, the Corporation's policies, procedures and practices relating to business, market, and operational risk.

III. Membership, and Operations of the Committee.

The Committee shall consist of a minimum of three (3) nonmanagement directors, appointed by the Board, based on the recommendations of the Board Corporate Governance and Nominating Committee and shall serve for such terms as the Board may determine and until their successors shall be duly qualified and appointed. The Board shall designate a chairperson for the Committee.

The Committee shall meet in conjunction with regularly scheduled Board meetings or as it otherwise deems necessary, and with respect to procedures as set forth in the Corporation's bylaws. The Committee may elect to meet from time to time in executive session with the CRO or any other member of management, as it deems appropriate.

IV. Duties, Responsibilities, and Authority of the Committee.

1. The Committee shall annually review and approve the Corporation's Risk Policy, and annually review those policies. In addition, the Committee may authorize management to develop and implement any additional detailed policies and procedures relating to risk management as may be consistent with these policies.
2. The Committee shall receive information from management, as appropriate, and shall discuss matters relating to risk-related activities, including the following:
   - Any material regulatory or rating agency issues.
   - Material emerging risks to the Corporation.
   - New or proposed products, services, or businesses that may expose the Corporation to new material types of risk or present material reputation risk.

EXHIBIT 8.2 BOARD RISK COMMITTEE CHARTER: GLOBAL COMPUTER PRODUCTS EXAMPLE *(CONTINUED)*

Global Computer Products Corporation Board of Directors
CHARTER OF THE RISK COMMITTEE

- Other significant matters relating to liquidity, credit, market, and operational risk.

3. The Committee shall receive information from the Asset and Liability Committee and management, as appropriate, and shall discuss matters including the following items:

- The capital and liquidity position of the Corporation.
- The sensitivity of the Corporation's earnings under varying interest rate scenarios.
- Trends in the economy in general and interest rates in particular, with a view toward their impact on the Corporation.
- Information relating to compliance with both external regulations and internal policies regarding asset, liability, and risk management.

4. The Committee shall receive information from management, as appropriate, and shall discuss matters, including the following:

- Risks relating to the Corporation's information technology activities, including the current operating environment and the strategic deployment of new technologies, and risks associated with the Corporation's technology infrastructure.
- The Corporation's compliance program, including the structure of the program and the assessment of risk regarding the Corporation's compliance with legal, regulatory, and ethical requirements.
- As appropriate, issues relating to business continuity planning, and risks relating to fiduciary, financial controls, human capital, implementation, legal, loss management, compliance, technology, and vendor management.

5. The Committee may also request other reports and information, as it may deem desirable from external or internal sources. In particular, in light of the responsibilities of the Board's Audit Committee with respect to risk assessment and compliance, the Committee and the Audit Committee shall each provide the other with information and reports regarding activities, as necessary and appropriate.

V. Reporting of Committee Activities to the Board of Directors; Delegation.

The Committee shall report its activities to the Board and, where appropriate, its recommendations for action by the Board at their next meeting subsequent to that of the Committee. Certain action by the Committee may be similarly reported to the Board for approval, ratification, and/or confirmation. The Committee may, in its discretion, delegate all or a portion of its duties and responsibilities to a subcommittee of the Committee. In addition, consistent with applicable law, regulations, and the Corporation's policies, the Committee may delegate certain of its authority to the CEO, or other appropriate members of management.

EXHIBIT 8.2 BOARD RISK COMMITTEE CHARTER: GLOBAL COMPUTER PRODUCTS EXAMPLE *(CONTINUED)*

Global Computer Products Corporation Board of Directors
CHARTER OF THE RISK COMMITTEE

VI. Review of Committee Charter and Committee Performance Evaluation.

The Committee shall review and reassess the adequacy of this Risk Management Charter at least annually. In addition, the Committee shall prepare and review with the Board an annual performance evaluation of the Committee.

VII. Committee Resources.

In order to carry out the duties conferred upon the Committee by this Charter, the Committee is authorized to select, retain, terminate, and approve the fees and other retention terms of special or independent counsel, or other professional advisors, as it deems appropriate, without seeking approval of management or the Board. The Corporation shall provide for appropriate funding, as determined by the Committee, for the payment of any such fees.

EXHIBIT 8.2 BOARD RISK COMMITTEE CHARTER: GLOBAL COMPUTER PRODUCTS EXAMPLE *(CONTINUED)*

- Reviews and approves the corporation's risk policy as well as other supporting risk management policies and procedures.
- Review and supervision of the activities of the CRO.
- Monitoring and reviewing appropriate risk management information received from management, including:
  - Any material regulatory or rating agency issues.
  - Material emerging risks to the corporation.
  - New or proposed products, services, or businesses that may expose the corporation to new material types of risk or present material reputation risk.
  - Risks relating to the corporation's information technology activities, including the current operating environment and the strategic deployment of new technologies, and technology infrastructure risks.
  - The corporation's compliance program, including the assessment of risk regarding legal, regulatory, and ethical requirements.
  - Risks related to business continuity planning, fiduciary, financial controls, human capital, implementation, legal, loss management, compliance, technology, and vendor management.

All of this says that members of the risk committee, as a component of the overall board, have a major responsibility in monitoring and managing a wide range of risks that may impact a corporation. Just as members of the

audit committee are expected to have a level of expertise on many financial regulatory accounting and reporting issues, the internal and external audit process, SOx regulations, and much more, the nonemployee directors serving on a corporate risk committee would be expected to have a wide range of at least general knowledge in many domain areas.

This charter outlines some high-level responsibilities for the directors responsible for the many risks facing the modern corporation.

While not an SEC-defined or -required board position at present, there are no formal or minimal requirements for a board risk committee position. The status of board audit committee positions, over the years before and after SOx, can provide some guidance regarding what a board should consider as it is establishing the director membership rules for a board risk committee. A first and very important requirement is that board risk committee members must be nonemployee directors. Just as directors of the audit committee must be nonemployees and independent from the financial functions that are being audited, a similar level of director independence is needed for assessments and decisions on when to properly review and accept some potentially risky activity.

In the years prior to SOx, there were no background or experience qualifications for audit committee members. They were expected to review and understand some often very complex financial and accounting issues, even though they may not have had the necessary experiences or qualifications. This matter really was highlighted during the hearings after the fall of Enron. Audit committee members there, often with impressive job titles, were asked to testify on why they passed judgment on what were sometimes very complex financial transactions. It turned out some did not understand or have the qualifications to understand. For readers here who have had some accounting training or experience, several of those Enron audit committee members did not even appear to understand the concept of an accounting accrual transaction—basic accounting and auditing language!

The finding that nonqualified audit committee members were part of the Enron board, and that they could not have really been monitoring things and understanding audit issues as they should, led to a requirement in the initial SOx rules requiring that at least one member of any corporate audit committee must be an accounting and auditing "expert." Those rules, first issued in a draft format, however, were so tight that many existing major corporation audit committee members would not have been qualified to remain in their positions. The rules were subsequently softened to make them more reasonable. However, at least one member of any corporate audit committee today must have a demonstrated level of skills or experiences to be able to review

and understand some of the financial and accounting internal control issues surrounding a public corporation today.

Just as at least one of the nonemployee director members of a corporate audit committee must have some specialized accounting and auditing experiences, today's board risk committee of nonemployee directors should have at least one director who has some demonstrated risk management qualifications. While there currently is no SEC requirement here, or even an accepted standard, Exhibit 8.3 outlines some of the skill requirements

---

Following the SEC rules requiring that at least one member of an Audit Committee must be a designated "Financial Expert" with designated and demonstrated attributes, it is our proposal that at lease one member of corporate board Risk Committee should be a risk management expert. While not an SEC requirement at this time, the requirements for at least one, non-employee director requirements for the Risk Management committee might be:

Attributes: The Risk Management Expert must have the following attributes:

- A good understanding of the COSO ERM model with an emphasis on techniques for risk identification, qualitative and quantitative risk assessment approaches, and risk monitoring.
- Experiencing in analyzing and developing appropriate response plans for a broad range of financial and operational risks in active organization environments, or experience in actively managing one or more persons engaged in risk management activities.
- An understanding of financial and general internal controls and procedures, with an emphasis on financial reporting requirements.
- A general understanding of information systems risks, including security and telecommunications.
- An understanding of Risk Committee functions and how they interrelate to the Audit Committee.

Qualification or Experiences to Obtain Risk Management Attributes: The Risk Management Expert must have acquired these Attributes through one or more of the following means:

- Education or experience as a principal risk management officer, key internal audit of financial executive, or in a consulting firm performing significant risk management activities.
- Experience in actively supervising one or more persons actively managing such risk management functions.
- Other relevant experience.

EXHIBIT 8.3 BOARD RISK COMMITTEE RISK MANAGEMENT KNOWLEDGE REQUIREMENTS

that might be expected of a risk committee board member who could claim a demonstrated knowledge of risk assessment and analysis skills.

The problem in identifying such risk management knowledge skills today is that there is no widely recognized risk management body of knowledge (i.e., a compendium of the minimum skills that a COSO ERM professional would be expected to have). An example of that concept can be found in the project management profession. For years, many professionals called themselves "project managers," even though in the eyes of many peers they really did not have many of the essential skills that might be expected of a project manager. The Project Management Institute, a professional organization, then worked with some true experts in the field to codify the essential requirements of project management skills into a publication called PMBOK (Project Management Book of Knowledge).[3] The standards outlined in their PMBOK have become the world-wide recognized standard for project management. PMBOK is briefly discussed in Chapter 10. Although a risk management codification or book of knowledge does not exist at the present time, it is very much a future possibility.

As the appreciation and understanding of COSO ERM grows and as more corporate boards establish risk management committees, we will almost certainly see the establishment of more risk committees on corporate boards and increased importance and stature of risk managers. The concept of board risk committees with qualified risk management professional members is not that far into the future.

AUDIT AND RISK COMMITTEE COORDINATION

The increased level of responsibility for, and attention given to audit committees today very much supports the concept of a board risk management committee, working in parallel with the audit committee. This split allows separate but independent board attention to be given to both audit committee matters and board risk management issues. Exhibit 8.4 shows how these two committees might operate in a board corporate governance framework. The risk committee and the audit committee would each operate as senior board committees, reporting directly to the full board of directors and its chair. Both board committees would directly supervise the work of the CFO, with the risk committee having additional responsibilities for the CRO. This exhibit shows the CRO reporting to the CFO, with the board risk committee managing the CRO through the CFO. The Exhibit 8.2 risk committee charter specified that the CRO would report directly to the risk committee and its chair. Either approach will work, but any board risk committee must have an

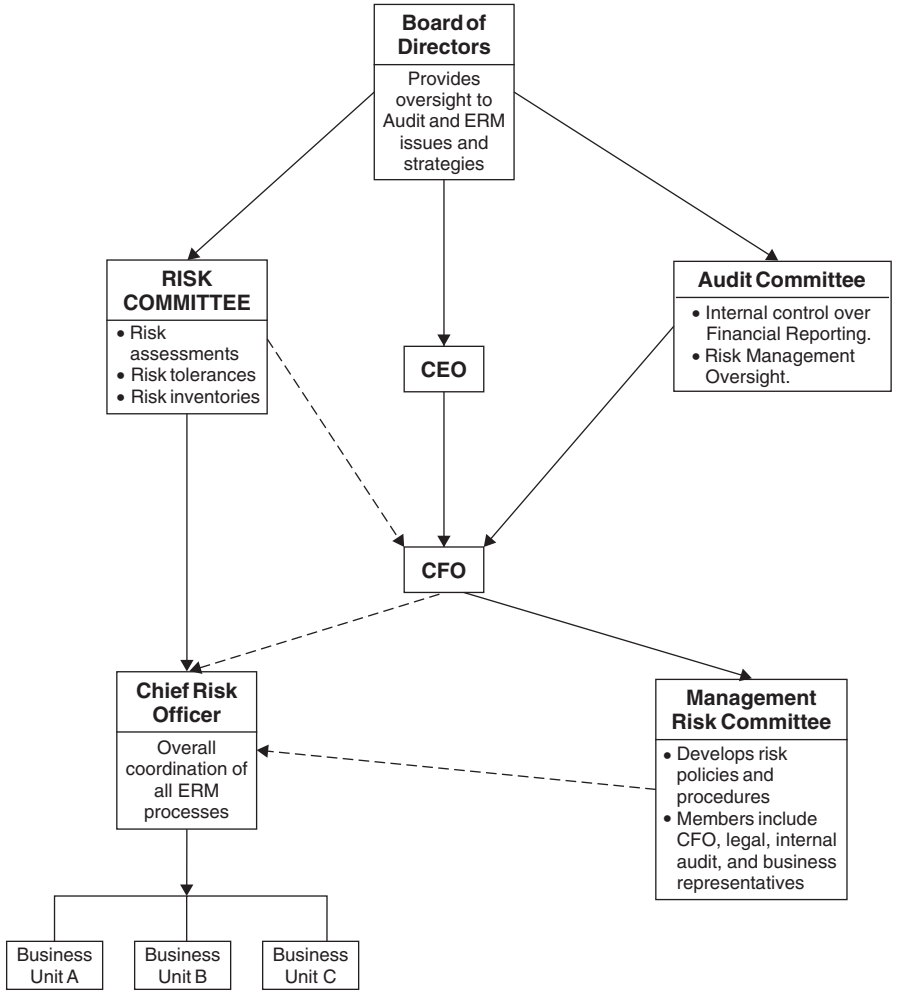

EXHIBIT 8.4 AUDIT COMMITTEE AND RISK COMMITTEE COORDINATION

active connection with its corporate CRO and the supporting risk management function.

This organization chart also describes the management risk committee, actually a subcommittee of the audit committee and the risk committee. With input from the CRO as well as members of the audit committee, the general counsel, and others, this is the type of policy formulation function to set general rules and guidance for the overall corporation. As Exhibit 8.4 shows, the risk committee would be responsible for managing the risk assessment and management functions at various operating units of a corporation.

COSO ERM AND CORPORATE GOVERNANCE

The concept of COSO ERM has not yet entered in the boardrooms of corporate management today, but we can expect that it will. In any event, whether it is through the audit committee or a separate risk committee, today's corporation should give more time and attention to assessing and managing its risks. The interested board member should become more acquainted with the concepts of COSO ERM and how it will help a board to better understand and manage enterprise-level risks. While not common today, we should soon see a wide number of corporate risk committees, with investors or others asking the board why they have not established such a risk committee at some future annual meeting. It is a soon-to-happen future development in corporate governance.

NOTES

1. Carolyn Kay Brancato, Ellen S. Hexter, Katharine Rose Newman, and Matteo Tonello, *The Role of U.S. Corporate Boards in Enterprise Risk Management.* The Conference Board, Report Number: R-1390-06-RR, June 2006.
2. Blue Ribbon Report on Risk Oversight, National Association of Corporate Directors, Washington, DC, 2002.
3. *A Guide to the Project Management Body of Knowledge,* Project Management Institute, Newtown Square, PA:, 2004.

9

Role of Internal Audit in ERM

Internal auditors represent the "eyes and ears" of management as specialists who visit all areas of an organization and report back to management on the status of the operations visited. They have historically had ongoing concerns and interests in risk management. In particular, internal auditors have regularly assessed the relative risks of areas to be examined when planning their upcoming audit activities, deciding which areas or functions within an organization to select for internal audits. With limited time and auditor resources, an internal audit function and its chief audit executive (CAE) would generally focus their time and attention on the riskier areas of the organization, deferring the other audit candidates for another time. We have used the term *audit* to refer to the multiple roles of internal auditors in providing reviews and assessments of internal controls as pure assessment audits and also providing service to management through consulting services. Risk assessment processes used for internal audit planning, however, were historically often informal and limited in scope. An internal audit function with the responsibility for reviews of multiple remote operations often would decide which of these remote offices to include in their

annual audit plan based only on some very informal risk measures. With only very limited knowledge, internal auditors often made quick, cursory decisions on whether some area should be considered high or low risk and then focused their audit planning on the assumed higher-risk areas. These risk assessment planning approaches were often based on only limited areas of the enterprise, with an emphasis on reviews at the unit's headquarters rather than over the entire enterprise. In some instances, enterprise management sometimes suggested an internal audit review of some area using the terminology of risk management to justify the review even though there may have been other reasons to schedule an audit in a given area.

Today's Committee of Sponsoring Organizations' enterprise risk management (COSO ERM) framework calls for a more formal and comprehensive approach to risk-based thinking and should encourage internal auditors to give much more attention to risk management when planning for and performing many of their reviews. The internal auditors' professional and standards setting organization, The Institute of Internal Auditors,[1] has been enthusiastically supportive of COSO ERM. Even when the COSO ERM framework[2] had just been released, internal audit guidance materials then suggested that "The modern internal auditor should be prepared to better understand risks under ERM as the years go by."[3] Providing that better understanding of COSO ERM, from an internal audit perspective, is a major objective of this chapter. We will consider how the multidimensional strategy-setting focus of COSO ERM can help both internal audit functions and individual internal auditors in their planning for new audit activities, whether internal controls review audits or consultative activities. We will also consider other risk-based approaches

to the overall internal audit process as well as internal audit's potential roles in helping to implement an effective risk management program for their organization.

INTERNAL AUDIT STANDARDS FOR EVALUATING RISK

With the wide range of reviews over many areas, and processes to be considered in any future internal audits, effective audit activity planning is a major responsibility of internal auditors at all levels. These range from the on-site auditor making sample item selections as part of a field-based operational audit to the CAE working to present a plan of audit activities for an upcoming year or period for presentation to the audit committee of the board of directors. Over the years, internal auditors have frequently asserted that their internal audit planning decisions were based on "risk" but often without a formal risk assessment approach or a good understanding of the various risks surrounding their organizations and how those risks should have impacted their audit planning. Despite this lack of a consistent approach about what had been meant by *risk,* many internal auditors have used this term over the years with only a general understanding of what it meant. It has often been easy for internal auditors to state that their audit work—particularly internal audit planning—focused on higher-risk areas of their organization without a good understanding of the concept.

The Institute of Internal Auditors (IIA)[4] is the prime worldwide professional organization for internal auditors, just as the American Institute of Certified Public Accountants (AICPA),[5] in the United States, is the professional organization for external auditors. The IIA maintains a set of periodically updated standards, the International Standards for the Professional Practice of Internal Auditing,[6] and all internal auditors that are members of the IIA are mandated to follow them.[7] While covering a wide range of internal audit activities, the standards contain multiple references to an internal auditor's responsibility to consider risk while planning and performing internal audits.

The standards state that internal auditors are expected to consider risk either when planning for a single audit or when developing an overall internal audit plan. Using the numbering scheme of these IIA standards, internal audit risk standards are covered in Section 2010, Planning, and Section 2110, Risk Management. IIA professional standards are further designated as either "A" sections, defining areas of internal audit normal activity, or "C," covering the frequent activities where internal auditors act

as consultants to their organizations. Key risk-related portions of the IIA standards follow, with specific references to risk highlighted:

> **2010 – Planning:** The chief audit executive should ***establish risk-based plans*** to determine the priorities of the internal audit activity, consistent with the organization's goals.
>
> > **2010.A1** - The internal audit activity's *plan of engagements should be based on a risk assessment*, undertaken at least annually. The input of senior management and the board should be considered in this process.
> >
> > **2010.C1** - The chief audit executive should consider accepting proposed consulting engagements based on the engagement's *potential to improve management of risks*, add value, and improve the organization's operations. Those engagements that have been accepted should be included in the plan.

To summarize this internal audit planning standard, the CAE is mandated to establish "risk-based plans" to determine internal audit planning priorities. The internal audit activity portion of this standard, designated as A1, goes on to say that audit planning should generally be based on an annual risk assessment. IIA standards also recognize that internal auditors often act as internal consultants to their organizations, and there is a separate set of internal audit consultant–related standards, designated as C1. This section of the standard talks about the "management of risks."

Another set of the IIA standards covering risk is found in a section on the nature of internal audit work, with a separate section on risk management:

> **2100 – Nature of Work.** The internal audit activity should ***evaluate and contribute to the improvement of risk management***, control, and governance processes using a systematic and disciplined approach.
>
> **2110 – Risk Management.** The internal audit activity should assist the organization by identifying and ***evaluating significant exposures to risk*** and contributing to the improvement of risk management and control systems.
>
> > **2110.A1** - The internal audit activity should monitor and evaluate the effectiveness of the **organization's risk management system**.
> >
> > **2110.A2** - The internal audit activity **should evaluate risk exposures** relating to the organization's governance, operations, and information systems regarding the
> >
> > - Reliability and integrity of financial and operational information.
> > - Effectiveness and efficiency of operations.
> > - Safeguarding of assets.
> > - Compliance with laws, regulations, and contracts.

> **2110.C1 -** During consulting engagements, internal auditors ***should address risk*** consistent with the engagement's objectives and be ***alert to the existence of other significant risks*.**
>
> **2110.C2** – Internal auditors ***should incorporate knowledge of risks*** gained from consulting engagements into the process of identifying and evaluating significant risk exposures of the organization.

While this is just one set of what are many sections taken from the entire set of the IIA standards covering a wide range of internal audit activities, risk management is or should be important to all internal auditors. While part of these are the overall standards, many internal auditors may not have given the attention to risk management in the past as would be anticipated from the standards. For example, 2110.A1 calls for internal auditors to monitor the effectiveness of the organization's risk management system. These IIA standards were issued well before the release of COSO ERM, and, as outlined in earlier chapters, many organizations did not have effective and consistent risk management systems prior to COSO ERM. This begs the question of how internal audit functions in the past had been able to evaluate the effectiveness of their organization's risk management systems when there was no consistent definition of risk management.

COSO ERM now provides an effective tool to allow internal auditors to better plan and understand risks in the course of their internal audit work. It is a standard outlining the key elements of an effective risk management system. This is a situation similar to the lack of a standard definition of internal controls prior to the release of the COSO internal controls framework, as has been discussed in earlier chapters. Prior to the release of the COSO internal control standards, there was no consistent definition of internal controls, and both auditors and management often talked about the "effectiveness of their internal controls" with no consistent measure of what was meant by that effectiveness. The earlier IIA standards did not have a specific section on risk management but discussed the "consideration of risk" as part of the standards for planning internal audits. That older and now superseded standard mentioned risk as part of audit planning in the then section 410.01.1.b, defining risk for internal auditors as follows:

> Audit objectives and procedures should address the risks associated with the activity under audit. The term "risk" is the probability that an event or action may adversely affect the activity under audit.

This now obsolete IIA standards section was supported by another set of steps for an individual audit risk assessment process. Our references here are only an example of an out-of-date set of IIA standards that have been renumbered and superseded with the current standards.

The 1990s-era IIA standards say a lot for how far the internal audit profession has moved in its acceptance and understanding of risk management. That older definition, stating that a risk was anything that could affect an audit activity, only indicated that if any processes or audit plans happened to go wrong during an internal audit, the failure could be called a "risk" or sort of a bump in the road, allowing the internal auditor to move on. Using those older terms, internal auditors often talked about "risk" without much understanding of what was meant by the expression. Prior to moving into internal audit management and to more senior levels of internal audit responsibility, this author served as a staff internal auditor early in his internal audit career and was often asked to consider "risk" in developing internal audit plans. At that time, there was not much understanding or guidance on what was meant by "risk," and "best guess" estimates were often used.

The current IIA standards go beyond calling risk just a probability, and they cover risk planning in a much better manner. However, they really still do not define what is meant by *risk*. For example, the current standards Section 2110, mentioned previously, states that internal audit "should assist the organization by identifying and evaluating significant exposures to risk and contributing to the improvement of risk management and control systems …." While the typical CAE can identify significant exposure risks in his or her organization, this is a judgment based on primarily personal and professional opinions. Internal auditors historically have not had strong standards-level guidance covering internal audit risks. This lack of using strong risk criteria by internal auditors is partially due to their expected "eyes and ears" roles. Management frequently has expected their internal auditors, for example, to visit a site to observe the taking of a physical inventory. They are independent outside representatives to observe and comment on that process. However, sometimes these physical inventory observations have been done in almost a rote manner with little concern over the internal controls aspects of those exercises. COSO ERM has changed things here and should promote better internal audit planning and performance at all levels.

COSO ERM FOR MORE EFFECTIVE INTERNAL AUDIT PLANNING

Internal audit standards call for the consideration of risk when selecting the appropriate auditable entities to review and audit. Many internal auditors in the past developed their own personal or audit department risk criteria for this audit planning process because there was no overall consistent professional definition of risk. As a past director of internal audit for a then major

U.S. corporation, this author recalls developing a risk criteria for audit selection and then using it for audit planning. This was entirely a "homegrown" process that sounded good, seemed to be effective, and was accepted by the audit committee, senior management, and external auditors. However, with no guidance or standards to follow, many internal audit functions often developed their own homegrown risk assessment processes. Beyond articles in professional magazines or discussions with peer internal audit directors and managers in other organizations, there was no means to determine if one selected approach to understanding and accepting risks was any better or worse than others. These annual internal audit plans are often based on audits in progress and requests by the audit committee and senior management but with only a limited understanding of audit risk. Internal auditors are often expected to observe the taking of physical inventories, as discussed, or serve as part of the team that performs a due-diligence review of a new acquisition. These are often roles in which there is little risk involved in the process. An example would be a plant that does an annual physical inventory and then reconciles those count results to the booked inventory. For some organizations, this may be a low-risk process where detailed instructions are issued to the count teams, there is ongoing management involvement in the process, and few count-related inventory problems are encountered. This probably would be a low risk type of exercise. Conversely, there may be a high likelihood of problems at a smaller plant with a high level of problem or failure significance. Nevertheless, management often expects internal audit representatives to be present at both inventories, making no allowances for relative risks.

Just as external auditors perform certain financial audit processes that are essentially low risk and "never" will cause problems, internal auditors are often expected to become involved in some other fairly low-risk types of activities. This is an important internal audit activity wherein management wants an independent observer to report on any problems. Although the probability of a fire in a facility may be very low, we still hang fire extinguishers on building walls. Internal audit often plays that kind of protective role, and the risk-related significance of these tasks should always be considered. Internal audit planning should include both these regular, protective types of audits as well as other reviews covering all auditable entities in their organizations.

Internal audit's annual planning exercise for an enterprise is often based on what is called the "audit universe," the total of all auditable entities or units in an organization—every business unit and function or operation within those units. This would include both the protective types of scheduled

reviews, such as physical inventory observations or external auditor assistance, and various types of operational and financial reviews with the total organization. These "audit universe" lists of auditable entities, however, often have not appropriately considered relative risks. Internal audit functions then have often used the lists of auditable entities, but with no risk rankings, to show the audit committee and management all of the areas where they could perform internal audits if they had enough resources and time.

"Audit universe" lists provide a repository of all auditable entities in an organization—large and small as well as close to home or distant—but usually do not provide a risk-based approach to developing those audit plans. This laundry-list approach to looking at all of the areas that could be included as potential internal audit candidates gave internal auditors an impressive list of the work that could be done but did not really help that much in the selection of appropriate areas or units to schedule for audits. As a result, the emphasis on internal audit planning has often been on audits at larger and more familiar business units closer to home. These internal audit plans are sometimes based somewhat on risk but do not give adequate attention to ERM considerations.

While there is no requirement for an internal audit organization to follow COSO ERM when developing an internal audit plan, that framework provides an excellent starting point for assessing risks and developing internal audit plans. It provides a consistent basis for internal audit functions today to develop a risk-based audit-planning approach strategy that should provide audits of all major areas of risk over time—an excellent first objective for developing internal audit plans.

Using COSO ERM to Build an Annual Audit Plan

Just as almost all financial functions develop an annual budget, internal audit functions prepare an annual audit plan to inform their audit committee and senior management of their planned upcoming internal audit activities. Prior to the Sarbanes-Oxley Act (SOx), when internal audit's reporting relationships to their audit committees were sometimes not that strong, other members of senior management often took a strong role in setting priorities, identifying risks, and developing an overall strategy for developing these internal audit plans. In those pre-SOx days, the CAE often had limited ongoing contact with the audit committee beyond quarterly board and audit committee meetings. Audit plans were developed based on the current experiences of the internal audit team or through guidance from the CFO or

some other senior officer. While risk assessment was considered part of this audit planning, this risk analysis process was often very subjective. Potential areas to audit were often just risk-ranked as high, medium, or low with little analysis beyond that. Although IIA standards called for the consideration of risk when developing audit plans, internal audit risk assessments were often not all that formal, and many internal audit planning decisions were heavily dependent on just the strategy and preferences of senior management.

Those pre-2002 days, prior to SOx, were also a period when internal audit outsourcing was becoming increasingly common. An organization's external auditors often would encourage the audit committee and senior management to give them overall responsibility for an internal audit function, arguing that internal audit would be better planned and managed with their guidance. This approach provided some improvements in internal audit practices and many of the then external audit firms probably had better audit-planning risk assessment processes than did many internal auditors at that time. However, the activities and plans of these outsourced internal auditors did not always consider the risks and objectives of the overall organization but tended to be much more aligned with the goals and often billing revenue objectives of their external auditors. As an example, the once major public accounting firm, Arthur Andersen, advertised how the outsourced internal auditors at their client, Enron, worked together as a team—internal and external auditors.[8] The separate and independent activities were somewhat lost. Looking at things after the fact, there certainly seemed to have been some high-risk areas at Enron that were not part of internal audit's scope. Some of the off-balance-sheet accounting issues that caused Enron to topple might have been discussed with a more independent internal audit function.

SOx has now prohibited external audit firms from taking responsibility for their audit clients' internal audit functions through outsourcing. While external providers—often other external audit firms that do not have financial audit responsibility—may manage internal audit through outsourcing, many CAEs today are often direct employees responsible for all aspects of internal audit, including risk-based internal audit planning.

Over the years, internal audit functions have often used the previously introduced "audit universe" concept of the total number of auditable entities in the organization to provide a basis for their internal audit planning. As discussed, the idea was to list all auditable entities in the organization—the audit universe—and to develop a plan that would allow for audits at each of these units over current and future periods. Although a very common approach for many internal audit functions today, this audit universe

list gave little consideration to risk; some units would be scheduled for annual internal audits even though past audit findings were minimal and risks low. In addition, many of the audits to be scheduled during an upcoming period were often based more on internal audit staff availability or other factors than because they were part of the total universe list that needed to be covered. Internal audit standards called for those annual audit plans to be based on risk considerations, but those earlier risk assessments often were fairly informal and subjective.

For many internal audit departments, this audit universe concept broke down because of a lack of audit resources to cover these long lists of auditable entities in any reasonable manner. While these audit universe lists often covered every area that could potentially be audited, the audit committee and management had little interest in auditing "every" organization entity. Some were just too small or otherwise not significant. Internal audit typically faces several problems in using the audit universe concept as the basis for risk-based internal audit planning:

- *Too many and too diverse auditable units in an organization.* An organization, such as our Global Computer Products example company that was first introduced in Chapter 3, has distribution centers, company-owned and -licensed manufacturing, and sales and distribution units scattered across the world. It is difficult to develop an audit plan with such a long and diverse list of auditable entities. This is even more difficult with a typical multinational, multidivision, and multibusiness organization.
- *Some units in the universe may not be easily auditable.* Organizations typically have units whose functions do not fit with an internal audit group's normal area of expertise. Often, these are areas such as product development laboratories or marketing research where internal audit does not have a sufficient level of specialized technical understanding to audit those units. Outside resources could be contracted to perform the reviews, but risks often did not appear to be sufficient.
- *Internal audit often does not have sufficient time or resources to cover all of their auditable entities.* There is little value in creating a huge to-do list of areas to audit if internal audit will never get to perform audits of many of them.

SOx and COSO ERM have changed all of this for developing and planning individual internal audits today. There is now a need to better consider

an organization's overall ERM environment as well as specific known audit risks and protective audit requirements when developing an annual internal audit plan. Easy to say here, but with COSO ERM still relatively new, many organizations today may not have not yet developed a formal ERM framework. Such a framework could have been developed by the organization's ERM group, as discussed in Chapter 5, by financial management or other units. However, for many organizations, an effective internal audit function will often be a catalyst in launching ERM. This is a key area for internal audit's business advisor or potential consulting role in an organization.

Internal audit does have a gatekeeper, protective role in determining that key internal controls are in place that takes it a little beyond just a pure risk-based internal audit decisions. There are many areas in organizational operations where internal audit's presence is needed, even though the review area has never been a problem. The plant physical inventory observation, discussed previously, is an example. In a large, multiplant organization, that observation may be necessary at some locations because of the large number of physical assets, even if past inventories have been clean with no expected problems. Similarly, the message that "the auditors are coming" may cause an organization to tighten things up in advance of any level of internal audit review.

Chapter 2 suggested that risks should be evaluated against two factors, the relative likelihood of the risks occurring and the significance of that risk to the enterprise. As an easy means of evaluating these risks, that chapter suggested using either numerical 1-to-9 ratings for each identified risk or a percentage decimal value. This same concept can be used to rank the audit universe list of auditable entities. However, each item on the list should be carefully defined into an internal audit activity that fits within the scope of internal audit's operations. That is, the listing should not just list the "Scarsdale plant" as an auditable item but should list the specific type or nature of any planned audit for that plant as a potential audit activity. This list should be broken down to enough detail to cover a series of specialized audit activities. That Scarsdale plant designation can be broken down to Scarsdale plant operations, plant finance and accounting, and plant information technology (IT) systems. These audit activities can be divided in greater detail as well. Scarsdale plant finance and accounting could become plant activity-based accounting, accounts payable, and other such specific audit activities. The idea is to break down this list of potential auditable entities into sufficient detail to define the specific audit areas to be performed.

We suggest using three different and linked scoring measures for each entity. As a major scoring for each auditable entity, assign an audit requirements score of either 0 or 1 following the guidelines:

> *Audit Requirement = 1.* This is for areas where internal audit knows that it will be performing an audit. Often, this is a senior management– or external audit–mandated request. No matter the level of risk, internal audit will be effectively required to schedule a review over this auditable entity.
>
> *Audit Requirement = 0.* This says the internal audit does *not* have a requirement to perform a review during the current period.

The audit requirement sets the rule of whether an entity should be reviewed by internal audit during a period. While an organization's external auditors or, more importantly, the audit committee should have risks in mind when they request that internal audit review some area, their risk evaluation criteria may be different than the measures used by internal audit. For example, there may be some overseas unit that internal audit does not plan to review because of a perception of a relatively low risk. However, the board of directors may be considering an acquisition near that overseas entity and is interested in an internal audit to get an up-to-date assessment of internal controls there. Such a request would rate an audit requirement score of 1.

For most enterprises and internal audit functions, these requested audits will be the exceptions. The audit committee and management will usually expect internal audit to develop their own risk-based internal audit plans. This leads to two other suggested risk-ranking factors or scores. Following the guidelines that were outlined in Exhibit 2.5, all other auditable entities should be rated according to the factors:

- *Internal control significance of the auditable entity.* Each item should receive a rating of between 0.01 and 0.99. The lower end of this range says that the auditable entity has essentially minimal internal control significance, from an internal audit perspective. While it is always easy to find some level of internal audit interest in almost any auditable entity, there will always be areas where internal audit sees little concern from their perspective. An example might be a review of document management internal controls in the corporate legal department. While there is a need there for strong document management controls, the corporate legal department should have its own professional internal control responsibilities, and internal audit would probably not need to get involved in any direct reviews of

such areas. The internal control significance ranking score here would be low.

Areas with significant internal control risks, such as IT applications security, general ledger balancing procedures, or the annual physical inventory, would receive relatively higher scores. As part of its audit-planning process, internal audit should take each auditable entity and rank or score it.

- *Likelihood of significant internal control weaknesses.* Each item again should receive a rating of between 0.01 and 0.99. This rating would be a relative ranking based on internal audit's assessment of the possible number of internal control failures in the area, following this approach:
  - Significant weaknesses from past internal audits would receive a higher score.
  - Lower scores would be assigned to areas with limited internal control exposures. For example, office materials inventories in a shipping department might receive a lower score.

This is again a relative ranking type of scoring. Internal audit should consider each of its auditable entities and assign an appropriate score or rating.

We now have three factors to help build a risk-ranking internal audit plan: (1) audit requirements, (2) internal control significance of the auditable entity, and (3) the likelihood of significant internal control weaknesses. These will provide support for building a risk-ranked internal audit plan. There are no IIA standards calling for this exact approach, but this should serve as an effective risk-scoring mechanism to help internal audit functions to build audit plans.

A simple example will help describe this process. Assume that a small internal audit function has two plants in its audit universe, XYZ and ABC. In addition, it has decided to identify three auditable entities at each—finance and accounting, IT operations, and plant operations—providing a total of six auditable entities over the two plants. For ABC finance and accounting operations, internal audit might review past audit records and decide that there were significant internal control weaknesses identified in the prior year's audit with limited assurances that they have been identified. This might result in a likelihood rating of 0.80. If ABC is not a significant operation in terms of other plants, it potentially would receive a score of 0.50. The relative score for ABC finance and accounting would be $(0.80) \times (0.50) = 0.40$. If there were no audit requirement score of 1 to review this

area, the 0.40 score would be used to rank this area with others. Of course, an audit requirement of 1 says that internal audit is mandated by management to review a given area, no matter what the likelihood or significance. This risk-ranking process is described in greater detail in the case study example that follows.

Risk Tolerance and Building Internal Audit Plans

Using the auditable entity risk assessment approach discussed in the previous section, internal audit and its CAE should next build and develop an annual audit plan for their organization based on both the COSO ERM risk-based framework and internal audit's responsibility to management to be the "eyes and ears" for reviewing all activities. This latter requirement says that an effective internal audit function also must at least consider planning reviews of all areas in an organization, even some lower-risk areas.

In the prior section, we suggested that internal audit should first identify all of its auditable entities and then determine relative significances and probabilities. This is a classification that may be subject to change as internal audit reviews and better understands the functions and practices of its various operating units. For example, we have suggested that rather than just listing Plant XYZ as an auditable entity, internal audit may want to think of XYZ in terms of separate financial, operational, and information systems reviews, each with their own internal control significance and likelihood ratings. Based on additional analysis and understandings of these operations, internal audit may want to divide the number of auditable entities even further. For example, it may list database management and information systems security as separate auditable entities for XYZ's information systems operations. There would possibly be three entries or potential audit candidates here for IT operations, database, security, and another for internal controls covering all other aspects of IT operations at the facility.

That internal audit plan should be based on the following general concepts:

- Understand the risk universe surrounding the organization, including the number of auditable entities in the organization and their estimated risk-related levels of significance and probability. It is not enough to just list that there is a manufacturing plant in city A and a distribution center in city B. Through questions and discussions, internal audit should attempt to determine the functions and scope of these various business units.

- Identify any auditable entities that will be required audits. Even if an area has been designated as relatively low in risk, if the audit committee or senior management strongly request the review, internal audit should make best efforts to schedule the review. The significance and likelihood ratings should be retained only for documentation purposes.
- Develop audit programs or approaches for performing various types of audits surrounding these potential audit universe candidates. There is little value including the organization's advertising research unit in the list of potential audit candidates if the organization has limited understanding of its operations and no approaches to auditing the unit.[9]
- Based on the mixture of required auditable entities and their risk-ranked units, develop a general audit plan for all areas in the organization. This should be discussed with senior management and others, including the chief risk officer (CRO), to outline the overall approach. Since planning is done on an annual basis covering what is usually a consistent activity, this general approach should reflect on audits in process.
- Develop time and duration estimates of the internal audit resource requirements to perform internal audits for these various auditable audit candidates. This analysis will depend on the skills and experiences of the internal audit function. For example, a review of an IT data warehouse operation may require a limited number of very technical internal auditors over an extended time duration but with limited hours in each visit, while a review of regional sales office internal controls could require only a team of more junior auditors to review all of the units over a limited time period.
- Based on current internal audit capacities and capabilities, develop a series of alternative internal audit plans to cover these audit universe auditable entities. Internal audit may not be able to cover some items in the audit universe list because they do not have enough audit resources or are lacking some tools to complete the work in the time period. Alternative audit plans should be developed to cover the current one-year period as well as the following period:
    - A plan to review as much as can be accomplished of the riskier items in the audit universe list, given current people and budget constraints.

  - A series of "How much will it take?" alternative plans to perform internal audits of riskier identified audit areas. This approach will be discussed in the following section.
- Review audit plan alternatives with the audit committee and senior management and obtain approval. Where necessary, begin to add resources or otherwise begin to execute internal audit plan.

The idea here is that internal audit groups should go beyond the "audit everything" internal audit universe approaches often used in the past and focus internal audit activities on the riskier areas in the organization. In addition, that risk-based approach should be based on an assessment of risks covering the overall organization, following the COSO ERM model. The sections that follow discuss these approaches along with an example following the Global Computer Products company.

Risk-Based Audit Plan: Global Computer Products Example

Our example company, Global Computer Products, was first introduced in Chapter 3, with a high-level description of this company found in Exhibit 3.5 and a list of significant risks described in Exhibit 3.6. While this list does not cover all of the risks facing the example company, this could become a basis for building a list of potential auditable entities as a basis for building an internal audit plan. However, many of the risks listed here cover areas where internal audit reviews will have little impact. For example, the second risk listed under organization strategic risks in Exhibit 3.6 is a currency valuation crisis involving one or another international operation. Such a risk goes well beyond the enterprise and certainly internal audit's controls. In this case, internal audit can plan a review to determine if there are appropriate hedging and other control procedures in place to cover such risks, but it certainly cannot do much about the actions of an often irresponsible government that may devalue its currency.

Given that there will be some areas out of its control, internal audit can use this high-level set of organization risks to build its own annual, risk-based internal audit plan. It can consider taking identified enterprise risks and use a selected set of them to build its own internal audit annual plan. For example, Exhibit 3.6 listed seven company operations risks:

1. A computer systems or network failure at one or several locations
2. The unexpected resignation of a key management or technical senior manager

3. Labor unrest or related problems at one or another facility
4. The failure to complete several key information systems planned upgrades
5. Product licensing disputes and resulting litigation
6. The failure of an audit based on International Organization for Standardization (ISO) procedures or some other standards audit
7. A loss in stock market capitalization value due to reported operating losses

Of these risks, internal audit can do little with risk 7. While good internal control procedures will hopefully keep the stock high, the forces in overall declining markets are certainly beyond the control of Global Computer Products and its internal auditors. However, assuming that the remaining six are the significant company operational risk areas for Global Computer Products, internal audit can construct an internal audit plan covering those six areas within their scope and capabilities.

Identify Auditable Entities within Internal Audit's Scope and Capabilities. We have started with a set of identified risks in an area of responsibility at the example company, Global Computer Products. These risks may have been established by the ERM function, as discussed in Chapter 5, by members of management and the audit committee, or by internal audit itself as part of an earlier review exercise. In order to build a plan of audit action items, there is almost always a need to reassess that list of auditable entities to determine which are within internal audit's scope and review capabilities. We have already identified one risk, number 7 in the preceding list, which was not an auditable entity in itself. Internal audit should go through this type of list and make similar audit scope corrections and adjustments as may be required.

Based on past internal audit activities, the nature of business operations, and a general understanding of risks and operations, internal audit should build a list of all potential auditable entities within the enterprise. This will be an expanded but more risk assessment-based version of the previously discussed audit universe lists to cover areas that might be subject to internal audits. Such compilations can grow into extensive lists of areas to be considered for individual internal audits. For example, Exhibit 9.1 lists a selection of the auditable entities that might be part of the sample company Global Computer Product' San Jose development facility, as described in

Control #	Entity Description	Required	Prev. Audit	Findings
San Jose Finance and Accounting Auditable Entities				
SJ FN 1	Accounts Receivable and Billing	Yes	Yes	Significant
SJ FN 2	Purchasing and Accounts Payable		Yes	Minimal
SJ FN 3	Financial Reporting	Yes	Yes	Minimal
SJ FN 4	Intracompany Transactions			
San Jose Operations Auditable Entities				
SJ OP 1	Shop Floor Scheduling			
SJ OP 2	Quality Assurance Procedures			
SJ OP 3	Packaging and Shipping			
SJ OP 4	Receiving and Inventory Controls	Yes	Yes	Significant
SJ OP 5	Order Processing		Yes	Minimal
San Jose Information Technology Auditable Entities				
SJ IT 1	IT Continuity Planning	Yes		
SJ IT 2	Applications Dev. SDLC Procedures		Yes	Significant
SJ IT 3	Service Support Help Desk Operations			
SJ IT 4	Service Delivery Operations Scheduling			

EXHIBIT 9.1 GLOBAL COMPUTER PRODUCTS' SAN JOSE DEVELOPMENT AUDITABLE ENTITIES

Exhibit 3.5. In addition to just listing the area, the exhibit lists whether the entity has been a requested audit area or was previously audited in a recent period and, if so, the significance of any weaknesses identified in the unit.

Redefine and Rank Risks. A list of auditable entities for this type of example organization could be lengthy and certainly would include many other audit areas beyond those shown in Exhibit 9.1. In this brief example, 13 auditable entities have been identified, internal audits of 4 were requested by the audit committee, and internal audit has previously completed reviews

in 6 of these total areas. The basic idea is that internal audit should identify specific areas where they might be able to schedule reviews. For this example covering San Jose operations, the types of internal audits to be performed are fairly detailed. In a larger company or one with a larger internal audit function, these auditable entities could become even more finite. For a smaller or more remote unit, such as the auditable entities for Global Computer Product's Bangalore, India, software distribution facility, the entire unit might be covered by one or two comprehensive internal audits covering all internal controls and operations. Depending on the size of the enterprise, internal audit should develop and refine this type of an appropriate list of auditable entities. If the list is too finite or detailed, they will never be able to effectively complete and deliver all of those internal audits. In the other extreme, a too general or too high-level approach might result in lengthy internal audits requiring considerable audit staff attention or internal audits that may miss key internal control areas.

Once internal audit has identified its auditable entities in the Global Computer Products example company, the next step is to estimate entity internal controls and their significances, as were discussed in the previous section. Using an arbitrary two-decimal-point measure, each entity should be rated on the internal control significance of the entity and on the likelihood of an internal control weakness. For example, the entity labeled as SJ IT 2, shown on Exhibit 9.1, covered SDLC application development procedures. Because other factors should be in place to detect internal control problems, the entity might be assigned an internal control significance score of only 0.30. However, because this area was subject to an internal audit in a previous period and significant internal control problems were found, the likelihood of an internal control weakness score might be assigned a 0.85. We have assumed here that internal audit has taken no steps to see if the weaknesses were corrected. Rounded to two decimals, the example entity would receive a preliminary score of $(0.30) \times (0.85) = 0.26$.

The internal audit team should go through each of the identified auditable entities and assign preliminary scores. We have used the term *preliminary* since some of these entity audits would have been requested by the audit committee or external auditors, and the requested audit requirement score of 1 is added to each of the preliminary scores to provide an audit rank score. Using just some arbitrary values from the Exhibit 9.1 audit entities, these scores are shown in Exhibit 9.2, along with a score to show the relative high-to-low score rank of each. This process allows internal audit to look at all of the potential auditable entities and decide which to include in their internal audits over the upcoming period.

Control #	Entity Description	Audit Requirement	I/C Significance	Weakness Likelihood	Prelim Score	Audit Score	Rank
San Jose Finance and Accounting Auditable Entities							
SJ FN 1	Accounts Receivable and Billing	1	0.90	0.90	0.81	1.81	1
SJ FN 2	Purchasing and Accounts Payable	0	0.65	0.60	0.39	0.39	9
SJ FN 3	Financial Reporting	1	0.95	0.60	0.57	1.57	3
SJ FN 4	Intracompany Transactions	0	0.85	0.65	0.55	0.55	7
San Jose Operations Auditable Entities							
SJ OP 1	Shop Floor Scheduling	0	0.65	0.72	0.47	0.47	8
SJ OP 2	Quality Assurance Procedures	0	0.25	0.55	0.14	0.14	12
SJ OP 3	Packaging and Shipping	0	0.80	0.90	0.72	0.72	5
SJ OP 4	Receiving and Inventory Controls	1	0.85	0.60	0.51	1.51	4
SJ OP 5	Order Processing	0	0.66	0.85	0.56	0.56	6
San Jose Information Technology Auditable Entities							
SJ IT 1	IT Continuity Planning	1	0.95	0.80	0.76	1.76	2
SJ IT 2	Applications Development SDLC Procedures	0	0.30	0.85	0.26	0.26	10
SJ IT 3	Service Support Help Desk Operations	0	0.40	0.45	0.18	0.18	11
SJ IT 4	Service Delivery Operations Scheduling	0	0.35	0.35	0.12	0.12	13

EXHIBIT 9.2 GLOBAL COMPUTER PRODUCTS RISK-RANKED AUDIT ENTITIES

Building an Internal Audit Plan. The preceding set of risk-ranked auditable entities provides an outline of the areas to review for an annual internal audit plan. Of course, building an effective plan is not quite this easy! We identified the higher-risk audits among the auditable entities, and a good next step is to reaffirm—and modify, if required—the estimated values and factors. The goal of this chapter is not to describe how to build effective internal audit plans but how to build risk-based plans.[10] However, the different approach here is that we are building the internal audit plan with an emphasis on performing audits in riskier areas of the enterprise.

For our example, Global Computer Products' San Jose operations, we have risk-ranked 13 potential audits, with 4 of these requested or required. Since the San Jose operation is only one component of the larger, multiunit Global Computer Products example company, these audit candidates should be merged with the risk-ranked auditable entities from other units of the organization. Since other units of the enterprise will include areas for potential suggested audits with other levels of risk, internal audit will need to look at its own staffing and capabilities to schedule planned audits among other higher-risk and other requested areas. This is always a major juggling effort by an internal audit function, but this risk-ranking process will allow them to better prioritize and schedule these internal audit reviews.

The audit requirement score factor of 1 can very much influence the other audit review scores. Even if internal audit has rated some internal audit candidate area with an internal control significance and a likelihood of 0.95, giving this example a total preliminary score of 0.90, an audit request of 1.00 would raise the rank even higher than some otherwise lower-risk audit candidates. The reality here is that if the external auditors or the audit committee requests an internal audit in some area, the CAE should comply with those requests. This risk-ranking audit planning approach gives an internal audit function the ability to plan and schedule higher-risk audits rather than just performing some reviews because internal audit has "always" reviewed that area.

We have looked at an internal audit plan for one year at a business unit. For most organizations and types of audits, internal audits are a continuous process crossing annual boundaries. In other instances, they will not be annual reviews but scheduled over multiple-year intervals. This means that the list of auditable entities will change from year to year, and internal audit should review and update this group of audit candidates before risk ranking and building the annual internal audit plan.

Execute Plan and Monitor Performance. With the auditable entities risk scored and selected for review, internal audit should go through their normal processes of planning and scheduling their internal audits. This is the normal internal audit process where audit programs or approaches should be developed, the audit entity reviewed and tested, and any findings and recommendations communicated through an internal audit report. The nature of those audit findings should better reflect risks, as discussed in the paragraphs following, but the overall internal audit process will not directly change because of COSO ERM. The planning of the audit, however, should be more sensitive to the risks encountered.

We have suggested that internal control significance and weakness likelihood scores should be evaluated as part of reviewing and auditable entities to constrict an annual audit plan. This exercise does not have to be totally reworked for every period, and estimates generally can be used period by period going forward. However, these estimates should be evaluated continuously with adjustments made as required. These may include the following factors:

- *The mix of auditable entities may have changed.* While there are some strong reasons for keeping adjustments to a minimum, enterprise reorganizations as well as too general or detailed audit requirements may cause changes. The team responsible for planning and scheduling internal audits should monitor developments and make changes to the internal audit auditable entity files as required.
- *Audit requirement request changes.* While external auditors may request that internal audit review some regular areas—such as a physical inventory observation at a major plant—the CAE and members of the internal audit team should question this when appropriate. While auditing standards call for certain types of periodic reviews, this is a responsibility that can be shared.
- *Risk rankings may require changes.* The range of 0.00 to 0.99 scores assigned for risks may require revisions due to internal audit's increased understanding of these estimates. For example, the results of a scheduled audit may reveal that an estimate was just wrong. Changes should be made to make future internal audits more responsive to the risk environments in the organization.

A risk-based model of auditable entities should provide an effective approach for internal audit planning. It will limit the number excessive or

insignificant audits planned today in some internal audit functions and should result in a more effective internal audit function.

RISK-BASED INTERNAL AUDIT FINDINGS AND RECOMMENDATIONS

An internal audit report, with its formal findings and recommendations, is the major output product from an internal audit function. Internal auditors will review internal control procedures, based on IIA standards, audit department procedures, and the individual auditor's own knowledge, and then will comment on the status of these controls through a formal audit report with its recommendations for corrective actions. Unless internal audit has some very strong quality assurance processes in place, those audit report findings and recommendations can sometimes cause problems for the people who were audited. It is sometimes difficult or impractical to implement the auditor's recommendations because the overall process was not fully considered in the audit report. Just as this chapter has suggested that internal auditors should consider risk when planning internal audits, those same risk considerations should be considered when drafting internal audit reports.

The point here is that internal audit report recommendations should give some consideration to the risks associated with recommended corrective actions when issuing internal audit reports. All too often, internal audit report recommendations sometimes suggest an ideal solution that is difficult, if not impossible to meet. For example, internal audit may have reviewed the purchasing operation in an area and found that many of its related processes were not documented. This could easily result in an internal audit report recommendation stating that "all purchasing department processes" should be documented. What did the author of that audit report mean by "all"? Auditee departments often take these types of words literally and initially embark on a program to document everything. However, if they start on the more minor processes, they may never get to the more complex and significant processes. The result may be only limited compliance with internal audit's recommendations but too much needless time and effort expended by auditees.

Just as internal auditors should think about the significance of internal controls in an area as they plan their reviews, they should consider the risk environment as they make their audit report recommendations. They should avoid the "document all processes" types of recommendations and focus on the areas of higher risk to be reviewed. This approach of going

after higher-risk areas first is consistent with current SOx review guidance, as was discussed in Chapter 7.

COSO ERM AND INTERNAL AUDIT

As a member of COSO, the IIA has been an early adopter of COSO ERM. Introductory and background material on this framework has been available to internal auditors almost since its initial release. The effective use of ERM should be an important element of internal audit's work. This chapter has suggested an approach to using ERM for overall audit department planning and to consider it when making audit report recommendations. These approaches should help an internal audit function to plan and perform more effective internal audits.

In addition to this internal audit planning and performing role, all internal auditors should develop a good understanding of the COSO ERM framework and use it where appropriate throughout their internal audit activities. We have used the example of internal audit as the "eyes and ears" to review and monitor enterprise activities. When an organization embraces a new initiative, such as COSO ERM, not all units will embrace things with the same intensity as others. For some it will be due to a lack of education or communication, while for others it will be the often natural resistance to change. An internal auditor who understands COSO ERM should be able to discuss and describe ERM risk-based audit planning to others and then help them in its appropriate application. Of course, when an internal auditor encounters resistance to new COSO ERM principles, the matter should be discussed in audit reports or raised to the audit committee when appropriate.

NOTES

1. The Institute of Internal Auditors, Altamonte Springs, FL, www.tiia.org.
2. COSO, *Enterprise Risk Management—Integrated Framework.* New York, Committee of Sponsoring Organizations, 2004.
3. Robert Moeller, *Brink's Modern Internal Auditing,* 6th ed. Hoboken, NJ: John Wiley & Sons, 2005, p. 122.
4. The Institute of Internal Auditors, Altamonte Springs, FL, www.tiia.org.
5. American Institute of Certified Public Accountants, New York, NY, www.aicpa.org.
6. *International Standards for the Professional Practice of Internal Auditing,* Altamonte Springs, FL: Institute of Internal Auditors.

7. The standards can be found at the IIA Web site (www.theiia.org) and are summarized in Robert Moeller, *Brink's Modern Internal Auditing,* 6th ed.
8. Deborah L. Lindberg and Frank D. Beck. "Before and After Enron: CPAs' Views on Auditor Independence", *The CPA Journal Online,* November 2004, www.ruesges.com.
9. For more information on building audit programs and approaches to auditing different business units, see Robert Moeller, *Brink's Modern Internal Auditing,* 6th ed.
10. For more information, see Robert Moeller, *Brink's Modern Internal Auditing,* 6th ed.

The Institute of Internal Auditors, Altamonate Springs, FL

10

UNDERSTANDING PROJECT MANAGEMENT RISKS

We often think of decision-making processes in terms of the lines of authority and responsibility found in classic organization charts where, as shown in Exhibit 10.1, a person or function A is directly responsible for B and C while, moving down one level on the chart, C is responsible for D's activities. These relationships are shown as solid lines on an organization chart when there is a direct reporting relationship, and as dotted lines when the reporting relationship is less formal. The solid lines from A to B and C and then from B on to D on the organization chart means that A has "straight-line" administrative responsibility for all of the persons or functions in a direct reporting relationship structured below A. This is the classic organization responsibility and reporting structure that has almost become a standard.

Of course, there are often many variations to this A to B to D direct reporting arrangement. In Exhibit 10.1, C is shown as having a dotted line relationship with E. This usually means that C does not have direct responsibility for all of E's activities. For example, E may directly report to W, perhaps a manager located elsewhere who does not have day-to-day oversight of B's efforts.

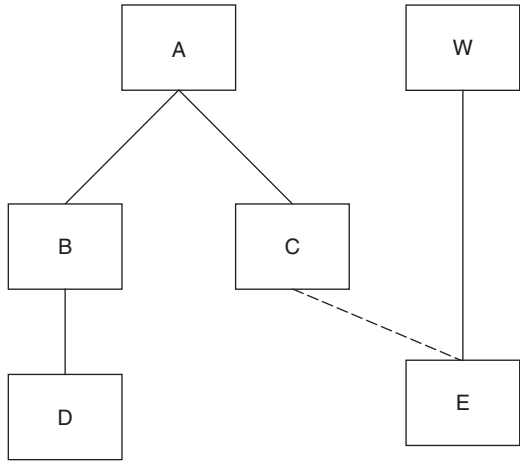

EXHIBIT 10.1 LINES OF AUTHORITY ORGANIZATION CHART EXAMPLE

Whether a straight- or dotted-line reporting structure, these classic organization charts tend to define regular enterprise activities, and many of the enterprise risk management (ERM) considerations discussed in past chapters are based on some form of this type of classic organization chart.

A project and project-based organizational structure represents a variation to this classic organization structure and presents some additional considerations to an organization's ERM. A project is a separate and often short-term effort to implement some objective where people or resources are assembled in a team—often outside of their regular day-to-day job duties—to perform or implement some special task or effort. Information technology (IT) projects, discussed in Chapter 12, are areas where many people have encountered the project management process in efforts to build new information systems. Beyond IT, many other organizational activities are also frequently organized as projects; examples of typical project activities include:

- A six-month, one-time project to move to a new office facility where regular organization functions

have handled the real estate and similar issues, but a special team is assembled do such things as mapping out office space moves, making certain that mailing address changes are posted, and handling employee communications regarding the move. Reporting to a designated project manger responsible for the overall move, the remainder of the project team would assist with this move on a part-time basis and would go back to their normal job responsibilities once the office move was complete.

- A continuing project to reduce product defects or otherwise improve manufacturing quality in an organization. Project team members with special skills would be drawn from many areas to develop strategies and help to implement changes throughout operations. Such a project might have one prime lead, with all of the others on the effort spending only a limited amount of their individual time on this effort. This could be a continuous effort, with the project team meeting periodically.
- A task force project to develop a new product or to launch a new marketing campaign. Here, project team members might work on this effort on a full-time basis, with some even brought in as new hires to develop the new product. If the initiative turns successful, the project team members might all become regular, continuing employees of a new organizational unit.

Each of these examples, as well as all projects in general, involves risks. Many of these are the same types of enterprise risks discussed in previous chapters. Other risks, however, often are more specifically related to the project management process. This chapter outlines the project management process and

introduces some of the specific risks associated with the success of management and completion of projects. These projects may cover limited-time special efforts, continuing special activities, or efforts that were initially launched as projects that become regular organization activities. The Committee of Sponsoring Organizations' enterprise resource management (COSO ERM) framework can be an important tool for both managing risks in existing projects and reducing risks in new project efforts.

PROJECT MANAGEMENT PROCESS

In past years, the term *project* often was used rather loosely and sometimes did not mean that much to many. A group of people in the organization would be asked to organize a "project" to implement some special effort. However, the organization and planning for such a project meant different things to different people. Sometimes, this effort often involved the designated lead's calling an assigned group together and doing little more than organizing the effort along the lines of, "I want you, you, and you" to perform various project tasks; there was little thought given to project organization and planning. These informal efforts often failed because the project team did not understand their objectives, time requirements, and the scope of the endeavor. In many instances, there were time and budget overruns or the project just failed for many other reasons. These types of failures are based on the lack of a consistent structured project management approach.

Several project-related definitions are important here. Project managers often use the term *program* when discussing multiple projects. A program usually refers to a high-level or supervisory project structure to manage or control a series of related or connected projects. For example, an organization may want to implement some fairly large initiative that is divided into a series of separate projects. Each of the projects can operate independently, but a program structure will manage all of them together. This chapter generally refers to a project either as one single effort or as a program of multiple projects.

With the exception of some U.S. government–led approaches, there was no consistent approach to project management until the Project Management Institute (PMI) a project management professional organization,[1] was launched in the 1990s. PMI is an international professional organization of well over 100,000 members in 125 countries. PMI has researched,

developed, and published a wide range of project management guidance materials. Their most significant document is a standards-like document called *A Guide to the Project Management Book of Knowledge (PMBOK Guide)*,[2] a comprehensive guide to all aspects of the project management process. Although not published as a government rules–type document, PMBOK has become the worldwide professional standard today for project management best practices.

PMI also has a professional project manager certification program, where PMI members who complete a professional examination and satisfy experience requirements can be certified as PMPs (project management professionals). While PMI and its PMBOK guide are de facto standards, there is also a Netherlands-based project management association called the International Project Management Association (IPMA).[3] IPMA is an organization of national project management associations, with the U.S. member organization being the American Society for the Advancement of Project Management (ASAPM). This smaller professional project management organization has goals similar to the much more prominent PMI.

PMBOK: Project Management Book of Knowledge

A search for books on project management in sources such as Amazon.com or Barnes & Noble will yield thousands of titles, covering all aspects and variations of project management. The better ones, however, are based on the previously referenced PMI PMBOK. This de facto standard describes all aspects of project management. Even if not involved in project management on a regular basis, the reader is encouraged to learn more about PMBOK and how it applies to project-level risk management. The following sections provide an overview of the PMBOK project management process, with an emphasis on its project risk management standards. Overall project risks will tend to be reduced if a management team follows these principles of good project management.

PMBOK identifies five basic project management process groups and nine knowledge areas that should be elements of almost all projects. These basic concepts are applicable to projects, programs, and operations and become a framework for effectively launching and executing projects. The five basic process groups are:

1. *Initiating.* There should be formal processes in place to launch any project effort, including a description of the project's objectives, estimated budgeting, and appropriate approvals.

2. *Planning.* Every project requires planning in terms of its time and resource estimates as well as for the linkages between components and other projects that require coordination.
3. *Executing.* These are the actual project activities—what needs to be done to accomplish project goals.
4. *Controlling.* An ongoing set of processes should be in place to monitor the appropriate completion of project elements, determining that budgets and objectives are being met. This can be an important component in project risk management.
5. *Closing.* The final process requires wrapping up the project effort and delivering the project components as well as summarizing and reporting the project results.

PMBOK looks at and defines each of these five project management processes as well as the nine knowledge areas, all in terms of their inputs, outputs, and tools and techniques. Project inputs include the documents, plans, and necessary resources to do the project, with outputs being the completed project materials. To go from the starting project inputs to the completed end product, a wide range of tools and mechanisms are necessary. A project to build a house, for example, would need lumber, a plan, and other supplies such as nails or roofing as the inputs. A hammer and a saw as well as knowledge of carpentry are the tools necessary to get started on the construction. The output in this simplified example is the completed house.

Although much more complex than just lumber, a hammer, and nails, the construction of a single-residence frame house is a relatively small and simple example of a project. Most projects launched by organizations of any type are much more complex. This complexity of project components is what has led to PMI and its PMBOK best-practices standards. Organizations had too often launched major project efforts that were developed as if they were little more than this example of lumber, nails, a few tools, and hopefully a plan as the project components to build a house. The results were often massive cost and time overruns as well as failures to even complete the project. New IT system implementation projects of the past, as discussed in Chapter 12, often were examples of poor project management techniques. Massive amounts of resources were expended, but the final project results were often late, over-budget, and missed original objectives. Many other non-IT projects had the same organization problems. All of them lacked consistent and thorough project management approaches.

PMBOK has defined this project management process in a consistent and well-controlled manner. In addition to the five basic project management processes, as discussed, the PMBOK guidance material defines nine project management knowledge areas:

1. Project integration management
2. Project scope management
3. Project time management
4. Project cost management
5. Project quality management
6. Project human resource management
7. Project communications management
8. Project risk management
9. Project procurement management

PMBOK guidance describes each of these knowledge areas—in terms of their inputs, tools, and outputs—with a considerable level of detail. For example, PMBOK's project procurement management knowledge area description includes input, tools, and output sections on:

- Procurement planning
- Solicitation planning
- Solicitation
- Source selection
- Contract administration
- Contract closeout

In addition to guidance on general management, PMBOK contains a fair degree of detail on what project management detailed tools and processes are needed in each of these knowledge areas. The purpose of this book is not to provide a detailed overview of all of PMBOK's knowledge areas but to emphasize the role of this tool in implementing effective risk management processes for the overall project management process. PMBOK is widely recognized today as the de facto standard for managing a project.

Chapter 1 discussed how, before the COSO internal control framework was launched, there was no consistent definition of what was meant by

internal control in organizations nor was there a regular process for defining and monitoring those internal controls. The launch of the COSO internal control framework in September 1992 as well as its adoption first in AICPA public corporation auditing standards and subsequently in the Sarbanes-Oxley Act (SOx) Section 404 internal control standards has defined the standards or approach for virtually all worldwide organizations today to define and document their internal controls. Will PMBOK become such a standard for the practice of project management? The International Organization for Standardization (ISO, www.iso.ch) has a draft international standard on project management, ISO 10006, which is very similar to PMBOK in terms of its content and structure. This approach will be the basis for effective project management standards going forward.

PMBOK: Risk Management for Project Managers

One of the nine PMBOK guidance materials knowledge areas is entitled Project Risk Management. Some of the project-related risk management standards here are very similar to the COSO ERM principles discussed in Chapters 3, 4, and others. The difference here is that the focus is on the management of risks for specific and often limited-time-duration *project* efforts, while much of the COSO ERM emphasis is on the management of risks for larger aspects of the organization and often on a recurring, ongoing basis. This section summarizes the PMBOK materials on risk management, but any professional interested in implementing overall effective project management tools and techniques should become familiar with all of the materials in PMBOK.

PMBOK has defined project risk management as[4]:

> Project Risk Management is the art and science of identifying, assessing and responding to project risk throughout the life of a project and in the best interests of its objectives.

This risk management knowledge area is broken down to specific elements, each with the defined processes of inputs, tools and techniques, and the element outputs. An overview of the PMBOK project risk management knowledge area is shown in Exhibit 10.2. The following sections summarize each of these areas and highlight how they relate to the COSO ERM framework. Just as risk management is an important but not the only important element of managing an enterprise, risk management is an important but certainly not the only key knowledge area in the overall process of launching and managing effective projects.

- Project Risk Identification
  - Inputs to Risk Identification
    - Project Descriptions
    - Other Project Planning Data
    - Historical Information
  - Risk Identification Tools and Techniques
    - Checklists
    - Flowcharting
    - Interviews and Observations
  - Outputs from Risk Identification
    - Sources of Risk
    - Potential Risk Events
    - Risk Symptoms
    - Inputs to Other Processes
- Quantification of Project Risks
  - Inputs to Risk Quantification
    - Stakeholder Appetite for Risk
    - Potential Risk Events
    - Sources of Project Risk
    - Cost Estimates
    - Activity Duration Estimates
  - Risk Quantification Tools and Techniques
    - Expected Monetary Value
    - Accounting Valuations
    - Simulation—Monte Carlo Techniques
    - Decision Trees
    - Judgment of Experts
  - Outputs from Risk Quantification
    - Opportunities to Peruse or Threats Requiring Responses
    - Opportunities to Ignore or Threats to Accept
- Risk Response Development
  - Inputs to Risk Response
    - Opportunities to Peruse or Threats Requiring Responses
    - Opportunities to Ignore or Threats to Accept

EXHIBIT 10.2 PMBOK PROJECT RISK MANAGEMENT KNOWLEDGE AREAS

- Risk Response Tools and Techniques
  - Procurement
  - Continuity Planning
  - Alternative Strategies
  - Insurance
- Outputs from Risk Response
  - Risk Management Plan
  - Inputs to Other Processes
  - Contingency Plans
  - Reserves
  - Contractual Agreements

Risk Response Controls

- Inputs to Risk Response Controls
  - Risk Management Plan
  - Actual Risk Events
  - Additional Risk Identification
- Risk Response Controls Tools & Techniques
  - Workarounds
  - Additional Risk Response Development
- Outputs from Risk Response Controls
  - Corrective Actions
  - Updates to the Risk Management Plan

EXHIBIT 10.2 PMBOK PROJECT RISK MANAGEMENT KNOWLEDGE AREAS *(CONTINUED)*

Risk Management Planning

Any new planned project needs the same types of organization environmental factors and process inputs that were discussed in Chapter 3 on understanding COSO ERM. The project manager launching a new project initiative needs to have an understanding of the overall organization's appetite for risk. If the organization has a low overall tolerance for risk, a project manager should exercise caution in planning and understanding the risks associated with a new project endeavor. Even if an organization takes a conservative, low-appetite-for-risk approach at an overall enterprise level, there sometimes may be situations where a project manager—under pressure to launch some new project-based initiative—will ignore the overall

organization culture to launch some relatively small project-based initiative. While it is perfectly proper to move in a different direction on a project initiative and to assume a bit more risk, the project manger should clear that initiative with responsible management and maintain documented and approved records of all activities regarding the higher-risk initiative. Even if the planned project is perceived to be very low risk in a normally high-risk organization environment, the project manager planning this work should keep these environmental factors in mind.

This risk management planning should also be reflected in other documents and tools used to launch any project endeavor. PMBOK defines the project scope statement and the management plan for a project as being key inputs to the project risk management planning process. While quite true, the risk environment for a new project should be a major influencing factor in developing both the scope and management plan. For example, if management wants to launch some new project initiative on a worldwide basis within a very tight time window, the risks of launching the effort over that wide scope and in a limited time frame should be considered.

The tools and techniques used in this project risk planning process should be similar to all the project-planning approaches used by an enterprise. If the organization has established a series of document formats in its other project management work, project risk planning documents should have the same touch and feel. Many project-planning elements that are described in PMBOK may lead the seasoned project manager to roll his eyes and say "Of course, that's obvious!" That can often be very true. An objective of this "Book of Knowledge" document is to summarize all aspects of some area as a constant reminder that they are important elements of the overall project management process.

After considering necessary inputs and required tools and techniques, the PMBOK section on risk management planning concludes with a discussion of the project management outputs from this risk planning process. The guidance material here calls for a formal risk management plan to be prepared for any new project. While a project to build a new guard gate at the entrance to a plant may not require much more than the minimum materials described in the PMBOK documentation, a similar project to launch an entire manufacturing floor unit will require a much more comprehensive analysis and identification of potential risk management planning outputs. The PMBOK material has a fairly extensive list of risk management planning outputs. Three are particularly important, regardless of the project's scope and size:

1. A definition of project risk roles and responsibilities
2. A documented risk breakdown structure (RBS)
3. An analysis of risk probabilities and their impacts

The first of these requires some management analysis followed by an assignment of responsibility. The point to remember, at this planning phase of project management, is not to define one person as being responsible for all of the overall risks that may impact the project but to assign specific responsibility for the *monitoring* of those risks. For example, if a new or planned project involves the launching of some new consumer product and if one of the risks associated with that product's success relates to the actions of competitors, some member of the overall project team should be given the responsibility for monitoring those competitor risks and reporting back to project management if there are any significant changes regarding these risks.

An RBS is an analysis and classification of the different types of risks that may impact a project. An RBS lists the different types of identified risks by hierarchy and category. As illustrated in Exhibit 10.3, this sample project—and probably many projects—will have external risks, and those external risks include regulator, market, and weather risks among others. The idea behind this RBS diagram is to think of all risks impacting a project and then classify them with as much detail necessary for effective risk management. The idea of a RBS is similar to the identification of various categories of enterprise risks, as discussed in Chapters 3 and 4. The term *breakdown structure* has been used here because the concept of a work breakdown structure is embedded in PMBOK and is familiar to many project managers. In order to effectively manage project risks, the RBS concept is an effective way to consider the risks impacting a project.

The third PMBOK project risk management planning key component is an analysis of the major project objective risks along with an assignment of their estimated probabilities and potential impact on the overall project. This is the type of analysis discussed in Chapter 2, and this project-specific analysis would typically be very similar to the sample business risk model shown in Exhibit 2.1. This type of analysis is an important part of the risk management project-planning process. Similar to any risk management planning exercise, the project management planning team should develop a good understanding of the various risks that are facing a new project about to be launched, how those risks relate to one another, and the relative probabilities of those risks occurring.

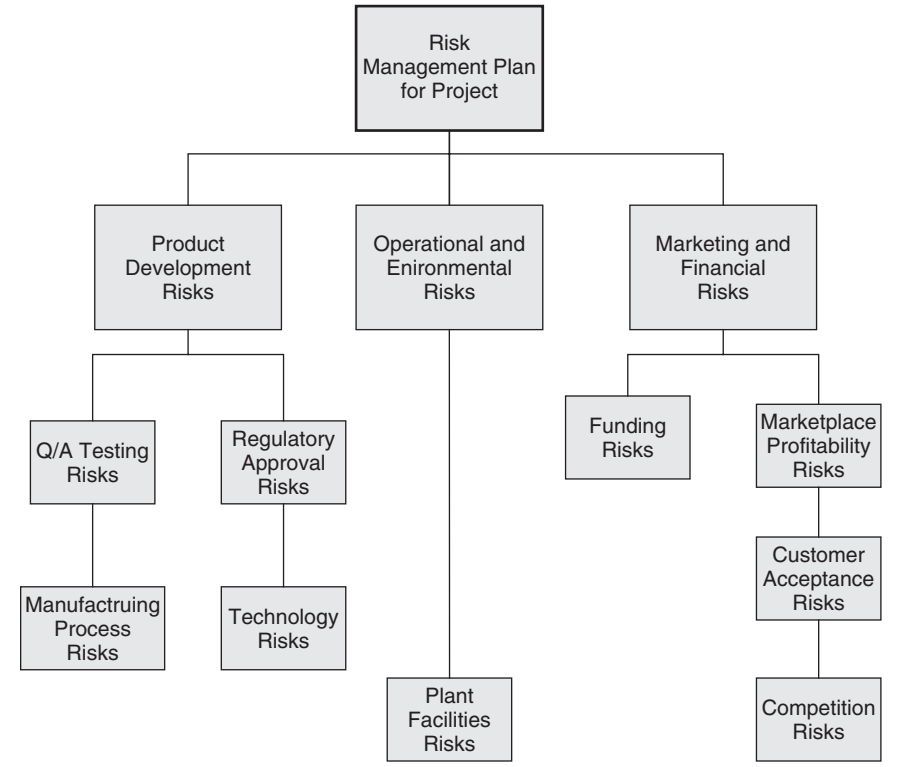

EXHIBIT 10.3 PROJECT RISK BREAKDOWN STRUCTURE EXAMPLE

Risk Identification

Closely related to risk management planning, PMBOK also specifies a phase in project management calling for the formal identification of the risks impacting a project. This should be an iterative process where the project management team looks at established project risk-related plans as well as other factors that could impact the overall project risk environment. The latter can include industry studies, the results of benchmarking, or academic studies, depending on the project environment. A project to develop a new electronic tool, for example, would benefit from an analysis of any published scientific papers covering that area. As a result of the information gathering, the project management team should review the gathered documentation and materials to identify and reaffirm potential project risks. Techniques such as brainstorming or a root cause analysis are examples of the many well-recognized techniques that can be used here.

The primary output from this phase of project-planning risk management is something called a risk register, a working document to list identified project risks, potential responses to those risks—on a high-level and very preliminary basis—and some documentation covering the root causes of those risks. Exhibit 10.4 shows an example of such a project-planning risk register control report. One person on the project team should have responsibility for the integrity of the register, but all interested parties including the project team and management should have access to this control document.

Project Qualitative Risk Analysis

This is the risk management project-planning process where the team involved with these phases of the project should formally prioritize the identified risks as a springboard for further action. The responsible project management team should take another hard look at the scope statement for the particular project, look at the identified risks from initial project planning, and give consideration to the lessons learned from past project endeavors. Because this section is really looking only at the risk management portion of the PMBOK project management process and because our overall topic is the COSO ERM framework and not project management, we are not emphasizing the overall project management process here. Activities such as a lessons learned analysis are procedures that would have been part of other projects and in other aspects of the project management process beyond just project risk management.

Here, the project management risk team should look at the threats and opportunities facing various risks identified from the risk register and map and describe them in a risk impact matrix, as shown in Exhibit 10.4. In today's era of color laser printers located in many offices, this is the type of report that is particularly meaningful when high-risk items are highlighted in red, medium in yellow, and low-risk in green. The reader may ask which members of a project team have the knowledge and understanding of project management tools to construct this or many of the other charts described in this chapter. The key resource to perform this level of analysis and other tasks described in this chapter is a PMP certified project manager. In addition to its PMBOK guidance, the previously referenced PMI professional organization also has a certification program where an experienced project manager can sit for a detailed examination to become a certified PMP. Just as hiring managers should look for candidates with certified internal auditor (CIA), certified information systems auditor (CISA), and certified public

Project: AB-789—Develop wireless monitor to link with Secure NET products

Risk Name	Risk Description	Impact	Likelihood	Planned Remediation	Current Status
Technology concerns	Project's technology as planned may not be able to meet performance specification requirements.	High—Failure would delay product introduction.	Low to medium-low	Tentative substitution product defined	Early stages of project—unknown
Product component shortages	Several key components are in short supply and supplies may be tight.	Medium—Substitutions are available	High—Products for prototype are in short supply.	Find appropriate alternative vendors.	Search in process for substitute vendors
Project may exceed approved development budget by over 25%.	Higher component costs and higher engineering cost than planned may cause missed objectives.	Medium—Would cause readjustment in financial plan.	High—Cost already exceeding expectations.	Tightly monitor development costs and seek other cost savings.	Monitoring costs, but no action plan to date

EXHIBIT 10.4 PROJECT PLANNING RISK REGISTER CONTROL REPORT

accountant (CPA) credentials when recruiting internal auditors, PMP credentials are the mark of an experienced project manager.

The prime output of this step in the project risk management planning process is an updated version of the previously referenced Exhibit 10.4 risk register. Based on the risk management planning analysis to date, this is where the project team can update this register to add such rankings as special priority numbers, grouping codes, and other items that will make this more of a day-to-day working document for the project management team. With this register example in an Excel spreadsheet format report, the document can be sorted and grouped by various codes for management attention.

Project Quantitative Risk Analysis

The PMBOK documentation for risk management planning has guidance material describing a fairly extensive set of techniques that the project management team should consider using when developing an understanding of the risks surrounding a new project. Using the risk register and the project management plan, the project team can develop a set of descriptive graphics to describe and then help analyze all aspects of the project. These might include:

- Sensitivity analysis to help determine which risks have the most potential impact on the project.
- Expected monetary value analysis to calculate the average expected outcomes when future events happen or do not happen. General statistical approaches for this type of analysis were discussed in Chapter 2 as risk management fundamentals.
- Decision tree analysis to look at the costs of various alternative outcomes. This is the kind of analysis that says we have an X percent chance of event A's happening, but if A does *not* happen, we then have a Y percent chance of either event B or C, each with their own costs and probabilities. Using various outcomes and potential costs, Exhibit 10.5 shows this type of decision tree chart in a project management context. This is a useful tool of many types of risk response planning and analysis. A decision tree risk response analysis was also discussed in Chapter 2 and described in Exhibit 2.7. Exhibit 10.5 is an example of this type of project-planning risk assessment exercise.

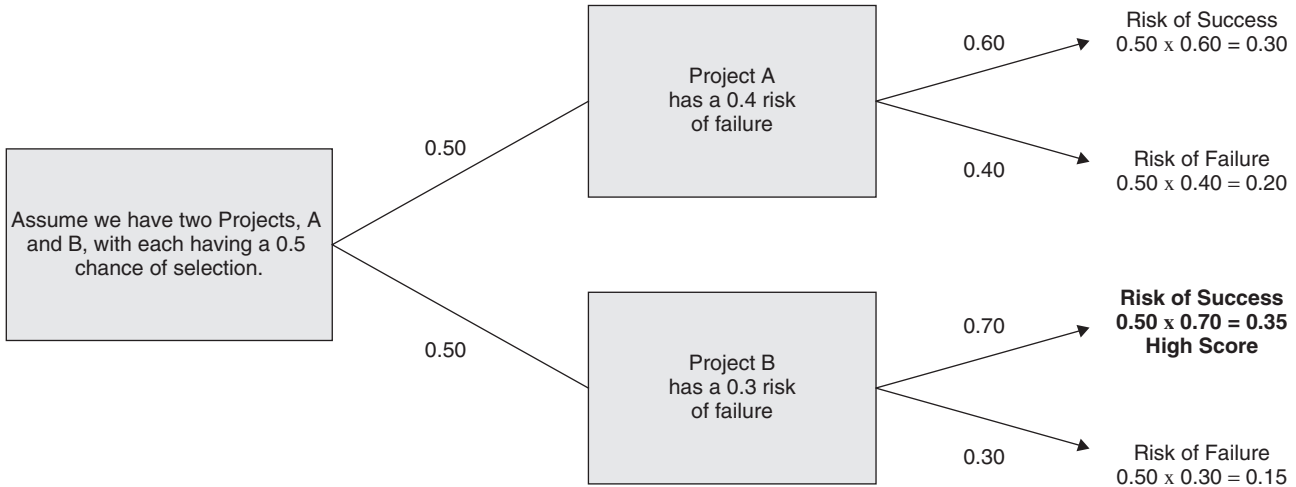

EXHIBIT 10.5 PROJECT MANAGEMENT DECISION TREE CHART

- Project cost simulation is another exercise for estimating probable project costs based on multiple expected costs and probabilities. Again, this technique was discussed in Chapter 2.

The PMBOK guidance lists a series of different types of quantitative risk analysis and planning tools, but almost certainly this entire suite of techniques will not all be used in its entirety for the risk response planning for a given project. While they can be useful analysis tools for project management in general, the project management team will generally want to select one or another that best describes and helps to manage risk in some given project endeavor. Often, this will be the choice of the senior managers reviewing project progress, and for very small projects there may be little, if any, quantitative analysis performed.

Project Risk Response Planning

Response planning is the process of developing options and actions to reduce the number and extent of potential project risks. This is the concept, in general, where the project management team has identified a series of risks that could impact a project, has assessed the costs and potential probabilities of those risks occurring, and now needs to develop plans if various potential risks do occur. This is often a very subjective type of exercise, because the project management team certainly does not have the time and resources to plan risk responses for all of the identified risks in a given project.

Risk response planning should be an exercise in which the project management team looks at the positive and negative risks that may impact a given project. As mentioned in other chapters, it is important to remember that there are often both positive and negative risks facing a project. Positive risks cover such matters as a project's failing to meet its planned time or cost objectives or perhaps the project-based launch of a new business with that business soon failing due to any of a variety of other factors. Positive risk means things occurring too quickly, too efficiently, or any of some other positive impacts. When faced with a "too good to be true" situation, the project management team needs a strategy to benefit from that positive risk. PMBOK suggests three strategies for dealing with these positive risks:

1. *Exploit the risk.* When things are turning out much better than expected, the project team can take such actions as adding more resources to the effort to ensure an earlier implementation or taking steps to provide better quality than originally planned.

2. *Share the risk.* The project team may have discovered a new approach that works much better than expected. This approach should be shared with other similar projects in the organization such that others can take advantage as well.
3. *Enhance the issue or area.* Based on positive outcomes, conditions can be expanded or capabilities increased. The concept here is that when the project management risk response process encounters an unexpected positive risk, the project team should be ready to take action to exploit the positive risk.

Because professionals at all levels tend to hope for the best, negative risks or threats are perhaps certainly more common in project management activities. There are three basic risk management strategy approaches that are used in many risk management environments and are also very applicable to project management risk planning:

- *Risk avoidance.* As much as is realizable, a project management team can adjust its plans and schedules or can adjust scope in some areas to avoid a potential project risk. The nature or magnitude of risks often arise early in the development of a project and can be avoided by such actions as clarifying requirements or adding expertise to the project team.
- *Risk transference.* The concept here is to give another party responsibility—some or full—for the liability of the risk. This can work when multiple units of an organization have some responsibility and the overall risk can be transferred to another organizational group. Risk transference is perhaps more common with finance-related projects where another party agrees to assume some risk through payment of a risk premium.
- *Risk mitigation.* This is the strategy of reducing the probability or impact of the risk occurring in the project by taking such action as adopting less complex processes, selecting more stable suppliers, or taking steps to repair damage. PMBOK uses the risk mitigation example of designing redundancy into a subsystem to reduce the impact of a failure of original components.

As strategies are developed and approved in the process, the project management team needs to document all actions through the previously discussed Exhibit 10.4 risk register, to update the project management plan,

as required, and for some risk strategies, to update risk-related contractual agreements.

Project Risk Monitoring and Control

The last component in PMBOK project risk management is a monitoring and control element. On a specific project level, the inputs, tools, and outputs here are similar to the monitoring component of the COSO ERM framework. While monitoring under COSO ERM is performed over the identified risks in a given business unit or even the entire enterprise, project management risk monitoring here covers an individual project, large or small. It is a subset or component of the overall ERM framework. An additional key word that is part of the PMBOK but not part of COSO ERM is *control.* As discussed in Chapter 3, COSO ERM talks about the importance of installing monitoring tools to view the status of various identified risks. Because PMBOK often places its emphasis on a much smaller-scope individual project level, the guidance emphasizes the need to install fallback strategies, contingency plans, and the like in the event of risk situations encountered during regular monitoring.

Project-planning risk monitoring involves taking the risk management plan, the risk register, approved changes, and performance reports to monitor the status of project risks. Many of the approaches discussed in Chapter 9 on the role of internal audit in risk management are very applicable here. These include risk-based audits, technical performance measurements, and both variance and trend analysis. The idea is to monitor the previously identified as well as any newly identified risks in the course of a project and to recommend preventive actions or changes as required.

PROJECT-RELATED RISKS: WHAT CAN GO WRONG

In many organizations and in many environments, individual projects present some very different and unique risks to an enterprise. Many think of projects primarily in terms of an IT environment where a project may include an initiative to install a new software package, an upgrade of some software version, or to install some new technology. Because of the impact of IT on the total organization, these projects often receive an inordinate level of organization-wide attention, particularly when there has been some failure or delay in organization operations due to the IT-related issue. As discussed in the introduction to this chapter, IT risk management issues will be discussed in Chapter 11. The typical organization today is involved

with many other non-IT project–related efforts as well, and risk assessment and management should receive adequate attention.

The typical project manager faces a wide variety of project risks in many project environments. Many of those represent what can be called red flags—that is, warnings to the project manager and project team that there may be risks associated with a project. Some typical red flags include:

- The project is very different from recent completed projects.
- The project scope, objectives, or deliverables are not clearly defined or understood.
- A large number of alternatives are perceived as a possible part of the project planning.
- Some or all of the necessary technical data to support the project is lacking.
- The technical approach or design selected is not mature.
- The standards for project performance are unrealistic or absent.
- Key measures—costs, schedules, or performance measures—are expressed in wide and uncertain ranges.
- Some or all environment or other governmental permits are outstanding.
- Other similar projects have been delayed or canceled.
- Some key subsystems or materials are sole source; that is, there is only one vendor.
- A large number of contingency issues are factored in the initial project plan.

Any of these conditions may represent a higher risk project environment and can cause situations wherein the project manager should take additional care in the management of that project.

Because IT projects have received so much attention over the years, organizations often fail to recognize that many other non-IT projects face similar problems and challenges. Many are run on a more casual basis, with little consideration given to the interaction of a given project with other management functions. Exhibit 10.6 shows how these types of project risk–related interactions start with project management integration at the top of the list and go through such areas as human resources, contracts and procurement, and then through quality and scope. Essentially every project

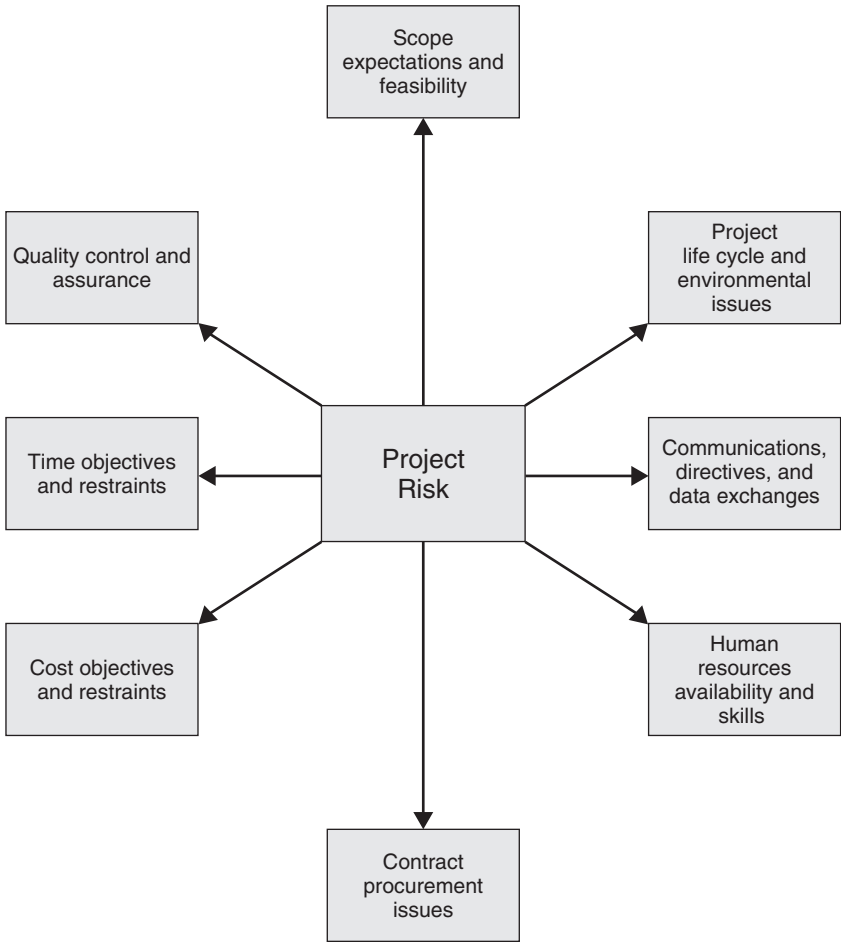

EXHIBIT 10.6 INTEGRATING PROJECT RISK WITH OTHER MANAGEMENT FUNCTIONS

effort, whether IT, production, financial, or any of many other areas, will have some degree of risk-related potential issues in each of these areas. The responsible project manager needs to understand the interactions and any risks associated with each of these areas.

The overall ERM framework has been described as a continuous but changing and ever-adapting process in the overall organization. The organization will manage a given risk situation, may adapt its processes to work with risks in a subsequent period, and often will go on and on in that manner. A project is a fixed-duration endeavor that will go through a series of

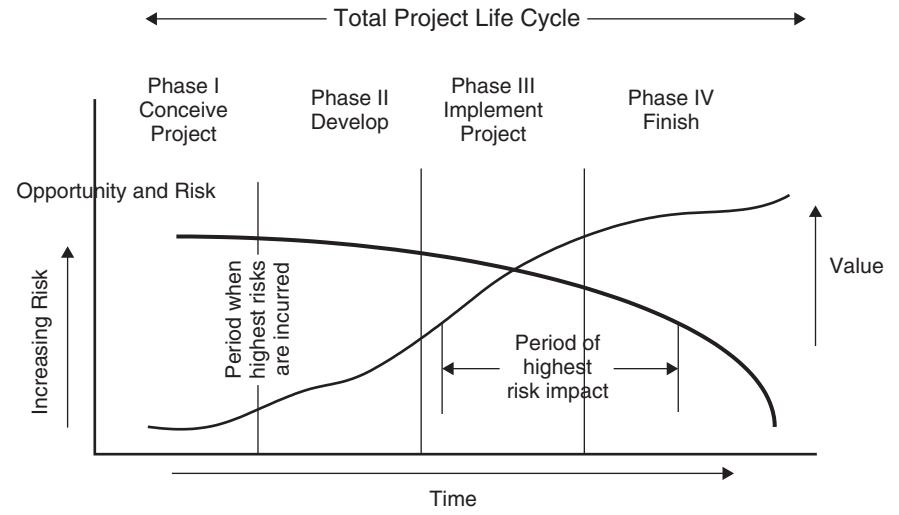

EXHIBIT 10.7 RISK VS. AMOUNT AT STAKE IN A PROJECT LIFE CYCLE

fairly consistent phases until the termination of the project and, hopefully, the delivery or completion of the planned project output. With this limited-time-period duration, project risk management is even more important.

Exhibit 10.7 shows this level of risk over the life of a project. Any project will go through a series of initial planning and development steps and then will move to development and implementation phases. As the exhibit shows, some of the highest project risks will be in the earliest phases of the project life cycle, where developers face the risks of making some very initial planning blunders regarding the project. However, as the project moves from planning and development to implementation, costs and time constraints will increase. Thus, as the exhibit shows, an individual project effort will face its highest risk during the implementation phase when many risks are still in place but have been covered and costs are increasing. This is the time in a project life cycle where there can be a high risk of project failure.

The objective of this chapter has not been to present a primer on good project management techniques but to discuss the importance of risk in the project management process. A project manager should very much keep risk in mind when planning and implementing any project. Those risk concerns should be very focused on the particular, limited-duration project in process but also must be closely coupled with the organization's overall ERM framework. There is a wealth of supplementary project risk-related

material published by the previously referenced PMI. Exhibit 10.8 lists some typical project risks and is adapted from a PMI book on project risk management.[5] Project managers should consider these types of risks when developing projects of any type, and general organization risk management should never lose focus on the many risks potentially associated with individual limited duration projects. Too often, these can fall out of the scope of the total ERM framework.

IMPLEMENTING COSO ERM FOR PROJECT MANAGERS

Good project managers should typically use the PMBOK process to manage and control all of their projects, whether limited duration, one time efforts, or larger and ongoing endeavors. We have used the word *typically* here because there is no required standard for the use of the PMBOK model, and some mangers will just plunge into new project efforts with little understanding of the good processes that are available to help achieve project success as well as the risks of potential project failures if those good processes are not used. As discussed throughout this book, many managers of various organizations' operating units had historically not thought much about the need for an appropriate set of risk management considerations before the recent introduction of COSO ERM. The traditional thinking was that "risk management"—the insurance department or function—would handle these risk-related issues, and individual managers were just responsible for completing their own objectives. COSO ERM has been or should be changing things for the general unit manager, and it should be of equal concern for the organization project manager.

The challenge for managers is to develop a greater appreciation and understanding of risk management within all project development activities and all project activities in the organization. This is often difficult for individual project exercises, as they are often launched as ad hoc, freestanding operations separate from many other organizational activities. The solution is to bring all project activities closer to the ERM function in the organization and to place some control over the project management process. This can be accomplished through establishment of a program management office and by requiring all projects adopt the PMI's PMBOK standards for all project activities in the organization.

Embracing Project Management Standards

When an organization has a strong project management culture, PMBOK has become the accepted standard, defining the language and practice of

Project Management Integration Risks

Risk Conditions

- Inadequate planning or resource allocation
- Failure to understand project objectives
- Lack of sufficient post-project reviews

Project Scope Risks

Risk Conditions

- Poor scope definition or breakdown in project structure
- Inadequate project planning or failure to recognize lead times
- Scope creep due to inadequate project management controls

Project Quality Risks

Risk Conditions

- Poor understanding of project deliverables quality
- Inadequate quality controls and quality assurance programs in place

Project Time-Related Risks

Risk Conditions

- Errors in estimating project task event times
- Resource availability or allocation risks
- Failure to readjust time estimated due to scope changes

Project Cost Risks

Risk Conditions

- Estimating errors or bad "best guesses"
- Inadequate controls over productivity, changes, or contingency estimates
- Problems with purchasing or other asset acquisitions

Unexpected Project Risks

Risk Conditions

- Ignoring potential risk conditions
- Inappropriate or unclear assignments of responsibility
- Poor insurance management
- Inappropriate or unclear contractual assignments of risk

EXHIBIT 10.8 TYPICAL PROJECT RISKS

Project Contract-Related Risks	Project Human Resources Risks	Project Communications Risks
Risk Conditions	Risk Conditions	Risk Conditions
• Unenforceable conditions or clauses • Unexpected contract adversarial relations • Inappropriate or unclear contractual assignment of risk	• Poor organization, definition of responsibility, or failure to inspire motivation • Absence of leadership or vacillating management styles • Failure to build strong project teams	• Poor overall planning or communicating • Improper handling of project complexities • Lack of adequate communication with internal and external parties related to project

EXHIBIT 10.8 TYPICAL PROJECT RISKS *(CONTINUED)*

project management. The language of PMBOK is often used for the implementation of various defined projects, and the growing number of professionals with PMP certification has strengthened the use of this standard. Other organizations tend to develop and manage their projects on much more of a casual, ad hoc basis. They assign people to some project-related effort with no concern given to good project management practices and certainly with a greater set of risk concerns. A good recommendation for any organization that manages any level of projects is to embrace the PMBOK project management standards. This will certainly improve the risk environment in an organization and the success rate of all implemented projects.

The main theme of this chapter and book is not on improved project management practices but on the utilization and implementation of COSO ERM and effective risk management. While the implementation of PMBOK in the organization will very much improve project risk management, the move from an ad hoc project management organization to one that embraces these standards and principles will take time and effort. Exhibit 10.9 outlines an action plan for adopting PMBOK and creating a project management culture in an organization.

PMBOK is a rich set of guidance materials that represent best practices but, admittedly, may be too much for the small organization that does not implement projects on a regular basis.

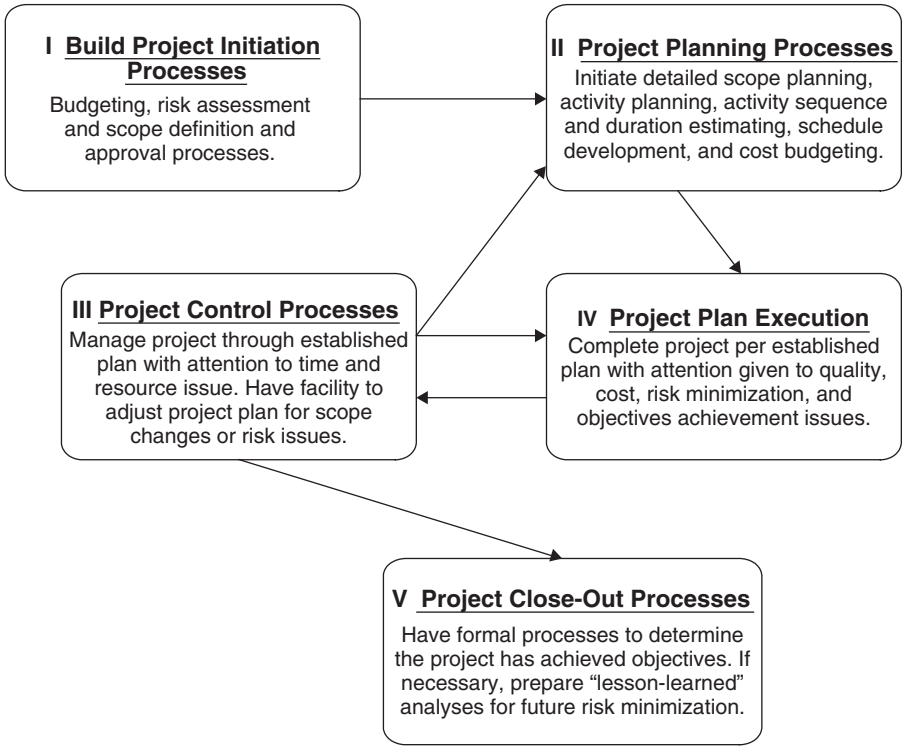

EXHIBIT 10.9 CREATING A PMBOK PROJECT MANAGEMENT ORGANIZATION

ESTABLISHING A PROGRAM MANAGEMENT OFFICE (PMO)

As discussed in the Project Management Process section of this chapter, a program is a senior-level project that serves as a vehicle to manage and supervise other, subordinate projects. This concept got started in IT where, for years, IT departments struggled to deliver projects on time and within budget. A solution was to rein in projects more closely through the establishment of a program management office (PMO) as a way to boost IT efficiency, cut costs, and improve on project delivery in terms of time and budget. What has worked for IT projects will work equally as well for all projects in an enterprise.

While a program is a senior-level type of project to manage other projects, a very effective approach is to establish a PMO function to manage all programs and projects in the organization. A senior-level fuction, a PMO is an authority that develops standards, acts on approval authority for all projects,

or even provides project management skills from a staff of PMP-certified people. A PMO office or function can often instill much-needed project management disciplines in their IT departments and all other groups involved with project management. PMOs can help by providing the structure needed to both standardized project management practices and facilitate project portfolio management, as well as determine methodologies for repeatable processes. The Sarbanes-Oxley Act (SOx) requires disclosure of major investments, such as large projects, that may affect operating performance. It is also a driver, since it forces companies to keep closer watch on project expenses and progress.

There are two basic models of PMOs: one that acts in a consulting capacity, providing project managers in business units with training, guidance, and best practices; and an alternate structure as a centralized version, with project managers and staff loaned out to business units to work on projects. How a PMO is organized and staffed depends on a myriad of organizational factors, including targeted goals, traditional strengths, and cultural imperatives. When deployed in line with an organization's culture, a PMO can help the enterprise deliver strategic projects that satisfy both the internal and external customers. Over time, a PMO should be able to save organizations money by enabling better resource management, reducing project failures, and supporting those projects that offer the biggest payback. The importance of this function will increase as the PMI has just launched a program manager PgMP certification program.

PMOs can vary in terms of size, structure, and responsibilities. They often function in the following areas:

- *Project support.* Provide project management guidance to project managers in business units.
- *Project management process/methodology.* Develop and implement a consistent and standardized process.
- *Training.* Conduct training programs or collect requirements for an outside company.
- *Home for project managers.* Maintain a centralized office from which project managers are loaned out to work on when a designated project ends.
- *Internal consulting and mentoring.* Advise employees about best practices with an emphasis on PMBOK.
- *Project management software tools.* Select and maintain project management tools for use by employees.

- *Portfolio management.* Establish a staff of program managers who can manage multiple projects that are related, such as infrastructure technologies, desktop applications and so on, and allocate resources accordingly.

There are many different approaches to managing a PMO function, but a centralized approach, typically marked by hands-on control over projects, often is most effective at organizations where the PMO regularly interacts with senior executives and has the power to cancel and prioritize projects. Using well-defined project management methodologies, the PMO often works with business units on every aspect of project management—from defining initial requirements to postimplementation audits. Maintaining consistent processes across the organization enables an organization to break down projects into manageable components and thereby minimize failures.

The responsibilities of PMOs range widely, from providing a clearinghouse of project management best practices to conducting formal portfolio management reviews. A PMO's oversight need not be limited to just project development and may include the coordinating and tracking of both projects and services. Coming up with a PMO that works for any given organization is an exercise in both customization and patience. When it comes to establishing a PMO, there are limited road maps to follow, benchmarks to shoot for, or metrics against which to measure. The most effective PMOs are those that reap improvements over time and continuously push the organization to improve on its performance.

Whether a full-functioning PMO or just active individual projects, effective risk management should be an important element in effective project management. An understanding of COSO ERM should use the concepts found in this framework to establish risk-related objectives, to identify those risk events, and to establish effective project-related responses to those risks. Project managers should try to embrace both the standards for good project management found in PMBOK and the elements of COSO ERM framework.

NOTES

1. Project Management Institute, Four Campus Boulevard, Newtown Square, PA www.pmi.org.
2. *A Guide to the Project Management Book of Knowledge (PMBOK Guide),* 3rd ed. Newtown Square, PA: Project Management Institute, 2004.

3. More information on this international project management organization can be found in *www.*IPMA.ch . IPMA is a popular set of initials. The same initials also stand for:

   International Public Management Association
   International Primary Market Association
   International Professional Management Association
   International Personnel Management Association
   Information Processing Management Association

   A web search for those initials may lead to wrong directions.

4. *See* note 2.
5. R. Max Wideman, ed., *Project and Program Risk Management*. Newtown Square, PA: Project Management Institute, 1999.

11

INFORMATION TECHNOLOGY AND ERM

Because of the complexity in building and maintaining information technology (IT) systems, their network interconnections, and all types of applications, risk management has been very important to IT processes. As discussed in Chapter 10 on project management risks, one does not have to have been a participant or observer of IT hardware and software projects for many years to have observed many IT projects that were launched with high expectations but subsequently failed for any of a variety of reasons. Just as people involved in marketing often have overly high expectations that some new initiative will succeed, IT processes often face similar risks.

IT-related issues and concerns are somewhat covered in the Committee of Sponsoring Organizations' enterprise risk management (COSO ERM) framework through that model's control activities and information and communications layers. The word *somewhat* is used because IT is so pervasive in business and operations processes that the high-level descriptions of risks in COSO ERM may seem to miss or ignore some of the many and evolving specific IT risks and concerns here. This is also a challenging area for

understanding risks and developing appropriate risk responses. As has been the pattern, no matter how strong the designed and implemented controls—particularly those that are software based—someone will find a way to violate and get around them.

While the range of IT risks is vast and extensive, this chapter will look at only three important broad IT areas and how COSO ERM should help an organization to better understand and manage those IT risks:

1. *Application systems risks.* Organizations often face significant risks when they purchase or develop new applications, implement them into full production status, and then maintain and revise them. There are multiple and often major risks associated with applications systems processes, and COSO ERM can help in better managing them.
2. *Effective continuity planning.* Once more commonly called disaster recovery planning, computer systems and operations can be subject to unexpected interruptions in their services. COSO ERM provides an enhanced framework to better understand and manage those risks.
3. *Worms, viruses, and systems network access risks.* There are many risks and threats in our world of interconnected systems and resources. COSO ERM provides guidance to assist an organization in deciding where it should allocate resources to protect from these risks. This chapter provides some high-level background discussions of this set of issues and discusses some of the more significant of these potential risks.

This chapter is not designed to provide technical guidance nor a discussion of new approaches for the strong IT professional. Rather, our objective is to provide a COSO ERM–oriented overview and discussion of issues for the many professionals involved in both IT processes and

concerns but more directly involved in IT technology matters on a regular basis.

IT AND THE COSO ERM FRAMEWORK

The COSO ERM information and communications layer and the control activities layers, as shown in Exhibit 3.1 and discussed in Chapter 3, represent the major areas where IT issues and concerns fit in this framework. The control activities materials discuss risk-related issues associated with both general and application controls. General controls include controls over IT management and its technology infrastructure, security management, and software acquisition, development, and maintenance. These controls apply to all IT systems—from legacy mainframe to client/server to laptop computer environments. Application controls cover specific controls related to one application, such as a fixed-asset control system, or groups of IT applications, such as all financial systems. An IT general control procedure may call for all applications to be backed up, per a specified frequency. A general-ledger IT application would be expected to be following those same general application control procedures but would perhaps have specific account balancing controls for general ledger accounts with that application.

Application controls then refer to specific processes in an IT environment. An enterprise may have an IT policy requiring that all IT new applications must be installed with a certain level of security and transaction balancing procedures. If we can determine that these general procedures are effective and working, the assumption will be that they are working for each specific application used within that IT infrastructure. This distinction between the general or pervasive IT control procedures and those that are specific to an application is a basic element necessary in understanding IT controls and risks. Exhibit 11.1 provides further definitions of these very basic IT control types. The COSO ERM guidance here is very high level, and many professionals would find a need for a greater level of background and support to IT control activities risks under the COSO ERM framework.

Because IT processes are so pervasive across an entity and beyond, the information and communications component of ERM should be an important information-transfer element across the ERM framework. Information—and particularly information managed and handled by IT systems—is an important concept in understanding and managing risks across all elements of the ERM framework. In many respects, the COSO internal controls framework—or at least in its earlier versions—as is shown in

General Controls

Information systems general controls include hardware, software, and administrative control procedures that apply to systems and applications, including:

- *Reliability of information systems processing.* Good controls need to be in place over all information systems operations. These controls often depend on the nature and management of the specific size and type of computer system used.
- *Integrity of data.* Processes should be in place to ensure a level of integrity over all data used in various application programs. These controls should, at a minimum, apply to all operating applications.
- *Integrity of programs.* New or revised programs should be developed in a well-controlled manner and follow consistent processes to provide accurate processing results.
- *Controls of the proper development and implementation of systems.* Controls should be in place to ensure the orderly development of new and revised information systems.
- *Continuity of processing.* Controls should be in place to back up key systems and to recover operations in the event of an unexpected outage—what was called disaster recovery planning or business continuity planning.

Application Controls

Applications apply to individual systems applications and are in addition to the overall general controls. For example, an IT operation may have strong general controls over the integrity of computer software revisions. An application to cover core strategic planning for the enterprise should have even stronger application controls including:

- *Controls of application inputs.* Individual applications should have error checking, security restrictions, and other controls to limit the risk of unauthorized inputs to the application.
- *Self-balancing and other financial and data controls.* Controls should be in place within individual applications to check for errors of computation or input and to provide accurate results that reflect on the objectives of the application.
- *Application output components.* Controls should place application output data on proper reports and in correct files, including transmissions or communications with other connected applications.

EXHIBIT 11.1 IT GENERAL AND APPLICATION CONTROLS EXAMPLES

Exhibit 6.1, does a better job of showing this concept of how IT and its information and communication component better fits in the COSO internal controls framework. There, the information and communications layer fits across multiple other internal control layers. This is similar to the way in which IT processes typically fit across and impact all aspects of internal controls in an enterprise.

Both COSO frameworks use the word *information,* a term or concept that covers many areas, including, but not just IT matters. However, both COSO framework guidelines talk about information in a very broad sense and generally do not specifically mention IT and its related risk issues. The ERM guideline simply states,[1] "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." The guidance material goes on to discuss strategic and integrated systems and highlights their integration with operations. The guidance continues with a discussion covering other important attributes of information such as its quality.

While COSO ERM provides some very high-level guidance on IT control issues in its control activities layer and through information and communications, there is a need to go down to a more specific level of detail to better understand and manage IT risks. Using the COSO ERM framework, the sections following discuss some important risk IT areas that impact many members of an enterprise. With any technology-based issue, of course, potential risks can become even greater as one goes down into an increasing level of detail, and we must always assume that IT controls are effective at some level. For example, when using a recognized software spreadsheet application, there will be a basic assumption that a numbers multiplication function (e.g., $3 \times 4 = 12$) is working. There may be a risk that rounding results could be wrong when processing very large volumes of data, but we generally assume there is a negligible risk that the basic multiplication function could be wrong.

APPLICATION SYSTEMS RISKS

Whether an automated system that helps design and build manufacturing products, a payroll application that covers periodic employee salaries, or the security system that denies access to an unauthorized person, IT applications are pervasive and can contain many risks. They represent software routines that have been custom developed by an enterprise, implemented purchased software products, or as software that is embedded in many

other tools and products. Some of the areas where an enterprise faces risks with its application systems include when an application development project is poorly planned or misses schedule or budget targets. Other risk areas include integrity and performance problems or just "bugs" in the application.

Without proper control procedures in place, failures here can cause problems or even embarrassments for an enterprise. A new application may be launched where only a limited set of conditions may have been tested. With an increased variation or volume of transactions, such an application can fail, sometimes dramatically. There have been many well-publicized failures over the years. Taking an example from the 1960s, a bug in the flight software for the United States' *Mariner 1* spacecraft caused it to divert from its intended path and crash into the Atlantic Ocean. An accident investigation discovered that a formula was improperly transcribed into its computer code, causing the miscalculation of the rocket. Whether it is a space rocket launch or a customer billing application, the causes for many, if not most, IT applications failures can be traced to poor design, testing processes, or change control processes. Adequate procedures and other good processes in place can limit those risks.

Application Development and Acquisition Risks

In the earlier days of computer systems applications and even up into the late 1980s, many organizations developed their own applications. Area management would decide they needed some type of reporting structure or specific application, and then would proceed to use their own in-house programming resources to build it. While some standard applications, such as payroll and fixed-asset applications have been offered by outside vendors and installed as purchased software for many years, many others have been built in-house, by enterprise development resources. There are risks associated with any new application development effort along with a somewhat different set of risks, depending on whether the application is based on essentially purchased software or built by in-house enterprise resources. Of course, as with so many matters, there generally is no all-or-nothing split here. Purchased applications typically take a large amount of programmer-intense tailoring work to install, and most in-house developed applications always use purchased software building blocks. With the possible exception of some desktop system applications, most require some degree of application development work. This may just include building tables or

parameter codes to operate the purchased software, but these still will have some development risks.

System Development Life Cycles. A term that was initiated by IBM in the very early days of systems application development procedures, the systems development life cycle (SDLC) refers to a traditional process for the development of new computer systems applications. This is the process for developing new applications that starts with establishing requirements for a new application, developing specifications to meet those requirements, and then going through the steps of developing, testing, and then implementing the application. This is called a life cycle process because once the application has been first installed, subsequent steps call for enhancing or retiring the applications to reflect expanded or revised needs to begin the cycle once again.

Although its origins date back to the days of freestanding batch applications, the SDLC process is still applicable in today's era of fast response, modular-based applications. Exhibit 11.2 shows such an SDLC process designed as a waterfall. Over the years, a variety of these types of processes have been launched by IT functions, depending on their management style and the technologies they are using. For purposes of understanding application development risks here, it is important that any application development effort of a project have some type of documented SDLC process in place to guide the development of those new applications. Following such a SDLC will ensure a consistent approach and reduce risks in the application development process.

On an almost continuous basis, various vendors have offered SDLC-like tools to assist IT functions in developing their IT applications. Some of these have been very documentation intensive, while others have erred in the other direction. From a risk minimization perspective, every IT application development function should have some type of SDLC process in place. Exhibit 11.03 is a checklist to help understand key SDLC risks. Having an effective SDLC process in place is a key risk minimization tool for any IT function.

Purchased Software Application Risks. Most of the IT applications developed or implemented in enterprises today are based on purchased software packages. These range from smaller, single-function tools that reside on a freestanding laptop machine to the extensive, all-function applications called enterprise resource planning (ERP) systems. These latter are often built on a series of interrelated databases that include all business functions such as

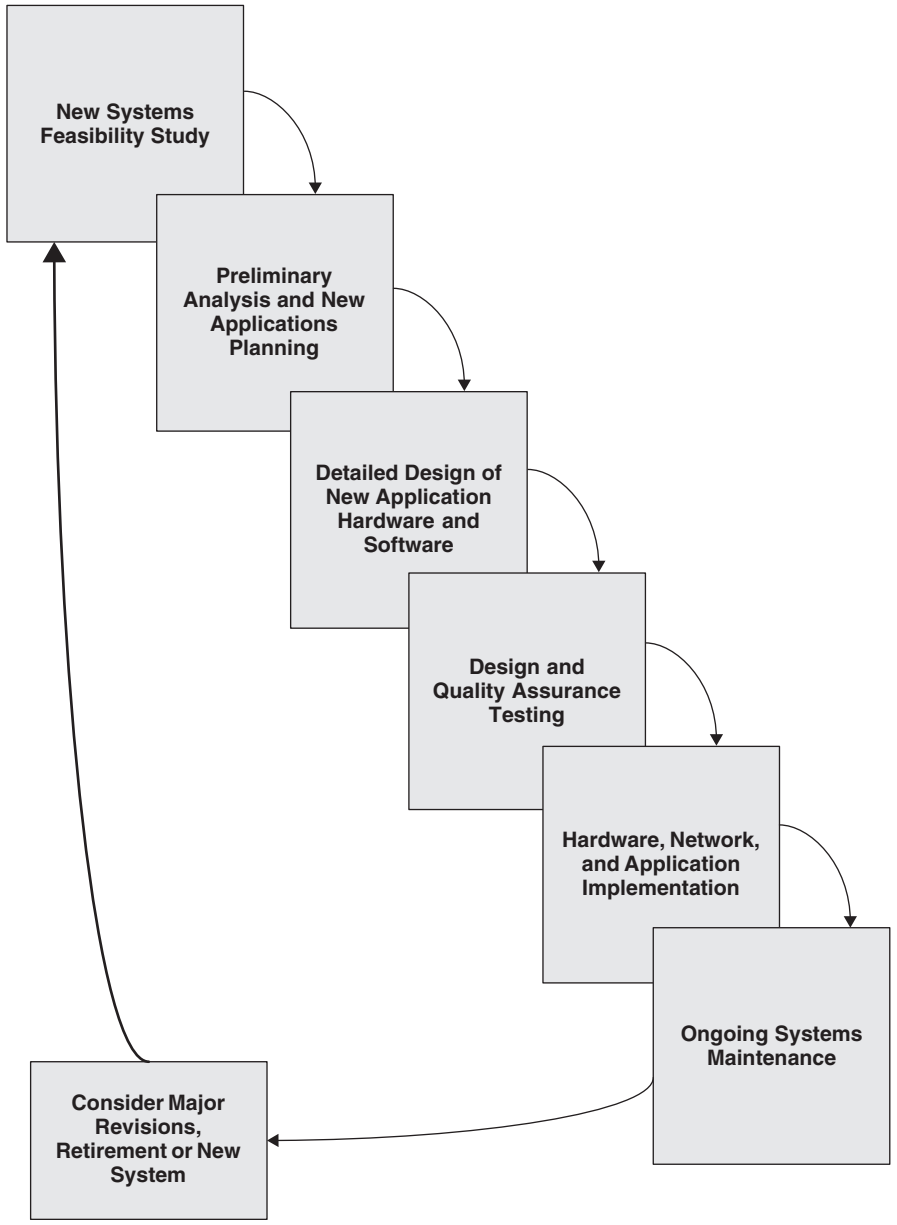

EXHIBIT 11.2 SDLC WATERFALL PROCESS

I New Systems Feasibility

- Has a formal feasibility study been prepared and approved per enterprise SDLC standards?
- Does the proposed new system use technology or processes that are new to the organization?
- Does the enterprise have a strong success rate in launching similar new systems?
- Did the feasibility study include an analysis of potential risks, such as:

  Risk of launching a new or untried process?

  Risk of new application not meeting its objectives?

  Risk of excessive cost or development time overruns?

II Preliminary Analysis

- Does the completed analysis map to the objectives outlined in the feasibility study?
- Have cost and performance estimates been prepared and are they achievable?
- Have estimates been prepared for overall new application costs and development resource needs?
- Does the design include a back out plan given the risk of systems failure?

III Detailed Design

- Does the design include any newer techniques or tools that are subject to failure?
- Have the risks of a potential supplier vendor failure been considered?
- Have detailed critical path level plans been developed with consideration given to the risks of missing those critical path linkages?
- Has the design considered interfaces with other systems or processes and the risks of failure of those connected entities?

IV Design and Quality Assurance Testing

- Does all testing activity focus on the achievement of planned system objectives?
- Have risks been considered when making "quick fixes" to repair any small problems encountered during the testing processes?

V Systems Implementation

- Have some types of customer satisfaction surveys been launched to identify any follow-up items with the new systems implementation?
- Have all risks identified during the earlier implementation phases been resolved?
- Has there been a detailed analysis to determine that the new application has met its established performance objectives?

EXHIBIT 11.3 MINIMIZING SDLC RISKS CHECKLIST

VI Ongoing Systems Maintenance

- If there were any ongoing or uncompleted items from the initial design, have plans been established to build them into a future version of the new application?
- Are there ongoing processes in place to monitor system performance and to make changes in light of problems or failure to meet expectations?

EXHIBIT 11.3 MINIMIZING SDLC RISKS CHECKLIST *(CONTINUED)*

general ledger, accounts receivable, accounts payable, fixed assets, inventory management, order entry, purchase orders and receiving, advanced distribution, electronic data interchange (*EDI*), bar coding, bills of material, standard costing, and standard product routing for a manufacturing enterprise, Exhibit 11.4 shows an ERP configuration. The concept behind these applications is that a change to one module—such as an inventory adjustment—will be reflected in related applications such as the general ledger and the bill of material. While extensive, these kinds of purchased ERP applications are not easy to install. They typically require massive changes to existing processes to better match business operations to the ERP software applications as well as some parameter-driven changes to the ERP software to make it a better business fit. An ERP implementation typically requires a long time period for its implementation, with a need for specialized staff training, as a beginning step, and outside consultants.

A major and expensive software investment, an ERP implementation project can introduce some major risks to an enterprise. For example, a survey in CIO magazine[2] discussed how Hershey, PA-based Hershey Foods had to issue two profit warnings in as many months because of massive distribution problems following a flawed implementation of their ERP system, which affected shipments to stores in their peak sales periods. Similarly, and at about the same time period, the domestic appliance manufacturer Whirlpool of Benton Harbor, MI, blamed shipping delays on difficulties associated with its ERP implementation. Both reported situations drove down their reported share prices. An enterprise can face some serious risk when implementing complex purchased software applications.

A problem associated with many of the major ERP implementations is the risk of selecting inappropriate software vendors and then the lack of appropriate project planning for launching the selected software package. Whether ERP or another purchased software product, there are multiple vendors offering similar and potentially very similar software products.

When purchasing any software package, and particularly software above a single user, desktop level, an enterprise should take some of the following steps to reduce risks associated with purchased software:

- Software Product Feasibility / Compatibility
  - Does the product match feasibility study requirements or at least is a best fit?
  - Is the software product fully compatible with the enterprise's systems and operating environment?
  - Do there appear to be any constraints – such as table sizes or value restrictions – that might require installation workarounds?
  - Will it be necessary to install customization parameters to install the software, and if so, does the amount of required work seem reasonable?
- Product History
  - Has the software been released and on the market for an appropriate length of time?
  - Was the software designed for the same general purposes and functions as were defined in feasibility requirements?
  - Is the software built around recognized and appropriate tools, such as the supporting database?
- Vendor Background
  - Has the vendor been established for an appropriate period of time?
  - Does the vendor appear to have an appropriate level of financial strength?
  - Is there any outstanding major litigation against the vendor that could cause software product concerns?
- Customer & Trade References
  - Can the vendor supply a list of other existing customers that can be contacted as references?
  - Has the vendor and this software product received favorable reviews and comments in the IT press?
- Revision Practices
  - Will the vendor make commitments to upgrading and improving the product?
  - Is there evidence of product revision history over past periods?
  - Is there a formal process in place for customer-initiated revision requests?
- Product Documentation & Training
  - Does the documentation supporting the product appear adequate?
  - Is there evidence that this software documentation is updated regularly or as required?
  - If necessary, are there facilities for customer training the use of the software product?

EXHIBIT 11.4 PURCHASED SOFTWARE CONTRACT GUIDELINES TO REDUCE RISKS

- Product Customer Support
  - Does the vendor have a customer support "help desk" that operates 24x7 or at least during normal business service hours?
  - Are there charges for customer support calls beyond a regular service contract?
  - In the event of some software major catastrophe, does the vendor have the capability to reinstall software on a quick fix basis?

EXHIBIT 11.4 PURCHASED SOFTWARE CONTRACT GUIDELINES TO REDUCE RISKS *(CONTINUED)*

Failure to select the appropriate software vendors can present major risks to any contracted software product. Although the goal of this book is certainly not to provide guidance on vendor selection best practices, Exhibit 11.4 provides suggested purchased software contract guidelines to reduce risks. These are just best practices, such as ascertaining the software vendor has successfully installed this same software product in a comparable environment.

We have focused on major-scale ERP software products as an example of the risks associated with purchased software applications, but there are many vendor software offerings where the same risk avoidance concerns are also applicable. Following up on the Exhibit 11.4 review criteria, an enterprise should determine that any purchased software vendor has procedures in place for such matters as regular updates of the software product.

In-House Developed Software Application Risks. There was a time when most enterprises developed their own computer systems applications. For example, enterprises once decided that they had to develop their applications because of their unique needs; that is, enterprises once frequently claimed that "Our accounts payable process is *different* when compared to our competitors, and we must develop our own unique system!" While this type of argument really does not apply for most organizations, many have used it over the years as a justification for developing their own software applications. While this strategy is not that common today, some enterprises still devote substantial efforts to developing their own unique applications. This is often more appropriate for very specialized applications, such as some manufacturing process control systems.

We have previously discussed the fact that there is not a strict dividing line between those applications that are purchased from software vendors and those developed in-house. The reality is that the software development process does not fit totally on one side of this divide or the other. Risks can

be limited through good SDLC procedures supporting by strong project management practices.

Software and Application Systems Testing

Although it is essential that, for any new or revised IT application, the SDLC requirements are defined and documented and that quality reviews ensure that the application is built according to those specifications, it also is necessary to test all new applications before placing them into production. An enterprise can face a major risk to the quality and integrity of its IT applications if new applications are not fully tested. This testing process should take place at an application level and for overall systems.

IT testing is of limited value unless there are strong procedures in place for developing initial testing plans, planning objectives, and for reviewing the results of those testing activities, including specified pass/fail criteria over the results of this testing. Many of these testing activities are similar to the Sarbanes-Oxley (SOx) Section 404 processes used for assessing and testing internals controls and described in Chapter 7.

An enterprise can face major risks to the quality and integrity of its IT application systems if they have not been adequately tested. Application tests should be performed primarily for one of the following reasons:

- To validate that the IT application is operating according to the SDLC documented procedures
- To determine the impact, if any, that a suboptimally designed application process may not have achieved its defined objectives

The type of testing performed will vary depending on the actual application being reviewed. The testing should be performed by the application developers—whether in-house programmers or the staff implementing purchased applications. In order to provide sufficient testing activities to minimize risks, the results of the test should be well documented so that an outside reviewer can assess the adequacy of this testing activity.

Control and Balancing Procedures

In addition to controlling risk by building and testing new IT applications with appropriate SDLC systems development and testing controls, the application itself should be designed with its own strong internal accounting controls. These are the “do the debits equal the credits?” types of internal control facilities that are key for all accounting and operational applications. Going back to the early days of IT applications and up to the

present, there has always been a need to build applications with such appropriate internal accounting controls.

The COSO ERM guidance materials on control activities recognizes the importance of these many application controls that are performed every day that serve to prevent and detect inaccurate, incomplete, inconsistent, or improper data capture and processing through calculation and logical comparison. Several of these controls are described in the framework section of COSO ERM reference materials[3]:

- *Balancing control activities.* Applications should detect data capture errors by reconciling amounts captured either manually or automatically to a control total. As an example, an application should automatically balance the total number of transactions processed and passed from its online order entry system to the number of transactions received in its billing system.
- *Check digits.* As an application control that goes back to the early days of computer systems with punched card inputs, calculations should validate data, with part numbers containing a check digit to detect and correct inaccurate ordering from suppliers.
- *Predefined data listings.* When appropriate, an application can provide the user with predefined lists of acceptable data. An intranet site, for example, can include drop-down lists of products available for purchase.
- *Data reasonableness tests.* Applications could compare data captured to 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 may trigger a review. This is the type of application control that should set off warning lights to invite more detailed scrutiny.
- *Logic tests.* The computer program code in applications should include the use of ranges limits, value checks, or alphanumeric tests. As an example, government agency application might detect potential errors in social security numbers by checking that all entered numbers are nine digits.

Used as examples in the COSO ERM guidance materials, the above are just a few of the many types of controls that should be built in effective applications to lower the risk of errors or miscalculations. Whether purchased software or developed in-house, these and many other similar control

procedures should be built in the application. Because these controls—such as checking to determine such elementary matter as if the inputs equal the outputs—are so basic to accounting controls and IT systems, it is often easy to forget to check that they exist.

Because the individual applications for an enterprise may have their own sets of objectives and implementation approaches, there will be differences in risk responses and related control activities. Even if two organizations had identical objectives and made similar decisions on how they should be achieved, their control activities would likely be different. Each is managed by different people who use individual judgments in effecting internal control. Moreover, controls reflect the environment and industry in which an entity operates, as well as the complexity of its organization, its history, and its culture.

The IT asset and application operating environment for any enterprise affects the risks to which it is exposed and may present unique reporting objectives or special legal or regulatory requirements. A pharmaceutical manufacturer, for example, must manage far greater IT quality and integrity risks than those facing some manufacturing companies.

The complexity of an IT operation, and the nature and scope of its key applications and other activities, affects its control activity risks. Complex organizations with diverse activities may face more difficult control issues than simple organizations with less varied activities. An organization with decentralized operations and an emphasis on local autonomy for its IT systems presents a different set of risks and control circumstances than a highly centralized one. In addition, the complexity and nature of enterprise controls including their location and geographical dispersion have an impact on the risks associated with IT applications and overall IT methods and processes.

EFFECTIVE IT CONTINUITY PLANNING

Just as we rely on electrical power and clean water to be in operation, an enterprise today depends on its IT systems to operate continuously and effectively. Power and water are usually supplied by outside utility providers, but an enterprise is largely responsible for the operation of its own IT resources. An enterprise faces numerous risks around the continued operation of its IT assets. There typically is not one major or central computer facility for handling major automated applications but a wide-range desktop of devices, servers, and other computer systems connected through often very complex communications, storage management networks, and

links to the Internet. An enterprise can face a major risk if it loses the ability to access and use its IT system for even a relatively short period of time. To limit those risks, there is a need to have procedures in place to promptly restore operations. Once known as IT disaster recovery planning, today these procedures are generally called continuity planning.

The concept of what was called IT disaster recovery planning goes back at least to the 1970s, and was originally based on the need to have processes in place to resume operations if some single disaster made the centralized computer center inoperable. We say "the computer center" because enterprises once used primarily single large centralized computer systems in contrast to today's environment of networks and servers. These systems support many enterprise operations, and the concept of having tools and procedures in place to rapidly restore overall business operations is called continuity planning. The user of an online order processing application is concerned both about whether server systems are operating and whether a customer order, submitted through an Internet site, can be processed properly and efficiently. In the event of an unexpected outage, the IT systems should be restored and operating as quickly and efficiently as possible in order to support and restore the business processes.

In addition to concerns about restoring operations in the case of some disaster or continuity event, an enterprise should also be concerned about the continued and high availability of its IT resources. Any form of computer systems downtime can be very costly to an organization. For example, the Disaster Recovery Institute[4] has estimated that the average hourly impact of an hour of systems downtime is $89,500 for an airline reservations system or $2.6 million for a credit card authorization provider, among others. Beyond just estimates, eBay's Internet auction site went down for 22 hours in August 1999. This caused $4 million in lost fees and a $5 billion drop in eBay's market value.[5] The message here is that high systems availability is very important to an enterprise, and the risk of an extended outage can be reduced through effective IT continuity plans.

In the distant past, IT functions often attempted to minimize the risk of systems outages by constructing what were called disaster recovery plans. After an extensive project to build such an older IT disaster recovery plan, the guidance materials were often published in thick books located on the desks of a few key IT and other enterprise managers. The idea was that in the event of some emergency event, people would pull out their disaster recovery manuals and be able to look up such data as the telephone number

of the designated backup site in order to report the emergency or the instructions for other emergency procedures. The material in these thick books might have worked in theory if the manuals were always kept up to date and the nature of the crisis event allowed enough time to review the manual first and then react. Many real-life events are much more crisis oriented, with little time to dig out the disaster recovery manual and read its documented information. When the building is on fire, for example, human nature says that one should get out of the building as soon as possible, not spend time studying the published evacuation instructions. To minimize risks, organizations need to think through these various possible situations in advance. They need an emergency response plan.

Two types of emergency incidents are significant. The first is the risk of a fire-in-the-building type of emergency incident. The supporting emergency response plan here would include posted fire exits and past experience with frequent fire drills. This type of emergency response plan should cover all organization operations, not just IT systems, and should be regularly tested. The second level of emergency response plan, however, covers specific individual incidents that may or may not turn out to be significant, but must be corrected at once followed by an investigation and a plan of corrective action to prevent further incidents. These are called emergency *incidents,* and they often include such matters as security breaches or the theft of hardware or software. A good emergency incident response plan should be acted on quickly to minimize the effects of any further breaches. It should also be formulated to reduce any negative publicity and to focus attention on quick reaction time. Rather than just an IT-related plan, all appropriate levels of enterprise operations should be covered.

An emergency incident response plan can be separated into four sections:

1. *Immediate response activities.* Whether a security breach, a theft of assets, or physical intrusion, resources should be in place to investigate the matter and take immediate corrective action.
2. *Incident investigation.* All reported matters should be fully investigated to determine the situation that caused the emergency and possible future corrective actions going forward.
3. *Correction or restoration.* Resources should be available to correct or restore things as necessary. Since emergency incidents can cover a wide variety of areas, these resources may include IT security specialists, building security managers, or others.

4. *Emergency incident reporting.* The entire emergency incident and the actions subsequently taken should be documented along with an analysis of lessons learned and any further plans for corrective actions.

In order to reduce risks, emergency incident responses must be decisive and executed quickly. The idea is to quickly pour water on a fire, not to build short-term strategies to prevent it from burning further. Quick actions are needed, with little room for error in most cases. By staging fire drill–like practice emergencies and measuring response times, it is possible to develop skills that foster speed and accuracy. Reacting quickly may minimize the impact of resource unavailability and the potential damage caused by any future systems or facility compromises. An organization faces many emergency incidents or other threats beyond the massive New York World Trade Center 9/11 type of emergency and the resultant overall failure of most impacted IT system resources. While the focus should always be on more major contingency planning issues, an organization needs to have mechanisms in place to respond to lower levels of unexpected emergency events as well.

An enterprise's risk management function should work with their IT operations to develop appropriate emergency response plans that will exist at a total facility level, such as a fire escape plan, and at an individual level, such as a plan to respond to a security breach. To reduce risks, these plans should be regularly updated and tested.

Beyond an emergency response plan, an enterprise needs to develop a set of IT continuity plans. This type of plan consists of an outline of the steps necessary to help an organization recover from major service disruptions, whether a fire type of emergency, a computer equipment or network telecommunications failure, or any other form of major disruption. The goal of such a plan is to help an enterprise reduce the risk of a disaster outage or extended service interruption to an acceptable level and to bring business operations back. This type of continuity plan represents a change in emphasis from what IT professionals once called disaster recovery plans. That older emphasis was to get data processing operations working while the continuity plan emphasized overall needs of the business unit. Today, these plans have been redesigned to broaden them and to reduce risks. As discussed, they are called business continuity plans (BCPs).

An effective BCP is an important tool to build or manage IT risks. There are many good practices and procedures for building a continuity plan that are beyond the scope of this book. There are, however, several professional organizations such as the U.S.-based Disaster Recovery Institute and the

London, England–based Business Continuity Institute that have adopted a frequently published and well-recognized set of ten BCP recommended professional practices as outlined in Exhibit 11.5. These have become the universally accepted standards in the industry for the key steps or components in a BCP. An effective BCP is a critical risk tool for an organization, and management is responsible for the survivability and sustainability of total operations to serve customers and service recipients. Many companies and most government organizations are required by law today to develop these continuity and contingency plans. In other instances, other legislation effectively requires a BCP. SOx, for example, requires registered organizations to be able to report their financial results in a timely manner. A systems failure cannot be an excuse, and an effective BCP will help to support the organization here.

A principal objective of a BCP should be a well-structured and coherent plan that will enable the enterprise to recover normal business operations as quickly and effectively as possible from any unforeseen disaster or emergency that interrupts normal IT services. There should also be subobjectives to ensure that all employees and stakeholders fully understand their duties for implementing the BCP, that information security policies are adhered to within the scope of the plan, and that the proposed contingency arrangements are cost effective. BCP deliverables should consist of the following components:

- Analysis of business risks and an impact analysis
- Documented activities necessary to prepare the organization for various possible emergencies
- Detailed activities for initially dealing with a disaster event
- Procedures for managing the business recovery processes, including testing plans
- Plans for BCP training at multiple levels in the organization
- Procedures for keeping the BCP up to date

A major objective here is to allow the organization to restore business operations as quickly and effectively as possible in light of a disaster event. This is an activity that requires active participation on many levels, and one where IT management, the risk management team, and internal audit should take a major role in helping to ensure its effectiveness.

The identification and analysis of risks here is essential. Risk or business impact analysis is a particularly important process for determining what applications and processes to include in the overall BCP. This process often includes developing a descriptive list of the organization's key business

The following recommended professional practices or steps were initially developed by the Disaster Recovery Institute:

1. *Project Initiation and Management*. BCP processes should be managed through formal project management processes and within agreed time and budget limits.
2. *Risk Evaluation and Control*. A formal BCP risk evaluation process should be used to determine events that can adversely affect the organization and its facilities with disruptions as well as major disasters, the damage such events can cause, and the controls needed to prevent or minimize the effects of potential loss. This should include a cost-benefit analysis to justify investments in controls to mitigate these risks.
3. *Business Impact Analysis*. Managers should understand the overall impacts resulting from disruptions and disaster events that can affect the organization as well as techniques that can be used to quantify and qualify them. This requires identifying critical functions, their recovery priorities, and interdependencies such that recovery time objectives can be set.
4. *Developing Business Continuity Strategies*. One single BCP is not applicable for all circumstances, and management should develop an appropriate strategy to determine and guide the selection of alternative business recovery operating strategies for recovery of business and information resources within the recovery time objective, while maintaining the organization's critical functions.
5. *Emergency Response and Operations*. Emergency procedures should be in place to respond to and stabilize the situation following an incident or event, including establishing and managing an Emergency Operations Center to be used as a command center during the emergency.
6. *Developing and Implementing Business Continuity Plans*. The BCP should be developed, documented, and implemented using a formal, best practices based process that provides recovery within established recovery time objectives.
7. *Awareness and Training Programs*. Processes should be in place to make all appropriate members of the organization aware of the appropriate BCP procedures with training programs in place on their usage.
8. *Maintaining and Exercising Business Continuity Plans*. The BCP and its key elements should be kept up to date with periodic testing of critical plan elements. Processes should be implemented to maintain and update the BCP in accordance with the organization's strategic direction.
9. *Public Relations and Crisis Coordination*. Processes should be in place to communicate all events surrounding a contingency event and to communicate with and, as appropriate, provide trauma counseling for employees and their families, key customers, critical suppliers, owners/stockholders, and corporate management during crisis. All stakeholders should be kept informed on an as-needed basis.
10. *Coordination with Public Authorities*. Processes should be in place for coordinating continuity and restoration activities with local authorities while ensuring compliance with applicable statutes or regulations.

EXHIBIT 11.5 DISASTER RECOVERY BUSINESS CONTINUITY PLANNING PROFESSIONAL PRACTICES

areas, typically ranked in order of importance to the business, as well as a brief description of the business process and its main dependencies on systems, communications, personnel, and data. If the organization already has prepared an assessment of its key business processes, this can be an excellent time for the BCP team to update that documentation and to evaluate the relative importance of each. It should be noted that this is an inventory of *business processes*, not of critical application systems. While the two are sometimes thought of as being one and the same, it is important that they be considered as the key processes to keep the business operating.

A next step here is to look at those key business processes in terms of potential business process outage failure impacts. The idea is to look at the impact of estimated outage times in each area on the basis of something like:

less than 2 hours outage

2 to 24 hours outage

24 to 48 hours outage

greater than 48 hours outage

This type of analysis would focus on each key business process, such as the impact on customer services, loss of customers, and the like. Within each of these risk factor areas, the criticality impacts of various levels of outages should be considered. The approach is to consider the risks of some specified application failure of less than two hours as well as the related risks of any impact on customer services; even the related exposure risk to possible litigation could be considered. Following the risk management techniques described in Chapter 2, monetary estimates of exposure losses should be considered. Monetary values should be added to a worksheet, as discussed in Chapter 2, to highlight key time-based exposures. The concept behind this analysis is to design an effective approach to get back in operation after a business continuity outage. An effective BCP is an important way to minimize the potential risks to IT services due to some unexpected, disaster-type event.

WORMS, VIRUSES, AND SYSTEM NETWORK RISKS

An enterprise's IT operation today consists of much more than just IT equipment and resources within their offices and plants, including a wide variety of other resources connected through the Internet and other networked

resources. Even if an enterprise effectively prohibits the regular employee use of the Internet during regular working sessions, it is still effectively connected to these networks today. Communications with banks and financial institutions, access to government reports, and even ordering certain parts and supplies requires Internet access. A fantastic tool, these interconnections contain many risks in terms of exposures to worms, viruses, and other types of malignant software code that can cause peril for all types of networked and connected computer systems, ranging from a home office desktop to a large central system.

A computer virus is a program or piece of program code that is loaded onto a computer system without the knowledge and participation of the computer system's owner. The virus then runs against the system owner's wishes and is called a virus because the program can spread and replicate itself similar to an infectious disease. A simple virus is a set of program codes that can make a copy of itself again and again until it has used all available memory and the system is brought to a halt. Other types of viruses are capable of transmitting themselves across networks and bypassing security systems.

The first computer virus programs appeared in 1986 on an IBM PC. Back then, the virus was slipped onto a floppy diskette used for loading and sharing data and programs. Once inserted in another computer, the virus jumped from the floppy and targeted the new host computer. While software tools were soon built to at least detect and protect from the initiation of system viruses, innovative and malicious persons developed other programs with such names as worms or Trojan horses.

A worm is similar to a virus but spreads from computer to computer without any help from a person. A worm takes advantage of file or information transport features on a system and can send out hundreds or thousands of copies of itself, creating a huge devastating effect. Malicious persons, ranging from creative programmers trying to "beat the system" to potential terrorists, have created these types of programs. The cost to society of lost business, time requirements to reconstruct, and privacy issues over lost data has been worldwide and major. A *Wall Street Journal* article[6] observed that computer-based crimes had caused $14.2 billion in damages to businesses around the globe in 2005, including the cost of repairing systems and lost business.

An enterprise needs to recognize the threat of what is often called CyberCrime and needs to take steps to protect from these risks. Establishing effective controls is a challenge. The above *Wall Street Journal* article referenced talks about two young men as CyberCrime perpetrators—one in

Turkey and the other in Morocco—and the FBI's difficulty in tracking them down and apprehending them for their CyberCrime activities. This is not an easy task, but an enterprise can reduce its risks and the threat of CyberCrime by:

- *Following "best practices" in establishing and maintaining an effective IT school security system.* A regular system of security maintenance should be established, including the regular updating of operating systems and software, enforcement of password policies, disabling unnecessary services, installation and updating of antivirus software on a very frequent basis, and the use of intrusion detection systems and firewalls. Prevention is always the best cure.
- *Remaining on high alert.* IT operations administrators should be on high alert for the warning signs of hostile cyber activity. Frequent scanning of Internet logs and incoming and outgoing e-mail should be performed regularly, and any suspicious activity should be looked into and reported to the local authorities, if necessary. An emergency incident plan could be established as well, in case any system is temporarily or permanently disabled by a virus.

We have admittedly used some technical terms—such as firewalls—that require more detailed descriptions and explanations than space allows here. This whole area of viruses, worms, and network IT and CyberSecurity is an ever-changing area for IT professionals and a growing area of risk for managers at all levels.[7] Members of an organization's ERM group, as discussed in Chapter 5, should be aware of these risks and techniques to limit them.

IT AND EFFECTIVE ERM PROCESSES

IT processes play a significant role in the operations of any enterprise and certainly are a major factor when assessing and understanding relative risks. This chapter has highlighted only three broad IT areas of concern—the application development process, IT continuity plans, and malicious network and other programs—where an organization can face some significant IT risks. An ever-growing and ever-changing set of issues, IT processes can cause some significant risks to an enterprise.

It is perhaps unfortunate that the COSO ERM framework did not devote more guidance and standards to IT-related issues. The assumption was perhaps that IT is so pervasive in enterprise operations that there is no real need to make it a separate, detailed topic. However, to effectively understand the COSO ERM framework and to install an effective set of processes,

considerable detail and attention should be devoted to an organization's IT controls and processes.

NOTES

1. *Enterprise Risk Management—Integrated Framework,* Executive Summary Framework, September 2004, New York: OSO, p. 67.
2. "ERP Training Stinks," *CIO Magazine,* June, 1, 2000.
3. COSO ERM Executive Summary, p. 66.
4. Disaster Recovery Institute International, Falls Church, VA (www.dri.org).
5. "Technology on the Web," *Forbes,* March 29, 2004.
6. "To Catch Crooks, FBI Goes Global," *Wall Street Journal,* November 22, 2006.
7. There are numerous other sources of supporting information through the Web and various books to allow the professional to gain a greater understanding of some of these evolving and ever-changing issues. A good source for some excellent background material is the National Institute for Science and Technology (NIST). The NIST Web site, www.nist.gov, contains some excellent guides and checklists to help the IT specialist and general, non-IT manager to better understand some of the evolving risks and issues here.

12

ESTABLISHING AN EFFECTIVE RISK CULTURE

The senior officers and board members of an enterprise can all talk amongst themselves about the importance of launching some new enterprise-wide cultural approach or philosophical direction. That type of new approach, however, will not launch new products in the marketplace or open new facilities. It is a concept that will be just talk until it is properly communicated to and accepted by all stakeholders in the enterprise. The matter or issue must become part of the enterprise's "culture"; a concept that sounds good but is difficult to execute. Some enterprises, due to many frequent changes, have never been able to establish a recognized culture, while others have built enduring cultures over the years. For example, 3M Corporation has had a culture, going back to its earliest days, of encouraging innovation. A former president and chairman of the board, William L. McKnight, believed "management that is destructively critical when mistakes are made kills initiative. It is essential that we have many people with initiative if we are to continue to grow."[1] In other words, he guided his managers and staff to take risks and signaled that senior management would not be overly

critical if some initiatives failed. These kinds of words created a culture to innovate at 3M that has led the company over the years to develop many new and valuable products. An example would be 3M's introduction of Post-it® notes many years ago. They had developed a paste or adhesive that did not work particularly well, but 3M then turned it into a product that has become very common and profitable. In a similar manner, Chapter 5 talked about how Johnson & Johnson used their culture and corporate credo to help them through a major corporate decision crisis. In both examples, the companies' organizational culture moved them along in correct directions.

Culture refers to an organization's values, beliefs, and behaviors. In general, it forms the basis on which people interpret experiences and behave, individually and in groups. Enterprises with strong cultures generally achieve higher results because employees sustain focus on both *what* to do and *how* to do it. These same factors are also essential for building an effective risk management culture in an enterprise. Whether the CEO and board have indicated that the enterprise wants to grow rapidly and are willing to take necessary steps to get there or they have indicated a strategy of cautious steps for new ventures, they are describing their culture and outlining a high-level risk strategy. In order to get an organization operating in either manner, these concepts should be communicated to become part of the overall organizational culture. That is, if a rapid growth strategy is planned, managers and staff at all levels need to think and make decisions to help promote that rapid growth. They are building a culture of growth for the enterprise!

That same concept is necessary to build an effective *risk culture* in an enterprise. Based on the overall Committee of Sponsoring Organizations' enterprise risk management (COSO ERM) framework and the discussions on implementing it from

previous chapters, this chapter outlines some processes for implementing an effective risk culture in an organization. This should be a culture that reflects the appetite for risk that has been described and defined by senior management but should be followed by stakeholders at all levels.

FIRST STEPS TO LAUNCHING THE CULTURE—AN EXAMPLE

COSO ERM has all of the correct concepts for building a risk management culture, such as emphasizing that an enterprise needs to know and understand its appetite for risk. In embracing these concepts, an enterprise can take such steps as appointing a chief risk officer (CRO), as was discussed in Chapter 4, or by encouraging the information technology (IT) function to be more aware of risk-related issues in their systems development and IT security efforts, as discussed in Chapter 11. However, these general concepts and concerns must be clearly communicated and understood by all organization stakeholders, whether employees, vendors, or others. This can be a difficult concept for many. While there is usually a general understanding as to the meaning of the term *risk,* many will have problems translating these concepts in any greater level of detail or action plans. This idea of a risk awareness culture needs to be introduced.

A good concept or model for building an enterprise-wide risk culture can be found in the way some organizations launched ethics initiatives and cultures in the early to mid-1990s. As frequently happens in the United States and in worldwide business cycles, the early 1990s was a period when many began to question the business practices and ethics of some enterprises. The COSO internal control framework had just recently been launched, but COSO's call for "tone at the top" messages were perhaps not all that well understood. At the time, this author had a management position with a large U.S. retail organization's internal audit function, and had a major role in developing the ethics function for that organization. The manner in which that ethics function was launched and the steps to develop an ethics culture there can serve as a model for launching an effective risk culture.

In the early 1990s, this retail organization was caught with a serious rules violation. As part of their retail operations, the retailer had a large automobile repair operation attached to many of their stores. Both at these auto repair shops and throughout the stores, there had been strong pressure

at all levels to increase sales to build the business. While certainly not within the purview of this author's internal audit position and not directed by senior management, state regulators found in the early 1990s that some automotive repair shop employees were being strongly encouraged by their direct supervisors to sell fraudulent auto repairs to customers. This message evidently was along the lines of supervisors telling their automotive repair staffs, "Your sales goal this week is to sell ten new engine tune-up jobs, whether customers needed them or not." These employee directives boosted automotive repair sales, and no employees evidently protested, saying such directives were wrong or raising their concerns up through the ranks. State regulators subsequently discovered the scheme, caught some repair shops essentially "red-handed" with these phony repairs, and threatened to shut down the company's auto repair operations state by state.

The word of these events quickly flashed back to corporate headquarters. This author was then asked to step away from his position as internal audit director and to join a selected team under the general counsel to develop a corrective actions plan. Many remedial and corrective actions were quickly launched, but a major conclusion of the connective action team was that there were no real company "rules" at that time prohibiting these fraudulent repair actions, that the organization's existing employee code of conduct was viewed as just another never-updated piece of paper, and that some type of an ethics culture was needed. Steps were then initiated to start to build an ethics culture at that retail organization. These actions are similar to the steps that would be essential today to build an enterprise-wide risk culture. This author was personally involved with directing or helping to launch this ethics culture initiative with some of the following actions:

- *Developed and released a revised employee code of conduct.* Covering more than fictitious auto repairs, a revised set of code of conduct rules was developed, released, and communicated through strong educational programs. After strong CEO and other senior management endorsements, employees were asked to formally acknowledge that they had read these code-of-conduct rules, understood them, and would follow them.

- *Launched a strong program of ethics education.* Through company classes, articles in newsletters, posters, and ongoing communications from senior managers, the message to always "do the right thing" was communicated to all stakeholders. The idea was to reinforce the idea of being ethical into the culture of the organization.

- *Revised and rewrote many existing policies and procedures.* The discovery that there were no real rules against selling fictitious auto repairs led to an overall examination of the entire set of this organization's policies and procedures. Many were revised and processes, hopefully, were put in place to better review and communicate these "new rules" types of procedures.
- *Established a whistleblower program.* This whole chain of events might not have happened if there already had been some sort of process in place where an employee at any level could "blow the whistle" and report that some first-level supervisor was asking the employee to sell phony repairs. Such a whistleblower program or facility was launched.

Time passed, this author left that retail organization, and the company itself was taken over by another. However, for at least that period of time, the actions outlined above did a lot to launch an ethical culture in the enterprise described. One would hope these cultural efforts had at least stayed with some members of that organization as part of their ongoing culture.

The above outlines what it took to launch an ethics function and start an organizational culture in the mid-1990s and can provide a model for building a risk culture in the latter half of this decade since the introduction of COSO ERM in 2004. The concept of risk awareness and of having an organizational risk culture is perhaps too new for some. However, in addition to implementing COSO ERM at various levels and the strengthening of risk management processes in an enterprise, there will be some value for launching a risk management culture in today's enterprise.

PROMOTING THE CONCEPT OF ENTERPRISE RISK

In some respects, as has been discussed in other chapters, the term *risk management* has become almost too "trendy" at present. Some internal audit departments have changed the names of their operational reviews or compliance audits to *risk assessments,* and enterprise insurance departments are frequently now calling themselves the risk management department. Employees and other stakeholders often do not see any real differences in these functions beside their changes of name. The individual who came in to review department travel expense vouchers is still going through the same steps, whether their title is internal auditor or a risk assessor. In any event, the message in the operating department of the organization will still be something along the lines of, "Careful! The auditors are

here," despite the fact that they may have changed their names to risk assessors.

Perhaps a tough sell to begin, the concept and importance of risk management needs to be communicated and constantly promoted to all members of the enterprise. In a very subtle way, this idea of building a risk awareness culture is a bit more difficult than promoting an ethics culture, as discussed above. With ethics, it is often sufficient to encourage employees to "do the right thing" with a shared value that most understand enough of right and wrong to easily make decisions. Risk management too often involves some "shades of gray" concepts where an enterprise may have an appetite for either high or low levels of risk, and with stakeholder decisions based on that philosophy. The challenge for senior management is to communicate their risk management approach throughout the enterprise, and to encourage all stakeholders to build this into their collective culture.

Defining the Risk Management Philosophy

Boards of directors regularly make major decisions involving millions in resources and the business careers of many people. Nevertheless, it may be often more difficult for a typical board member to make a risk-based decision than it would be for the risk-based decisions of an IT project manager who is deciding whether to use some promising but untried new technology. The IT project manager often has a wide range of specific technology-based references handy, while the board member is making these decisions on a higher and often more abstract basis. This is where a mutual understanding of the enterprise risk culture is important! Similar to the manner in which we write the codes of conduct, discussed in Chapter 1, that should apply to all—whether senior officer or staff—an enterprise needs to clearly define its risk management philosophy in a manner that can be understood at all levels.

Chapter 5 discussed the roles and responsibilities of the CRO as well as materials for launching an ERM function; this chapter discusses some techniques and procedures for helping to launch a risk management culture within the enterprise. Whether it is words from the CEO or from other recognized authorities, an enterprise needs to communicate its risk culture message to all of its stakeholders.

Communicating a risk management philosophy can be difficult because there are always shades of variability in any enterprise's approach to managing its risks. A stated philosophy of "Don't engage in any risky business transactions," for example, just does not make sense, as virtually all business

transactions have some elements of risk. Management needs to carefully define and communicate their organization's risk management philosophy in a manner that can be clearly understood by all stakeholders. Prior chapters have discussed the steps necessary to build an effective ERM function and to integrate it into other functions, such as Sarbanes-Oxley (SOx) review procedures and IT project management, but an enterprise needs also to develop a clear statement of its risk management philosophy that can be communicated throughout the enterprise. Properly executed, this will become a keystone element in building, or at least launching, an ERM culture. Using the Global Computer Products example company, Exhibit 12.1 is a sample ERM philosophy statement.

In many respects, drafting such a formal ERM philosophy statement is similar to developing any high-level statement, such as a management objective or a code of conduct. We began this chapter with a description of this author's role in launching an ethics initiative or cultural movement in a large U.S. organization. In addition to all of the other approaches used to introduce the idea of always considering "ethics" to that organization were a series of ongoing messages on the importance of this initiative from the CEO and other senior managers. This is the "tone at the top" idea that is emphasized in both the discussions of the COSO ERM and COSO internal control frameworks.

Global Computer Products

Our Risk Management Philosophy

Risk management is not just a process or procedure. It is a fundamental component of Global Computer Products' business. Our company is dedicated to keeping risk management as a key component of all of our business dealings.

We believe that risk management is first and foremost the responsibility of all associates, including management up to the most senior level. Just as a successful business must manage its costs, it must manage its risks. This includes hazard risk, financial risk, and credit risk.

The management of risks must be incorporated into the fiber of our organization. All associates must consider potential risks as they make all decisions, whether in sales, product development, or other areas of operations.

EXHIBIT 12.1 RISK MANAGEMENT PHILOSOPHY: GLOBAL COMPUTER PRODUCTS

In a precise and explicit manner, these statements and messages must express a risk management philosophy in a clear and succinct manner. Depending on the talents and skills within the enterprise, drafting such published statements may require the talents and skills of specialized people in the organization or through outside contracted help. Considerable care must be given to the nature of the message in that philosophy. It must emphasize that there are risks associated with all business transactions and that stakeholders must make decisions that are consistent with the enterprise's risk philosophy.

Much more than just a published statement of philosophy is needed to initiate and build any type of organization/stakeholder culture. The statement of philosophy can too easily become just another "nice-sounding" set of words. Stakeholders need to understand any such statement and to take active steps to implement it in their day-to-day business activities. They need to understand that all activities involve some risks, but their activities should be consistent with that philosophy. The Global Computer Products statement in Exhibit 12.1 describes a philosophy of accepting a moderate level of risk in order to grow, but taking only small and not totally bold steps when faced with making decisions in riskier areas.

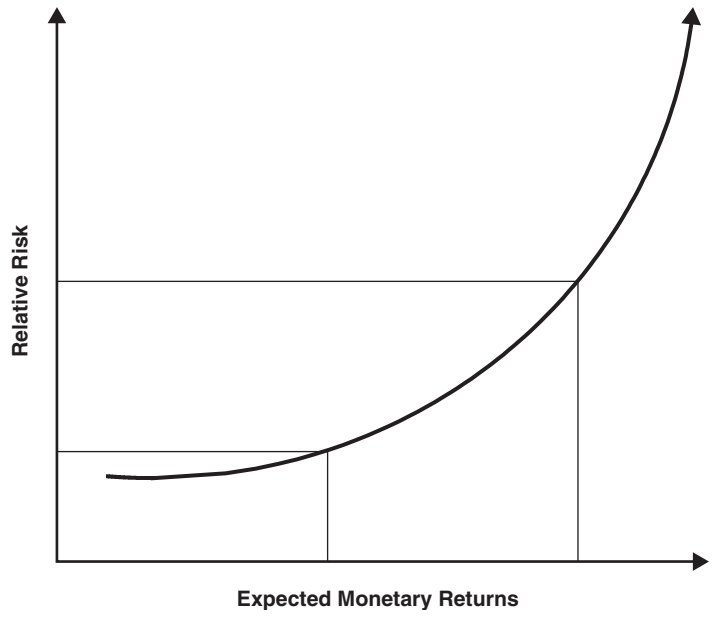

EXHIBIT 12.2 SPECTRUM OF RISK MANAGEMENT PHILOSOPHIES

A risk management philosophy can bridge the entire spectrum of always taking very conservative approaches and minimizing most risks, to being as aggressive as possible despite the potential risks. Most enterprises are somewhere within these two extremes, and senior management always needs to communicate this high-level risk philosophy to all stakeholders. Exhibit 12.2 shows this spectrum of risk versus expected return management philosophies. Increasing relative risks by a small degree on the vertical scale will provide a satisfying level of increased returns on the horizontal scale. However, to move out even further on the horizontal scale causes the relative risks to go up and up. This trade-off chart encompasses more than just accepting higher- or lower-risk projects and includes such areas as attitudes regarding internal control procedures. That is, an enterprise that has installed very tight approval limits on spending transactions or authorizations can be viewed as more of an organization concerned about limiting risks.

Translating a Risk Philosophy into a Culture

Statements by the CEO at the annual meeting or resolutions passed by a board risk committee will do little to build a risk culture in an enterprise unless all stakeholders know and understand that philosophy. 3M Corporation, mentioned earlier, is a good example of a company where stakeholders at all levels are encouraged to try new products or ventures to build the business. Not every new venture works, but the team there has evidently been encouraged over the years to take some prudent risks in order to encourage strong growth patterns. Although we are not part of the inner workings of that corporation, this appears to be an environment where some risk is tolerated in order to achieve growth.

The challenge on the Exhibit 12.2 low-to-high-risk spectrum is not to go too far! Perhaps a good example of an enterprise that got far too involved in high-risk business ventures is the now defunct corporation that had a lot to do with launching SOx in the United States—Enron. In the years until its total collapse in about 2002, Enron had a very strong growth record and was viewed by the investment community as an aggressive, innovative, and risk-taking organization.[2] From at least published accounts, as Enron grew over the late 1990s, employees were encouraged to take on ever more risky business ventures to pursue strong growth objectives. While key employees were lavishly rewarded for their entrepreneurial business ventures and stockholders were happy with the ever-increasing market prices, some employees or other stakeholders engaged in side deals to keep growth moving up as well as to benefit themselves. Investment markets then became concerned and put a little bit of a

squeeze on the company. The "house of cards" that was Enron's financial structure then quickly fell; Enron went into bankruptcy; their once prominent external auditors, Arthur Andersen, failed as well; and SOx became law.

Going over business history over the years, Enron is certainly not the first high-growth, highly aggressive corporation to suddenly fail, but it introduces a case where too much of a high-risk culture is usually not good. There are numerous examples of enterprises that were too concerned about taking on risks. The typical result is that the very conservative, low-risk enterprise sat on the sidelines as its competitors grew ever stronger. Both of these extremes of very high or very low-risk approaches are the results of fairly deliberate management strategies that are understood by stakeholders. In order to establish an appropriate enterprise risk culture, some action items include:

- *Repeat higher-risk or lower-risk strategies in all business communications.* Just a message along the lines of "XYZ Corp. promotes good conservative business practices," should get stakeholders thinking as they engage in transactions.
- *Clearly reward people for making appropriate risk-based decisions.* Whether it is a thank you to a manager of a new product venture that looked good but did not take off or accolades for the originator of new control procedures, persons should be recognized for taking the right risk-based decisions.
- Constantly remind stakeholders to always make decisions or operate in a manner consistent with ERM policies, procedures, and *philosophies*. We have emphasized the latter word here, as this is a major step to building a culture. Specific procedures can never cover all details and situations, but a high-level understanding of risk alternatives and approaches will often fill in the details.

The goal of building any risk management culture in an enterprise is to expect employees and other stakeholders to almost automatically react to risk-based decisions with responses along the lines of, "We're XYZ Corp. and wouldn't want to get involved in that kind of transaction" or "Your proposal sounds very interesting and appears to be a good fit with our operations." Either of these responses are the sort of automatic words that will come from an organization that has a strong risk management culture that is known and understood by all of its stakeholders. Basic to this concept, however, all members of the enterprise should try to look at all ventures with an added perspective of considerations of relative risks in addition to

just the quantitative go or no-go decision processes so common today. That is, even though a calculated number for an estimated return on investment (ROI) may look good as part of a financial analysis process, a risk-sensitive culture will or should always look at the same set of estimates from a perspective of considering any potential risks associated with that investment decision. An enterprise has established an effective risk management culture when persons at all levels can look at alternatives and effectively say "This does not smell right!"

BUILDING THE COSO ERM CULTURE: RISK-RELATED EDUCATION PROGRAMS

Beyond strong messages, an appreciation of risk management should be communicated through ongoing training programs. New stakeholders at all levels should have an opportunity to learn that their organization faces risks at all levels, but that they are expected to take appropriate actions to consider those risks and to install corrective actions to guard against them. While many enterprises are not large enough nor have the time and resources to develop specialized risk management training materials, the message of the enterprise's risk management culture can be folded into other training materials covering other areas.

The COSO ERM framework is elegant and instructive, as has been discussed in previous chapters. However, we are not suggesting an educational program based on just that framework. Rather, the idea of any risk assessment educational materials should be to introduce and reinforce the importance of making decisions consistent with that risk philosophy at all levels. A general program introducing the enterprise's risk management approach and the importance of always considering relative risks should be launched. Exhibit 12.3 is an outline for an "understanding risk management" session that could be delivered as part of continuing education offerings for an enterprise such as the Global Computer Products example company. Time is important, and such a session would perhaps be limited to perhaps 30 minutes of a Web-driven session or perhaps longer with some audio beyond just the text.

Perhaps more important than just a pure "understanding risk management" session, an enterprise should take steps to introduce risk-related consideration in all of its continuing education offerings. Exhibit 12.4 is an example of a class slide for a session on establishing effective internal controls for new department processes. This foil outlines rules for fixed-asset request form procedures and highlights such matters as the need to check

Global Computer Products

Understanding Risk Management

Continuing Education Course Outline

This Web-based risk training will be offered to all members of the Global team.

1. Introduction to enterprise risk management
   a. Global's risk management philosophy and a message from the CEO
   b. The COSO ERM framework and how it fits
2. The risk management team and your ongoing responsibilities
   a. Significant new risk-based policies and procedures
   b. The Global risk team—the CRO and others
3. Your company's periodic risk assessment process
   a. Updating periodic risk inventories: Updating existing risks and identifying new risks
   b. Responding and reacting to risk assessment reports
4. Steps for identifying potential new risk concerns
5. Building risk remediation strategies into your regular business processes
6. Case study: Considering risks in new product planning

EXHIBIT 12.3 UNDERSTANDING RISK MANAGEMENT COURSE OUTLINE

vendor references. The purpose of this sample PowerPoint slide is not to show good internal control techniques but to introduce the concept of always considering risk issues in any relevant area of an organization's continuing educational offerings. The constant reinforcement of a message to always consider risks will very much help to build an appreciation for risk management into an organization's culture.

KEEPING THE RISK CULTURE CURRENT

Enterprise initiatives too often have only short-term effects that can be quickly forgotten as periods go by or as the enterprise leadership changes. Exhibit 12.1 described a high-level risk philosophy for an enterprise. Such a philosophy would be communicated through statements by the CEO, messages in training materials, and through other sources. Some words in it should remain constant from year to year, with no need for revisions.

Global Computer Products

Fixed-Asset Request Form Procedures

1. Check supplier references and reverify estimates.
2. Calculate rate of return based on vendor estimates.
3. Reassess inherent risks of installing new fixed asset.
4. Determine if estimated risks are within company's risk criteria.
5. Assess whether estimated rate of return is greater than company standards.
6. If fixed-asset rate of return or estimated risk ranking does not meet standards, reject fixed-asset request proposal.

This is an example of combining risk assessments with other procedures

EXHIBIT 12.4 INTEGRATING RISK MANAGEMENT WITH OTHER BUSINESS PROCEDURES

However, such a statement and all of its related supporting materials should be reviewed and reexamined on a regular basis.

The CRO or, if such a risk officer position has not been established, another appropriate senior member of the enterprise management team, should review existing risk management guidance materials on a regular basis and make appropriate changes to keep the both current and fresh looking. Once established, that risk culture will stay and mature with various elements of the enterprise. However, new people arrive and business conditions change. The risk culture of the enterprise must be continually reexamined and refreshed.

NOTES

1. www.ideafinder.com/features/century/3m.htm.
2. The story of the fall of Enron has been told in many publications. A good account can be found in Kurt Eichenwald, *Conspiracy of Fools: A True Story.* New York: Broadway Books, 2005.

13

ERM Worldwide

As discussed in Chapter 3, when the Committee of Sponsoring Organizations' enterprise risk management (COSO ERM) first appeared as a draft document, many U.S.-based professionals initially tended to think of it as an extension of the COSO internal control framework. Even today, some professionals still refer to COSO ERM as COSO #2, with little recognition of its unique objectives. For many, there initially was not that much appreciation of this newer term—*enterprise risk management.* As many other professionals become familiar with COSO ERM today, there is a growing appreciation of that framework and some recognition that it may evolve into a standard in the United States, just as COSO internal controls have become that level of a now recognized standard. While COSO internal controls have created a new set of internal control standards—first in the United States and now worldwide—COSO ERM is not the first or necessarily the only defining standard for ERM. There is a need to look at ERM from a worldwide perspective.

Although there have been many approaches and definitions of risk management, national "standards" on risk management first appeared in Australia and New Zealand in 1995, Canada in 1997, and the United Kingdom in 2000. Other countries and

regions, such as the European Union (EU) are currently studying similar standards, and the International Organization for Standardization (ISO) has drafted a list of common global definitions for risk management terms, and international accounting standards have been released for risk standards and for some risk management financial reporting procedures. There is a growing recognition of the need for a worldwide risk management standard, and ERM is becoming a major influencing factor here.

This chapter will briefly look at COSO ERM from this worldwide perspective and will focus on other global risk management standards to examine how they compare with the COSO ERM framework. While many U.S.-based professionals are primarily familiar with American standards and guidelines, and while the United States remains the dominant world power in economics and business today, other countries and areas—such as the EU—have strong needs and concerns to develop standards and procedures that are consistent with their own views of businesses at national and international levels. ERM procedures are a key component in this understanding.

ERM "STANDARDS" VERSUS AN ERM FRAMEWORK

For many, the terms *standard* and framework sound to be just about the same thing. The COSO ERM framework outlines an overall model to help an organization to better understand and manage its risks. However, there are no specific requirements here, and the idea of a framework only provides some broad guidelines. The idea of the "tone at the top" messages from the CEO and other senior managers is an example of this idea of a framework or guideline. Even though an individual CEO may not communicate these messages through speaking in front of key employees or in published reports, such a "tone at the top" message can still be communicated through other means, such as communicating a strong management philosophy that appears to be the message from the CEO. A standard is

more precise. In order to comply with a "tone at the top" standard, a reviewer or evaluator would tend to look for specific communications from the CEO.

Outside of the United States, the tendency is more to use identified and recognized standards rather than the more loosely defined framework guidelines. The set of ISO international standards includes some documents that are only defined as ISO "guidelines" while others are specific document-level ISO "standards." The approach in the United States can be better demonstrated by the accounting term of generally accepted accounting principles (GAAP). An enterprise is not required to use GAAP rules, but virtually all do and they must be able to demonstrate to their external auditors and the Securities and Exchange Commission (SEC) why they have chosen to follow any different non-GAAP path. Although not at all common, some business units have a need to follow somewhat non-GAAP procedures. Another reason for this split between guidelines—such as GAAP—and standards is the litigation atmosphere in the United States. If an enterprise does not follow a standard, and particularly a published standard, they could easily become more subject to litigation.

There are many other risk management fine points here, but the following sections introduce risk management "standards" that were released prior to COSO ERM first in Australia/New Zealand, then Canada, and later the United Kingdom. We will also look at some other national risk management standards, the risk-related components of the International Federation of Accountants (IFAC) internal accounting standards and work to date from ISO.

Risk Management Guidelines in Australia and New Zealand

People in the northern hemispheres of the world, such as the United States and Canada or in Europe, too often think of faraway Australia and New Zealand as just that—far distant locations where businesses are not conducted with the same high standards and intensity found on the other side of the equator. This assessment is certainly wrong, and Australia and New Zealand have taken a lead on establishing risk management standards that have become a model for others to follow. Two separate and distant independent countries, Australia and New Zealand, frequently collaborate on various policies, rules, and standards. Well ahead of countries to the north, a project was initiated there in 1993 to develop risk management standards. Although the document has been regularly updated, the risk management standards for Australia and New Zealand were first released in 1995 with

their current, latest updated edition dated 2004.[1] The stated objective of these standards was to create a "generic framework" for the risk management discipline and an "iterative process consisting of well-defined steps" to "support better decision making." Perhaps well ahead of its time when compared to other standards, the standard allows that risk management should be "an integral part of good management practice" and should become "part of an organization's culture."

This standard is divided into five sections: (1) scope, application, and definitions; (2) risk management requirements; (3) risk management overview; (4) risk management process; and (5) documentation; and it continues to provide excellent guidance on risk management. Originally published at a time when there were essentially no standards for ERM outside of perhaps the insurance industry, the New Zealand/Australia standard provided a variety of process definitions. In a time frame when risk management often tended to be just an insurance department function, this standard provides some ERM-like definitions. For example, *risk* is defined as "the chance of something happening that will have an impact upon management or organizational objectives," measured in terms of consequence and likelihood. This standard also defines the "context" of risk management broadly, including "financial, operational, competitive, political (public perceptions/image), social, client, cultural, and legal aspects of the organization's functions." The standard brings us closer to the enterprise model and framework that was introduced in Chapter 3.

These standards are supported by a set of published *Risk Management Guidelines* that discuss many aspects of the discipline, from an Australian and New Zealand perspective, for a wide range of organizations including:

- Public-sector entities at national, regional, and local levels
- Commercial enterprises, including companies, joint ventures, firms, and franchises
- Partnerships and sole practices
- Nongovernment organizations
- Voluntary organizations such as charities, social groupings, and sporting clubs

This risk guideline also provides some risk management guidance for directors, elected officials, chief executive officers (CEOs), senior executives, line managers, and staff when any or all are developing processes, systems, and techniques for managing risk that are appropriate to the

context of their organization or their roles. These standards take a broad view of ERM and cover virtually all entities.

This Australian and New Zealand standard was an important first step in establishing worldwide risk management standards and almost certainly got others, such as Canada and the United Kingdom, thinking about standards publishing in this area. With additional input since its initial publication from risk managers, teaching institutions, and organizations such as the Institute for Risk Management in the United Kingdom, the Center for Risk Management in Washington, DC and the Insurance Institute of America in Philadelphia, PA may have started the thinking about ERM in the United States. While we do not have any direct evidence here, this standard was almost certainly an influence on the content and even development of COSO ERM.

Canadian Risk Management Guidelines

Accounting, auditing, and internal control standards in Canada often seem to follow their neighbor across the border to the south. For risk management, however, Canada followed Australia and New Zealand and was ahead of the United States when the Canadian Standards Association (CSA) published its "guideline" on risk management in 1997.[2] This Canadian standard is perhaps more of a public policy document discussing risk than it is a financial or operational risk management guide, but it emphasized the importance of risk management to professionals in Canada.

This CSA standard defines risk as having "three key issues": (1) the frequency, (2) the consequences, and (3) the perception of loss. This concept of a "concern for the public perception of risk" is rather different than anything in the COSO ERM framework. The guideline has a thorough discussion on how public perceptions of risk are often far more important than just probabilistic estimates. There is a good discussion of public perceptions of risk including the loss of personal control, the potential for a catastrophe, and the distribution of risks and benefits. The guideline also focuses on how risk affects all stakeholders, and it emphasizes the importance of communications among stakeholders in the process of seeking responses.

Going beyond the role of the chief risk officer (CRO) introduced here in Chapter 5, the Canadian guidelines recommend the creation of a "risk management team," a multidisciplinary group of internal and external experts, plus perhaps some stakeholder representatives, to address the major risk issues facing an organization. It suggests creating a "risk information library" that includes documentation of issues, scope of decisions,

identification of roles and responsibilities, identification of decision makers, details of analyses, stakeholder responses, and support documentation for decisions. In addition to this documentation repository, the standard suggests "third-party reviews" to confirm the integrity of an enterprise's risk management analysis process and its actual risk management decisions. This is an interesting concept or suggestion. The guideline calls for perhaps the CRO or the board risk committee—it does not really specify whom—to have outside reviewers periodically look at an enterprise's risk management processes, perhaps along the lines of the annual financial audit. This is an interesting concept, but there certainly are needs for more generally accepted review standards here.

While this Canadian risk management standard contains a wealth of guidance on risk management concerns, it is perhaps too much of a government-like public policy document than specific business guidance. It is really lacking a complete overview of risk management, including financial and operational aspects, and does not at all focus on risk management from the perspective of the COSO ERM framework. Released well before COSO ERM, the Canadian guidelines very much highlighted the importance of risk management for North American enterprises and remain a useful supplement to the COSO ERM framework.

British Risk Management Standards

In historic times, the course of the British Empire moved westward, but the course of risk management standards, however, appears to have been in reverse. As discussed, the first national risk management standard was created by New Zealand and Australia in 1995, followed by the Canadian risk management standards in 1997; the British published their standard in the year 2000, *Project Management, Part 3: Guide to the Management of Business Related Project Risk.*[3] Although the title implies just project management guidance as opposed to an emphasis on overall enterprise risks, this standard describes risk management as "a core process within any business or organization, regardless of size, activity, or sector" that "can make a significant contribution to the economic and general welfare of society." Arguing that "it is rare for all risks to be identified and taken into account systematically in the early stages of planning," this standard very much defines a process for identifying, assessing, and controlling risks within a broad framework. Although the focus of this U.K. standard is on projects, the material in the standard reminds the reader that projects are "the principal means by which a business moves forward."

The British risk management framework contains sections for identifying risk, risk analysis, risk evaluation, and risk treatment. It contains definitions that are often fairly wordy, but it provides strong guidance on risk management. An example here is its definition of risk management as "the systematic application of policies, procedures, methods, and practices to the tasks of identifying, analyzing, evaluating, treating and monitoring risk." While called a "concise definition," it is much too wordy for the CEO to use in a public forum when asked a pertinent question. The standard document also includes an appendix section with a description of multiple risk management and analytical tools, including assumptions analysis, brainstorming, checklists, criticality analysis, cumulative frequency plots, decision analysis, Delphi technique, expert interviews, event tree analysis, fault tree analysis, something called HAZOP studies, influence diagrams, Monte Carlo simulation, prompt lists, risk registers, databases, and sensitivity analysis. This is almost too much and too technical for the typical risk manager in an enterprise. We have touched on some of these topics in our Chapter 2, but not even to the extent of the appendix to this standard.

Beyond the published British standard, the supporting British Standards Institutes had published a wide range of risk management guidance documents in a Web format. Risk management there is covered through their RM/1, the e-committee site for the BSI committee working on risk management. Supported by numerous technical papers, this *www.bsi-global.com* site has a risk management objective, as follows:

- To formulate a U.K. strategy for standardization in risk management through a broad consultation with relevant stakeholders
- To ensure that the U.K. view influences the European Union and the ISO Working Group for risk management
- To develop and support formal standards and other standardization documents in the area of risk management and to promote their use by industry and other potential users
- To ensure due consideration of the need for standards and standardization is given by U.K. risk management networks and organizations, and to coordinate activities and actions in this area

The second bullet point is important here, as U.K. risk management standards have essentially set an ERM standard for the EU and for many other countries in the world, beyond the United States.

Beyond the United Kingdom: The FERMA Risk Management Standards

British risk management standards have been translated into a set of common standards for use throughout the EU as well as for other interested countries such as China and Saudi Arabia. These common British risk management standards have been promoted and communicated through the international organization Federation of European Risk Management Associations (FERMA).[4] A professional organization of some 20 national risk management organizations, FERMA has adopted the 2002 British risk management standard. Versions have been published in multiple languages of this pan-European standard of best practices in risk management. The FERMA risk management standard sets out a strategic process, starting with an organization's overall objectives and aspirations, through the identification, evaluation, and mitigation of risk, and finally the transfer of some of that risk to an insurer.

Based on the British model, FERMA uses a diagram, as shown in Exhibit 13.1, to illustrate its risk management model or framework. Many of the elements here, from risk assessments to risk monitoring, are similar to one side of the COSO ERM framework, but the model does not have the multidimensional enterprise-level perspective found in COSO ERM. There are also some elements or terminology in this model that are not found in the COSO ERM descriptions of previous chapters. For example, there is a framework layer called *risk treatment*, the process of selecting and implementing measures to modify the risk. Risk treatment includes as its major element risk control/mitigation, but extends further to, for example, risk avoidance, risk transfer, and risk financing. Another very worthwhile aspect of the British and FERMA international risk model standard is that every element is formally set up as being subject to audit. This is much broader than the role of audit in ERM, as discussed in Chapter 9, but has some attractive attributes.

Our objective here is not to analyze differences between this FERMA risk management framework and COSO ERM but to highlight that similar perspectives and approaches are used on essentially a worldwide basis. Perhaps a major difference with the FERMA and other risk management standards described in this section and the COSO ERM model is that these other international standards have been developed and are used from more of an insurance industry perspective, while the discussion of risk management in other chapters of this book has been on the management of risks within the business enterprise and all of its operating units. As risk management standards move

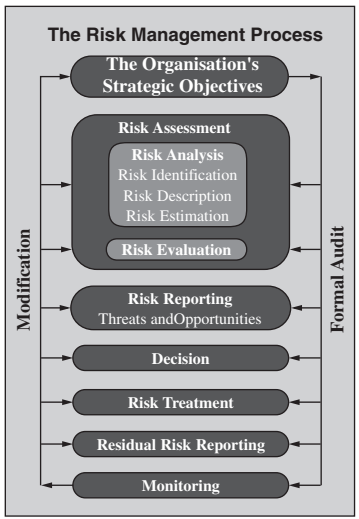

EXHIBIT 13.1 FERMA RISK MANAGEMENT PROCESS STANDARDS

worldwide to more of an enterprise or business management tool, there will almost certainly be changes in the risk management model perspective.

ERM AND ISO

We live in a world of an increasing number of global standards, with many of them published by ISO in Geneva, Switzerland. These standards appear as lengthy numbers in many business documents, such as ISO 9001 for quality management systems. Each of these standards is lengthy, detailed, and very precise. However, if an enterprise wants to hold itself out as having, for example, effective quality management systems in its processes, it will go through the procedure of practicing and documenting its compliance with that ISO standard. As a final step, a certified outside reviewer would periodically be contracted to review and certify the enterprise's compliance to that standard. Once certified, the enterprise can advertise to the outside world that they do have an effective process in place that meets a specific ISO standard, such as this ISO 9001 quality management standard.

ISO standards cover a wide variety of areas. Some are very broad, such as ISO 14001, covering effective environmental control systems, while others are very detailed and precise such as standards covering details such as the size and thickness of a plastic credit card. Just as the broad standards are important so that all enterprises are talking the same language about what constitutes an effective quality management system, the detailed ones are also very critical so that an automated teller machine anywhere in the world will expect to receive the same type and thickness of credit card.

Because numerous international governmental authorities, professional groups, and individual experts are involved in such a standard-setting process, the process of building any ISO document typically is a long and slow process. An expert committee develops an initial draft standard covering some area, the draft is sent out for review and comment with a specified comments due date, and the committee then goes back to review draft comments before either issuing the new standard or sending a revised draft out for another round of review and suggested changes.

At the time that this book is being published, there currently is no ISO standard for risk management. A draft standard, "Risk Management–Guidelines for Principles and Implementation of Risk Management"—was released for comment in late December 2005, and a final version of that standard has not yet been released as we begin 2007. While certainly not a tutorial on risk management, the draft now in process has objectives to establish a terminology that will achieve a consensus among worldwide

risk management practitioners. While it is still in draft format and subject to change, the words in the draft point to a common recognized acceptance of risk management practices going forward, with the ISO draft comments:

> Risk management touches all of the organization's activities. It is the foundation of the control environment and sound corporate governance. The implementation of an effective risk management process achieves a more confident and rigorous basis for decision making and planning, including:
>
> Better identification of opportunities and threats;
>
> More effective strategic and operational planning with established linkages;
>
> Greater confidence in achieving planned operational and strategic objectives;
>
> Enhanced organizational resilience that reduces the time lost on 'fighting fires,' and improves the organization's potential to exploit opportunities;
>
> Gaining value from uncertainty and variability;
>
> Pro-active rather than re-active management;
>
> More effective allocation and use of resources;
>
> Improvement in interested parties' confidence and trust;
>
> Improved compliance with relevant legislation;
>
> Better corporate governance;
>
> Risk management is a key business process within both the private and public sectors around the world.

These ISO draft comments have been extracted from portions of the introduction of this draft ISO risk management standard. As the document becomes official and is circulated worldwide, the overall level of attention given to COSO ERM can only be expected to increase. Based on a cursory review of the current draft ISO risk management standard, however, there also appears to be little that will be in conflict with the COSO ERM framework.

Impacts and Influences of International Accounting Standards

Accounting standards are rules that enterprises use to record business transactions and to report on those results. They cover a variety of day-to-day business as well as more complex issues. An example would be: When should a business record a sale—when a contract is signed with no product delivery or payment, after all steps in the transaction have been completed, or at some intermediate steps? The whole idea here is that everyone should account for similar transactions in a like manner. They should follow consistent accounting standards. These standards have evolved over the years on a

country-by-country basis. France, for example, once had slightly different accounting standards than did Germany. In the United States, these standards have been set by the very independent Financial Accounting Standards Board (FASB) with a historical connection to the American Institute of Certified Public Accountants (AICPA). Because of size and economic power, U.S. accounting standards have been a major driver in this process, even though other countries in the past kept their own standards and rules.

First with the establishment of the EU, and now as we move more toward a global economy, there is a recognized need for common, consistent standards in many areas, and particularly in accounting. The international federation of accountants (IFAC) has established accounting standards that apply to most of the world, with the exception of the United States. Over time, these differences between U.S. and IFAC accounting standards are getting resolved, with the hopeful objective of one worldwide set of accounting standards. Although we have discussed the Australian and British risk management "standards," ERM procedures do not lend themselves to the same type of rules as would be found in accounting procedures. As discussed in earlier chapters, COSO ERM is a framework or a model for an enterprise to build its own specific rules and procedures. A search for "enterprise risk management" on either the AICPA or the IFAC Web site brings up references to the COSO ERM framework.

Any differences between the U.S. and international sources are more on the level of guidance on how to use and implement COSO ERM. While the AICPA has some guidance materials on how CPAs should build effective risk management processes, IFAC appears to have even more. An example of the IFAC material is the publication "Enhancing Shareholder Wealth by Better Managing Business Risk."[5] This 1999 publication, predating COSO ERM, contains very similar guidance materials, and was drafted by PricewaterhouseCoopers (PwC) under contract from IFAC. PwC was also the contractor that took the lead role in developing the COSO ERM framework. Going forward and based on materials listed on their respective Web sites, it appears that international accounting guidance, under IFAC, will also follow COSO ERM.

CONVERGENCE OF RISK MANAGEMENT STANDARDS AND PRACTICES

With risk management standards first published for Australia in 1999 and then moving across the world, the COSO ERM framework, and now the soon-to-be-released ISO guidance on risk management, there appears to be

a growing need to have a worldwide consistent level of standards and practices for ERM. Standards are one thing, but there also is a growing implementation of risk management practices by major corporations worldwide.

NOTES

1. AS/NZS 4360:2004 Risk Management, Standards Australia, Sydney, NSW 2001, Australia, or Standards New Zealand, Wellington 6020, New Zealand.
2. *Risk Management: Guideline for Decision-Makers, A National Standard for Canada*, Canadian Standards Association, # CAN/CSA-Q850-97 (October 1997), Etobicoke, Ontario M9W 1R3, Canada.
3. BS 6079-3:2000, British Standards Institute, www.bsi.org.uk.
4. Institute of Risk Management, www.theirm.org/index.html.
5. International Federation of Accountants, New York, 1999.

14

COSO ERM Going Forward

The preceding chapters in this book have attempted to introduce the Committee of Sponsoring Organizations' enterprise risk management (COSO ERM) to a wide range of people in today's enterprises, whether a public corporation, private company, or a not-for-profit business. The focus was on a wide range of professionals including members of the board of directors, senior management, internal audit, and many information technology (IT) professionals. After existing in a published draft form for some time, COSO ERM became "official" in very late 2004. While the prior chapters of this book talked about the importance of COSO ERM as a framework to help better manage and understand enterprise risks, what will happen next is always an unknown.

Using the model of the COSO internal controls framework as well as the current interest in risk management issues in many areas, this final chapter will speculate on where ERM will perhaps be moving in future years. Future speculation is always a difficult guess, but given the continuing trends in improved corporate governance and internal controls, there appears to be a growing interest and concern with the COSO ERM framework.

FUTURE PROSPECT FOR COSO ERM

A possible direction of where COSO ERM may be going can be taken from its namesake, the COSO internal controls framework. As discussed in Chapter 3, the first COSO internal control framework report was released in 1992,[1] but at first the report did not receive much enterprise-wide attention beyond the internal audit and public accounting communities. The COSO internal controls three-dimensional framework, as shown in Exhibit 1.1, may have even thrown off some professionals, and it remained an elegant but interesting approach to evaluating internal controls. The framework crept into public accounting's auditing standards, but the framework was not given any strong, official support until recognized as the approved internal control standard with the Sarbanes-Oxley Act (SOx) in 2002.

As perhaps a lesson that can be used for ERM, this really says that it had taken COSO internal controls some ten years to get the sort of full recognition that might have been expected when that framework was first published. Even today, there are evidently many in business that still do not understand or know how to use this internal controls framework. For example, as this book moves to publication, COSO has announced it is seeking a consultant to develop guidance designed to help organizations monitor the quality of their COSO internal control systems. The requested end product here is expected to serve as a tool for effectively monitoring internal controls, as well as complying with associated aspects of SOx. To quote the COSO chairman, Larry Rittenberg, PhD, as part of this COSO guidance project request for proposal, "There is a tremendous gap between the value good monitoring brings to a system of internal control and management's understanding of that value."

With its still evolving ten years that it has taken COSO internal controls to become more fully recognized, one might ask if this will be the fate of ERM as well. We think not. For a series of reasons as described below, COSO ERM is becoming, or will soon become, a much more important tool and will see a much faster adoption than COSO internal controls' ten years of not seeing many actual implementations:

- *COSO internal controls were really launched before the pervasive use of Internet technology and applications.* The Internet was certainly with us in the early 1990s when COSO internal controls first appeared, but it did not at all have the pervasive presence that we find today. Beyond COSO itself, professional organizations such as the Institute of Internal Auditors (IIA) or consulting firms, such as

Protiviti, have published excellent Web-accessible guidance materials on ERM.

- *Because of the internal controls framework model, ERM is easier to understand and use.* The three-dimensional COSO internal controls framework was elegant and certainly caused many to ask, "That's really correct! Why didn't I ever think of internal controls in this manner, and how can I use this?" The ERM framework will almost certainly be understood and accepted much more quickly.
- *Risk has become a much more accepted concept almost worldwide.* It may be because of the 9/11 World Trade Center act of terrorism in the United States or more recent acts of terrorism in Madrid, London, and elsewhere, but the threat or *risk* of acts of terrorism are around us. Although ERM controls are not at all related to "War on Terrorism" issues, these types of events have many thinking more about risks and risk management.
- *COSO ERM concerns and impacts people beyond the executive offices and boardroom.* Many have thought the concern for internal controls was more of an accountants' and auditors' issue and that it did not affect them. While certainly not true, internal controls remain a "do the debits equal the credits?" type of concerns by many outside of the controller's and other accounting offices. ERM is more pervasive. Whether a marketing manager developing a sales strategy or an IT professional considering a new technology, many people in the enterprise should have a concern and appreciation for risk management.

The above may or may not be correct but will not be the only reasons why COSO ERM is adopted. We are suggesting a trend here and believe there should be a greater appreciation for ERM issues in the years going forward.

ERM provides an organization with the processes it needs to become more anticipatory and effective at evaluating, embracing, and managing the uncertainties it faces as it creates sustainable value for stakeholders. It helps an organization manage its risks to protect and enhance enterprise value in three ways. First, it helps to establish a competitive advantage. Second, it optimizes the cost of managing risk. Third, it helps management improve business performance. COSO ERM contributes to an organization through the elevation of risk management to a strategic level by broadening the application and focus of the risk management process to *all* sources of value, not just physical and financial ones.

COSO ERM AND ISO

In many respects, the draft risk management International Organization for Standardization (ISO) guidelines highlighted in Chapter 13 may be a very significant predictor of where ERM may be going in future years. Many in audit and financial fields miss the importance of the ISO guidelines, but in areas or disciplines where they have been launched, they can very much change industry attitudes and profession practices. The development and release of these ISO standards is a slow, almost ponderous process requiring extensive levels of documented controls and procedures. However, it is a process that can have strong benefits to enterprises that adopt these standards. The status of ISO 9000 quality management standards and the actions of the American Society for Quality (ASQ, www.asq.org.) might provide an example of how things evolve over time.

Quality control has been a series of manufacturing processes that essentially evolved out of the high-production factories during World War II in the United States and United Kingdom. In addition to pure manufacturing to produce error-free components and parts, processes were developed to measure production rates and to quickly adjust things if something got out of line in the assembly plant. The monitoring and measuring processes here were particularly important for high-production, assembly-line operations involving many manual steps. Within the United States, the ASQ, under its earlier name of American Society for Quality Control, played a leading role in setting standards and promoting best practices.

In the late 1940s, manufacturing processes become much more complex and automated. While there still was a need for quality control, the focus grew to much more of an emphasis on *total* quality. Goods had to be well designed and well configured; the emphasis and attention also moved from the classic manufacturing production line to the production engineer and others involved with delivering the products. With the help of U.S. consultants such as Frederick Deming, this quality movement really got started first in Japan with their high-quality products. Of course, companies throughout the world wanted to attest and advertise that they were also producing quality products. This is where ISO came into the picture.

As discussed in Chapter 13, ISO will develop an auditable standard in some area of worldwide interest. Organizations that want to claim that they are in compliance with that standard will have designated outside reviewers to check on their compliance and award certifications where appropriate. As business becomes global, these ISO standards are very important. A manufacturer in Illinois may be considering outsourcing the manufacturing of some components

to China. The Illinois manufacturer would look for the supplier in China to be ISO quality management certified as assurance of supplier production quality. Similarly, a customer in France might want to see that the same Illinois manufacturer is ISO quality management certified before purchasing the product. Although the control of these standards is through ISO in Geneva, the ASQ continues to play a very important role in these processes though its publications, educational offerings, standards interpretations, and the like.

What does all of this have to do with ISO's forthcoming risk management standard? This is admittedly speculation, but a strong and widely adopted ISO risk management standard could very much enhance the interest and adoption of COSO ERM:

- At least in its current draft form, many aspects of COSO ERM are consistent with the draft ISO standard, *"Risk Management—Guidelines for Principles and Implementation of Risk Management."* This means that enterprises worldwide may develop risk management frameworks that are consistent with COSO ERM's common and recognized framework.
- COSO may take a more active role in developing and issuing more ERM guidance. We would see this trend for COSO similar to the manner in which the ASQ provides a breadth of quality system-related guidance.

Trends do not happen overnight, but a strong ISO risk management standard could have some broad implications. It would allow enterprises, worldwide, to assert that they have effective risk management processes in place.

Even more speculative, another future trend here may be a level of closer integration between COSO internal controls and its ERM framework. We discussed in earlier chapters that some professionals initially viewed ERM as a revision or update to COSO internal controls. Of course, any level of study then showed the differences. However, there are common elements of internal control in risk management and internal control concerns in effective risk management systems, and there may be greater linkages between these two standards going forward—nothing that will happen in the near future, but could be a potential development going forward. It certainly would have some strong implications for the CPA-focused financial auditor calling for a need to rethink some processes.

LEARNING MORE ABOUT RISK MANAGEMENT

Previous chapters have discussed how many of the basic concepts of risk management are derived from the insurance industry, with its tools to assess and estimate risk-based probabilities. ERM under COSO moves

beyond just insurance to the management of multiple aspects of risk within the enterprise, whether a for-profit corporation or some other entity. It also calls for people with often different backgrounds and training to become risk management professionals. Developing this knowledge and acquiring skills can be a learning challenge, as many may have moved from audit, IT, or accounting-related positions; they may find it difficult to make an easy transition. There is a need for these new ERM practitioners to better understand the risk management-related roles and approaches. There is some information on ERM concepts through professional organizations, such as the American Institute of Certified Public Accountants (AICPA), IIA, or Information Systems Audit and Control Association (ISACA), but those materials are limited from a COSO ERM perspective. These chapters have tried to expand that guidance, but an ERM professional also might benefit from learning more about the professional risk management tools and materials that are published and circulated as part of the insurance industry.

Reviewing some of the published insurance industry materials here may be a real surprise for the noninsurance professional whose insurance industry experiences are limited to the woes of paying premiums for auto liability policies or experiences with overly aggressive life insurance salespersons back in college days. Beyond these, there is a high level of interest in ERM tools and techniques throughout the insurance industry. There should be! Insurance companies and related reinsurance companies make their living by sorting out the risk profiles of others, analyzing and helping to minimize those risks, and finally providing financing for them. For the noninsurance professional, there is much to be learned from insurance industry publications, Web sites, and other sources.

There are a large number of professional organizations covering risk management. A Web search on risk management professional organizations will almost overwhelm someone unacquainted with this industry and profession. Some groups focus on risk management in private and public sectors, others are interested in insurance risks covering specialized industries such as construction, and still others are interested in actuarial calculations. Although many of these insurance-related professional organizations charge membership fees, they offer seminars, published papers, or specialized publications. Based on a limited review of insurance industry enterprise risk offerings, two that might be of interest to the noninsurance professional trying to learn more about the insurance industry's perspective of risk management are the Risk Management Association (RMA)[2] or the Loss Executives Association.[3] The RMA, in particular, appears to have a good perspective and overview of COSO ERM matters. It is a member-driven

professional association whose stated objective is to further the ability of its members to identify, assess, and manage the impacts of credit risk, operational risk, and market risk on their businesses and their customers. The RMA provides education, networking, and leadership opportunities for its membership.

Another professional organization with some interesting publications is the Global Association of Risk Professionals (GARP, www.garp.com). The focus here is much more on financial risk, and their bimonthly publication, the *Global Risk Review,* provides analyses of risk management topics, including ERM, credit derivatives, asset liability management, hedge funds, energy risk, financial accounting, and regulatory risk. A membership-based organization with local chapters, the GARP offers an affiliate classification of Web membership where an applicant can have access to some, but not all, of the GARP's publications and access to an extensive library list of risk-related books. The emphasis within the GARP Web site is on multiple forms of financial risk, but this is useful information for the professional interested in expanding knowledge in this area.

The effective use of analytical tools is another area that a professional can use to expand personal skills and enhance the capability of an organization's ERM function. We are referring here to topics such as Monte Carlo analyses, briefly discussed in Chapter 2, and other probability theory–based approaches. Many of the tools and approaches used here are mathematically very complex and difficult to implement, while others can be useful when faced with sorting through large numbers of potential risks. Many of these approaches go under the name of management sciences and are usually part of the coursework in any good MBA program.

Whether it is the insurance-related topics previously discussed, management decision theory approaches, expanded use of probability studies, or any of many other approaches and directions, there are numerous areas where an individual can expand personal knowledge and enhance the capability of his or her ERM activities. Professionals who expand their knowledge should be able to enhance their own professional credentials and improve operations in the organizations.

ERM: NEW PROFESSIONAL OPPORTUNITIES

With its launch in late 2004, COSO ERM is relatively new and will only become more common and recognized in future years. As indicated throughout this book, COSO ERM has now and will increasingly have important roles in many areas of enterprise management, including IT

operations, project management, SOx internal control reviews, and the corporate boardroom. This book has attempted to better introduce COSO ERM and explain its growing level of importance.

COSO ERM is becoming increasingly important to today's organization, and business professions should understand and use this framework tool. Just as COSO ERM has become the de facto worldwide standard for assessing internal controls, we expect a similar role for COSO ERM going forward. Its multidimensional format, which covers all aspects of risk management activity, seems superior to any of the enterprise risk frameworks proposed today. We will be using it more and more in upcoming years!

NOTES

1. *Internal Control—Integrated Framework.* Committee of Sponsoring Organizations of the Treadway Commission, New York, 1992.
2. Risk Management Association, 1801 Market Street, Suite 300, Philadelphia, PA, www.rmahq.org.
3. Loss Executives Association, Tenafly, NJ, www.lossexecutivesassoc.org.

INDEX

B

C