COSO ENTERPRISE RISK MANAGEMENT

Understanding the New Integrated ERM Framework

Robert R. Moeller

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

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

COSO Enterprise Risk Management

To my very best friend and wife,
Lois Moeller

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.

CONTENTS

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