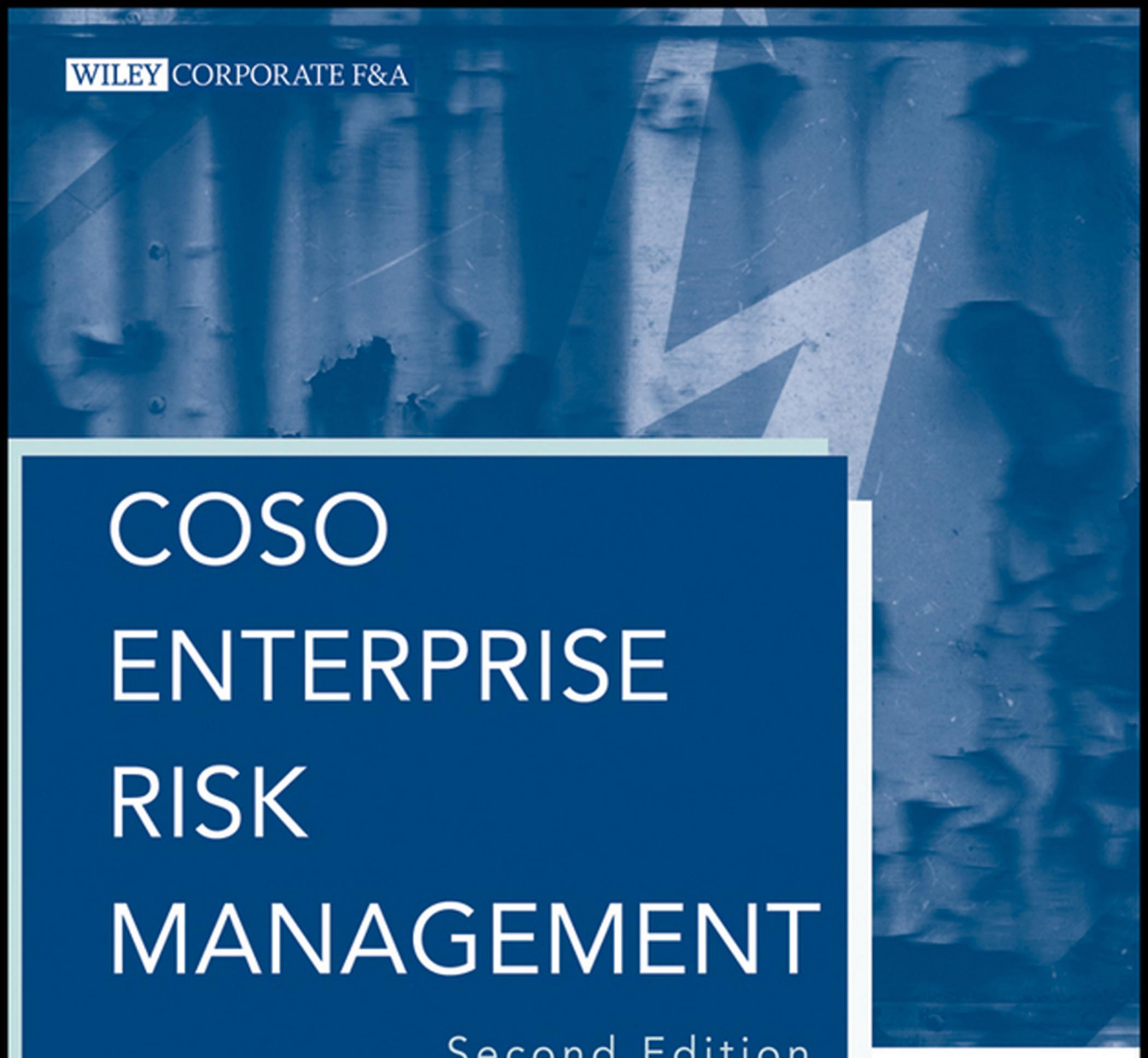

WILEY CORPORATE F&A

COSO ENTERPRISE RISK MANAGEMENT

Second Edition

Establishing Effective Governance, Risk, and Compliance Processes

ROBERT R. MOELLER

COSO Enterprise Risk Management

COSO Enterprise Risk Management

Establishing Effective Governance, Risk, and Compliance Processes

Second Edition

ROBERT R. MOELLER

WILEY

John Wiley & Sons, Inc.

Copyright © 2007, 2011 by John Wiley & Sons, Inc. All rights reserved. First edition 2007

Second edition 2011

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

Published simultaneously in Canada.

"PMI" and "PMBOK" are registered marks for the Project Management Institute, Inc.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600, or on the Web at www.copyright.com. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at http://www.wiley.com/go/permissions.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services or for 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 www.wiley.com.

Library of Congress Cataloging-in-Publication Data

Moeller, Robert R

COSO enterprise risk management : establishing effective governance, risk, and compliance processes / Robert R. Moeller.—2nd ed.

p. cm.—(Wiley corporate f&a ; 560)

Includes index.

ISBN 978-0-470-91288-1 (hardback); ISBN 978-1-118-10252-7 (ebk);

ISBN 978-1-118-10253-4 (ebk); ISBN 978-1-118-10254-1 (ebk)

1. Risk management. I. Title.

HD61.M568 2011

658.15'5—dc22 2011012021

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

To my wife and very best friend, Lois Moeller

Contents

Preface

RISK MANAGEMENT IS ONE of those concepts where many business professionals will agree that, "Yes, we need a good risk management program!" but those same professionals often have difficulty, when pressed for a better definition, explaining what they mean by the term *risk management*. For many business professionals, this lack of a consistent understanding of risk management has been similar, until recently, to the earlier lack of a general understanding of the term *internal controls*. Going as far back as the 1950s in the United States, internal and external auditors as well as many business professionals 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 COSO internal control framework that we have had a consistent and widely recognized definition of internal controls for all enterprises.

Risk management has had a similar history of inconsistent and not always clearly understood definitions. Insurance enterprises 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 high, medium, or low risk without fully understanding the meaning of such a rating. Over past years and until the very recent present, many enterprises including for-profit entities, not-for-profits, or governmental agencies have not had a consistent definition of the meaning of risk management and what was necessary to establish an effective risk management structure or framework. To help with this definition problem, the COSO guidance setting entity[1] developed a risk management definition or framework definition called COSO Enterprise Risk Management or COSO ERM. This risk management framework, updated with COSO guidance and published in 2011,[2] provides a structure and set of definitions to allow enterprises of all types and sizes to understand and better manage their risk environments.

Similar to our concerns about a better way to look at and understand risk management, enterprises have had similar needs to improve their enterprise governance practices and both regulatory and ethics compliance standards. Although there have always been issues, interests in better enterprise governance and compliance standards first became particularly important at the beginning of this century with the corporate fraud–related failure of the high-flying corporation Enron. This led to the passage of the Sarbanes-Oxley Act (SOx) in the United States and a worldwide

interest in enterprise governance and compliance issues. These concerns became even more significant with the worldwide financial recession starting around 2008.

While enterprise risk management is a major focus of this book, governance, risk, and compliance issues are all equally important. Using the initials for each, we frequently refer to these as GRC issues and standards. Enterprises need to build and launch effective GRC processes.

Starting with the letter R of this concept, a 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 concepts and best practices in general and make more effective use of the COSO ERM risk management framework. 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 an enterprise's appetite for risk to help make appropriate decisions in many areas of business operations.

COSO ERM concepts are important for all levels of an enterprise. In addition to its applicability for more senior managers, the chapters following will explain how all professionals in an enterprise can make better decisions through use of this COSO ERM framework and its recently released supporting guidance. The COSO ERM framework provides an improved way of looking at all aspects of risk in today's enterprise. This book is designed to help professionals to develop and follow an effective risk culture for many business and operating decisions.

This updated second edition will also discuss effective enterprise governance practices including some of the key regulatory issues currently facing the modern enterprise. Our emphasis is not to just discuss rules and standards but to emphasize effective processes, particularly with an emphasis on using IT tools and processes and utilizing the internal audit function. Also, many of the following chapters will reference an example company that we have called Global Computer Products to help the reader understand the use and practical application of COSO ERM and other effective GRC processes. This hypothetical example company will be described in more detail in the chapters following.

Chapter by chapter, this new second edition covers the following COSO ERM and GRC process description and recommended good practices:

- **Chapter 1. Introduction: Enterprise Risk Management Today.** This introductory chapter introduces the concept of enterprise risk management and the related concepts of enterprise governance and compliance standards. We start by looking at an important standard for defining internal control, the Committee of Sponsoring Organizations (COSO) internal control framework, a worldwide accepted set of guidance materials for defining internal control in enterprises today. From this internal controls framework the chapter then introduces the similar looking in appearance, but very different, COSO enterprise risk management (ERM) framework, the major topic of many of the chapters in this book. We should note here that the COSO materials are not really *standards* in the sense of an SEC-mandated standards requirement, but they are really very strong

guidance materials. Because they are so pervasive today, we will frequently reference them as standard practices. The chapter will also introduce us to an example company, Global Computer Products, which will be referenced for many examples throughout the book. However, the major objective of this chapter is to introduce COSO ERM and related governance and compliance principles and how they have changed since our first edition.

- **Chapter 2. Importance of Governance, Risk, and Compliance (GRC) Principles.** Events such as the collapse of the energy trading firm, Enron, and its public accounting firm, Arthur Andersen, and the enactment of the Sarbanes-Oxley Act (SOx) in 2002 raised a whole series of enterprise GRC issues that had been previously all but ignored. The collapse of housing markets almost worldwide during our recent great recession has also focused on needs today for improved compliance processes. This chapter reviews the elements of effective GRC processes and discusses why past events such as Enron and the more recent financial crises have emphasized the growing importance of enterprise governance, risk, and compliance processes.
- **Chapter 3. Risk Management Fundamentals.** Key concepts and the 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 used for risk transfers and assessments. These concepts will be helpful in understanding risks in both a quantitative and qualitative sense and in using and understanding COSO ERM. This chapter also will introduce some of the basic concepts of probability and how they are used to measure and assess risks.
- **Chapter 4. The COSO ERM Framework.** 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. We introduce the three-dimensional model or framework for understanding enterprise risk, COSO ERM, with its eight vertical components or layers as one model dimension, a second dimension of four vertical columns covering key risk objectives, and a third dimension describing the enterprise units in the risk framework. An understanding of these framework components sets the stage for understanding and using COSO ERM. The chapter also highlights some of the recent guidance material released by COSO on how to more effectively implement and use COSO ERM.
- **Chapter 5. Implementing ERM in the Enterprise.** Risk management must be understood in terms of its strategic, operational, reporting, and compliance objectives as well how it should be implemented throughout the enterprise, from an individual business unit to the entire enterprise. Beyond the Chapter 3 discussion of risk management fundamentals and the introduction of COSO ERM, these are the other two dimensions of this risk management framework, this chapter discusses these other two elements and how all three relate together. The idea is to think of enterprise risk management as an overall structure that will allow managers to understand and manage risks throughout an enterprise.

- **Chapter 6. Importance of Strong Governance Practices.** We outline why all enterprises and public corporations, in particular, are expected to have some social and governance responsibilities. Governance principles can also be introduced at an overall stakeholder level through effective ethics programs and codes of conduct.
- **Chapter 7. Enterprise Compliance Issues Today.** Enterprises today face growing amounts of legal and regulatory requirements at national, local, and regional levels. The chapter discusses the multiple issues facing an enterprise and introduces processes for reviewing and assessing compliance at all levels of an enterprise today.
- **Chapter 8. Integrating ERM with COSO Internal Controls.** Prior chapters have only referenced the COSO internal controls framework in contrasting it to COSO ERM. This chapter will dig a bit deeper and provide a more detailed look at the components and objectives of the COSO internal controls framework as well as some background on its origins. Since the COSO internal controls framework has a risk component, we will also discuss its relationship to COSO ERM. An overall objective of this chapter will be to describe how managers can use and apply effective enterprise risk management practices when building strong COSO internal control practices.
- **Chapter 9. Sarbanes-Oxley and Enterprise Risk Management Concerns.** SOx has had a major impact on corporations whose securities are registered with the U.S. Securities and Exchange Commission (SEC) and has changed the financial reporting and public accounting regulatory landscape from one of self-regulation by external audit firms to quasi-governmental rules. Both SOx and COSO ERM have some important interdependencies on each other, and today's enterprise manager must have a general understanding of both. This chapter provides general background on SOx and describes some of its enterprise risk–related attributes.
- **Chapter 10. Corporate Culture and Risk Portfolio Management.** This chapter looks at several important areas for implementing an effective enterprise risk management culture, including the help and support resources necessary for enterprise codes of conduct and the role of whistleblower functions both in support of SOx requirements and as an escape mechanism to manage enterprise risks. Enterprises need such a whistleblower facility where a stakeholder can independently report a problem without fear of retribution and can seek further information about some rule or procedure and ask for help.

  Our second topic in this chapter is risk portfolio management. Any enterprise faces a wide range of different types of risks and potential consequences. In order to effectively manage them, an effective approach is to divide these many and diverse risks into separate portfolios and then to assess and manage the risks on a portfolio basis.
- **Chapter 11. OCEG Capability Model GRC Standards.** The Open Compliance and Ethics Group (OCEG) is an industry-led nonprofit organization that develops standards and helps enterprises enhance their governance, risk management,

and compliance processes. OCEG is a relatively new organization and certainly did not exist at the time of the first edition of this book. While the OCEG does not have the standards-setting authority that might be found in the American Institute of Certified Public Accountants' (AICPA's) standards or even in some of the ISO 31000 guidance discussed in Chapter 17, it has published several guidance standards such as a GRC capability model. This chapter reviews several of the currently published OCEG guidance materials, including their "Red Book" on a GRC capability model, what they call their "Burgundy Book" on GRC capability processes, and related materials. Many of these OCEG guidance materials are very similar to the GRC and ERM framework guidance information found in other chapters, but with a slightly different emphasis or approach.

- **Chapter 12. Importance of ERM in the Corporate Board Room.** This chapter will consider the importance of corporate boards of directors in subscribing to good GRC principles as well as introducing COSO ERM and effective GRC principles to today's boards and their decision-making processes. It will suggest approaches for effectively implementing COSO ERM both for overall enterprise decision-making guidance and as a process for helping boards make decisions. While boards have a basic responsibility for the governance of their enterprises and related compliance issues, this chapter will emphasize the need for strong board-level GRC principles. The chapter will also discuss the importance of establishing a board-level risk committee operating in parallel with the audit committee. A broad enterprise-wide perspective of COSO ERM is an important tool for helping board members to better consider and evaluate the risks facing their enterprises.
- **Chapter 13. Role of Internal Audit in Enterprise Governance, Risk, and Compliance.** Internal audit plays an important role in monitoring and assessing all GRC processes in the enterprise. They may also act as internal consultants for helping to support GRC processes, internal controls implementations and maintenance. The chapter looks at important roles for internal audit in reviewing critical GRC systems and processes as well as techniques for building risk-based approaches for the overall internal audit process. Internal auditors have always considered risks in planning and performing audits, but COSO ERM as well as the recently updated Institute of Internal Auditors (IIA) internal audit standards suggest a greater need for emphasis on ERM.
- **Chapter 14. Understanding Project Management Risks.** Many enterprise efforts are organized as projects—limited duration activities that are managed as separate efforts within normal enterprise boundaries. The chapter introduces the Project Management Institute's standard *A Guide to the Project Management Book of Knowledge* (*PMBOK® Guide*) with its own risk management component. This chapter will discuss how to integrate *PMBOK® Guide* risk guidance materials with the overall ERM framework to better manage and control project risks.
- **Chapter 15. Information Technology and Enterprise Risk Management.** Because of the complexity in building and maintaining computer systems and

applications, risk management has been very important to information technology (IT) processes. The chapter will look at three important IT areas and how COSO ERM can help an enterprise to better understand those IT risks:

- **Application Systems Risks.** Enterprises often face significant risks when they purchase or develop new applications, implement them to 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.
- **Effective Continuity Planning.** Once more commonly called disaster recovery planning, continuity planning can help IT systems and operations, which can be subject to unexpected interruptions in their services, deal with those risks. COSO ERM provides an enhanced framework to understand and manage those risks.
- **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 enterprise in deciding where it should allocate resources. This chapter also discusses the more significant of these potential risks.

- **Chapter 16. Establishing an Effective GRC Culture throughout the Enterprise.** Effective risk management needs to go beyond implementing COSO ERM or announcing a GRC program as an initiative with one or another enterprise functions. It should be an overall philosophy that is understood and used throughout the enterprise. The chapter discusses how to establish an ERM function and GRC culture in a larger enterprise as well as the roles and responsibilities of the chief risk officer who would lead such a function.
- **Chapter 17. ISO 31000 and 38500 Risk Management Worldwide Standards.** While COSO ERM was first introduced as a U.S.-based guidance standard, other risk management standards have now been released throughout the world. The chapter will look at both ISO 31000 and 38500,[3] two related international risk management standards, and will discuss how these international standards relate to COSO ERM.
- **Chapter 18. ERM and GRC Principles Going Forward.** The concept of COSO ERM and GRC principles has changed very much since the first edition of this COSO ERM book was published in 2007. In today's highly regulated environment, enterprises are increasingly pressured by governance, risk, and compliance concerns while at the same time they have strong needs to drive their business performance and to enhance stakeholder confidence. Underlying these GRC management issues, an enterprise must coordinate and manage a wide range of manual and IT infrastructure processes that directly support the tools and systems in a GRC business environment. This final chapter summarizes some of the current trends and issues that will continue to make GRC management increasingly important. In particular, it reviews some of the areas that several professional organizations are promoting to increase an awareness of GRC and ERM.

NOTES

1. COSO stands for the Committee of Sponsoring Enterprises. Its role will be described in Chapter 1.
2. "Embracing Enterprise Risk Management: Practical Approaches to Getting Started," COSO, 2011, www.coso.org.
3. ISO stands for the International Organization for Standards, a French language–based authority in Geneva, Switzerland. See www.iso.org.

CHAPTER ONE

1 Introduction: Enterprise Risk Management Today

WELL-RECOGNIZED OR MANDATED STANDARDS are important for effective enterprise governance and management. Compliance with these standards allows the enterprise to demonstrate they are following best practices and complying with regulatory rules. For example, the enterprise's financial statements are audited by an external audit firm to determine whether they are consistent with generally accepted accounting principles (GAAP) in the United States or are fairly stated following international financial reporting standards (IFRS). This financial audit process applies to virtually all enterprises worldwide, no matter their size or enterprise structure. Investors and lenders want an external party—an independent auditor—to examine financial records and attest whether they are fairly stated. In order to attest to these financial statements, that same auditor has to determine that there are good supporting internal controls surrounding all significant financial transactions.

Internal controls cover many areas in enterprise operations. An example here 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 that check for payment. Two independent people should be involved with the release of checks that take cash from the enterprise. This is a common and well-recognized internal control, and many others relate to similar situations where one person or process should always be in a position to independently check the work of another party. Good internal control processes are essential for effective risk management systems in an enterprise.

This introductory chapter briefly looks at an important guidance standard for defining internal control, the Committee of Sponsoring Organizations' (COSO) internal control framework. This COSO guidance has become the worldwide accepted standard

for defining internal control in enterprises today. From this internal controls framework the chapter then introduces the similar looking in appearance, but very different, COSO enterprise risk management (ERM) framework, the major topic of many of the chapters in this book.

The chapter will also introduce us to an example company, Global Computer Products, which will be referenced in many examples throughout other chapters. The Global Computer Products hypothetical enterprise is a U.S.-headquartered computer hardware and software products manufacturer with worldwide development and distribution facilities. Although no example can be comprehensive or complete, we will try to use this Global Computer Products example as a vehicle to better understand and implement COSO ERM and governance, risk and compliance (GRC) issues in an enterprise today as well as to use them for implementing effective enterprise practices.

THE COSO INTERNAL CONTROLS FRAMEWORK: HOW DID WE GET HERE?

Similar to the many acronyms for products and techniques common in information technology (IT), product and process names are quickly turned into acronyms in the worlds of auditing, accounting, and corporate management. In the IT world, we quickly forget the names, words, or even the concepts that created the acronym and just use the several-letter acronyms. For example, International Business Machines Corporation (IBM) launched a custom software product for just one customer called the Customer Information Control System (CICS), back in the old mainframe or legacy computer system days of the early 1970s when IBM needed to develop software to access files in an online basis. Other computer manufacturing competitors at that time had online, real-time software, but IBM did not. IBM's CICS product was enhanced and generalized over the years. It is still around today for legacy systems, and today's users call it "Kicks" as their pronunciation of CICS. The definition or meaning of this acronym has been essentially forgotten and CICS has now become an IT "word."

The internal control guidance-setting organization, COSO, is a similar example with an abbreviated name standing for the Committee of Sponsoring Organizations of the Treadway Commission. Of course, an explanation of that COSO name does not offer much help—who is this committee, what are they sponsoring, and what is the Treadway Commission? 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 enterprise financial failures in the United States due to conditions including very high inflation, the resultant high interest rates, and some aggressive enterprise accounting approaches. The scope of these failures seems minor today when contrasted with the financial meltdowns of 2009 and 2010 or the financial frauds at the beginning of this century that led to the Sarbanes-Oxley Act (SOx). Financial crises will always be with us, and a concern back in the 1970s was that several major corporations suffered a financial collapse even though their recently published audited financial reports, signed

by their external auditors, showed both adequate earnings and good financial health. Some of these failures were caused by fraudulent financial reporting, but most turned out to be victims of the high inflation and resultant high interest rates during that period. It was not uncommon for many companies that failed to have issued fairly positive annual reports despite the bad news about to come. This also was another 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, called the National Commission on Fraudulent Financial Reporting, was formed to study the issue. Five U.S. professional financial organizations sponsored this National 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, SEC Commissioner James C. Treadway, the authority adopted 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 enterprise risk management but on the reasons behind the internal control problems that had contributed to those financial reporting failures of many years ago. 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 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 guidance or framework.

That COSO report on internal controls was released in 1992 with the official title *Internal Control–Integrated Framework.*[2] Throughout this book, it is referred to as the COSO Internal Controls report or framework to differentiate it from the COSO Enterprise Risk Management or the COSO ERM framework, our main topic. The COSO Internal Controls 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.

THE COSO INTERNAL CONTROLS FRAMEWORK

The term *internal control* had been part of the vocabulary of business for many years, but it historically never had had a precise, consistent definition. COSO 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

The COSO definition of internal control uses a three-dimensional model to describe an internal control system in an enterprise. 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, as shown in the exhibit, might be viewed in terms of its $5 \times 3 \times 3$ or 45 individual cells or components. However, these are not individual and separate components but are all interconnected with

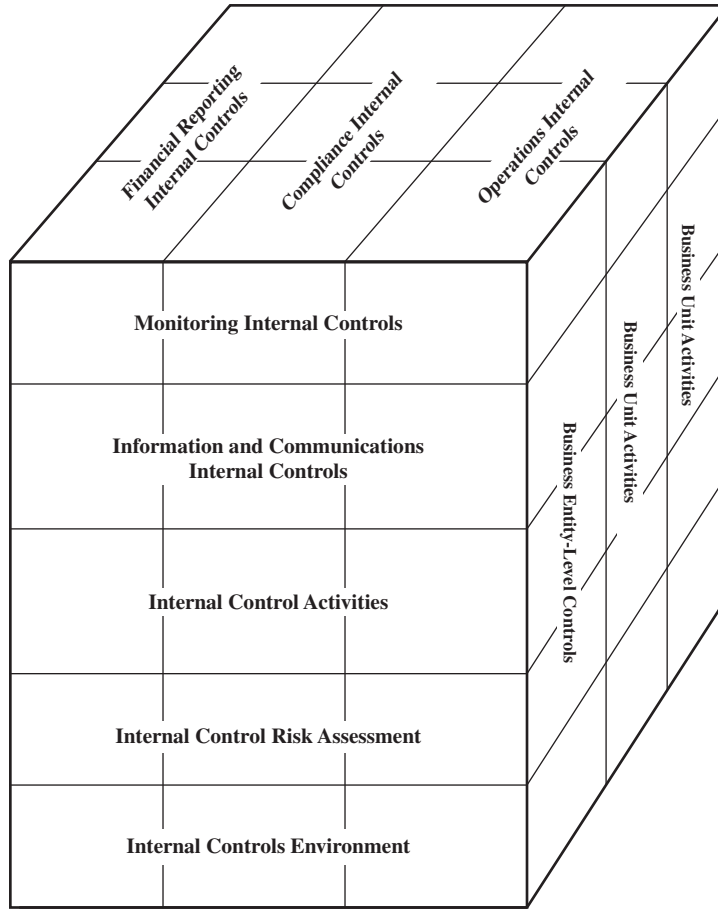

EXHIBIT 1.1 COSO Internal Controls Framework

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 enterprise, 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 Chapter 4 and illustrated in Exhibit 4.1.

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. An enterprise's control environment influences how business activities are structured and risks assessed in an enterprise. 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 enterprise.

An enterprise's history and culture plays a major role in forming its control environment. For example, when an enterprise and its management places a strong emphasis on producing error-free products, when senior management continues to emphasize the importance of error-free products, and if this message has been communicated to all levels, this becomes an important control environment factor for the enterprise. The words of the chief executive officer (CEO) and other members of senior management communicate a strong message to employees, customers, and other stakeholders. This very important set of these messages is known as the *tone at the top*. However, if senior management has had a reputation of "looking the other way" at policy violations and other matters, this message—that management does not really seem to care—will be quickly communicated to others 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 enterprise.

The COSO control environment component has major elements that managers and auditors should always understand and keep in mind when implementing enterprise changes or performing reviews of activities or business 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 enterprise operations and should consider them as essential components of the internal control framework. The control environment, as well as other elements of the COSO internal controls model, is further divided into multiple control factors. Definitions of this standard can be confusing with the internal controls framework having a controls environment component consisting of multiple control factors. While space in this chapter does not allow a discussion of the entire COSO internal control framework, the following are key identified control factors for the COSO internal control framework's

control environment. These also should help to provide an understanding of how the overall COSO internal control framework is defined:

1. **Control Environment Factors: Integrity and Ethical Values.** An enterprise's overall integrity and ethical values are essential elements of its control environment that are often defined and communicated through senior management "tone at the top" messages. If an enterprise has developed a strong code of business conduct that emphasizes integrity and ethical values, and if its stakeholders appear to follow that code, these are strong messages that the enterprise has a good set of ethical values. A code of conduct today is an important component of organizational governance. However, its principles can be violated through ignorance of that code as well as 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 enterprise'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, these policies and values must be communicated to all levels of an enterprise. While there can always be "bad apples" in any enterprise, a strong policy and demonstrated appropriate actions will encourage everyone to act correctly. Going back to our check issuance separation of duties internal control example, enterprise ethical values should be strong enough that an approving party is obligated to review a check request rather than just "rubber stamping" a signature approval 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 enterprise.

   All managers and other stakeholders should have a good understanding of their enterprise's code of conduct and how it is applied and communicated. If the code is out-of-date, if it does not appear to address important ethical issues facing an enterprise, or is not communicated to all stakeholders on a recurring basis, this failure may represent a significant enterprise internal control deficiency. What types of issues are included in a code of conduct? Exhibit 1.2 is an example of such a code of conduct table of contents. The topics will vary with the enterprise's business area, but each section here should contain strong guidance statements.

   While a code of conduct describes the rules for ethical behavior in an enterprise and while senior members of management may regularly communicate proper ethical messages, other incentives and temptations can erode this overall internal control environment. Individuals 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 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:

Enterprise Code of Conduct Typical Topic Areas

I. INTRODUCTION
- A. Purpose of This Code of Conduct: A general statement about the Code of Conduct's background.
- B. Commitment to Strong Ethical Standards: A restatement of the enterprise Mission Statement and a supporting letter from the CEO.
- C. Where to Seek Guidance: A description of enterprise help and counseling processes.
- D. Reporting Noncompliance: Guidance for Whistleblowers—How to report.
- E. Responsibilities to Acknowledge the Code: A description of the code acknowledgment process.

II. ENTERPRISE FAIR DEALING PRACTICES
- A. Selling Practices: Guidance for dealing with customers.
- B. 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 an employees's responsibility to protect all enterprise assets.
- B. Computer Systems Resources: A statement on a stakeholders's responsibility to protect and not misuse computer system and network resources.
- C. Use of the Company's Name: A rule that the company name should only be used 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 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: Rules 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 on not 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

- 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, reducing 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, losing 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 enterprise performance, and should be skeptical and perform appropriate tests when reviewing operations. When things look "too good," a manager might want to look a bit harder. This more detailed assessment of operations should not be to just find something wrong in the reported "too-good-to-be-true" numbers but to assess whether deficiencies in the control environment may lead to possible fraudulent activities. The factors of integrity and ethical values should always be a major component of the COSO control environment. Strong integrity standards and high ethical values are important for good enterprise internal controls.

2. **Control Environment Factors: Commitment to Competence.** An enterprise's control environment can be seriously eroded if a significant number of positions are filled by persons lacking required job skills. Managers will encounter this 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 enterprise should specify required competence levels for its job tasks and translate those requirements into necessary levels of knowledge and skill. By placing the proper people in appropriate jobs and giving them adequate training when required, an enterprise is making an overall *commitment to competence*, an important element in the enterprise'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.

   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 in an enterprise unit 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 efforts to satisfy overall enterprise objectives. If a manager or internal audit 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 both for

this operating unit and for larger units of the enterprise. This type of issue should be discussed with first-line managers at 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 in the enterprise even though there is no evidence that the child has the experience or skill to handle the job. These arrangements work best 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 enterprise's commitment to competence.

3. **Control Environment Factors: Board of Directors and the Audit Committee.** The control environment is very much influenced by the actions of an enterprise'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 enterprise senior management with only limited, minority representation from outside shareholders. This created situations where 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. SOx has now changed all of that, and boards today have a greater corporate governance role, and their audit committees are required to consist of independent, outside directors.

   In addition to SOx legal requirements, an active and independent board is an essential component of an enterprise's control environment. Board members should ask appropriate questions to top management and give all aspects of the enterprise detailed scrutiny. 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."

4. **Control Environment Factors: Management's Philosophy and Operating Style.** These senior management factors have a considerable influence over an enterprise's control environment. As discussed in Chapter 5 on implementing an effective risk management program, some top-level managers frequently take significant enterprise 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 very aggressive approaches in the interpretations of tax and financial-reporting rules while another may prefer to go strictly 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 enterprise 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 enterprise control environment. 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. 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 enterprise. While discussed as part of the internal controls environment here, the need to better understand risk-related control environment factors is one of the reasons for COSO ERM.

5. **Control Environment Factors: Organization Structure.** These components provide a framework for planning, executing, controlling, and monitoring activities for achieving overall objectives. This aspect of the control environment relates to the way various functions are managed and organized, following a classic enterprise chart. Some enterprises 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. Organizational structure is a very important aspect of the enterprise's control environment, but no one structure provides a preferred environment for internal controls.

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

   An enterprise can be described as the way a collection of individual work efforts are both assigned and subsequently integrated for the achievement of overall goals. While this concept could be applied to the manner in which a single individual organizes individual efforts, it is more applicable to group efforts. A strong plan of enterprise 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—whether a business, government unit, philanthropic group, or another 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 organizational structure. Often, a weakness in organization 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 the size of the enterprise 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 enterprise.

   Complex or poorly organized enterprise structures can cause some major challenges. In today's economy, enterprise divisions or units are sometimes spun off as independent corporations by the former parent company. Employees of this newly spun-off corporation would have followed the systems and procedures of the