CHAPTER ONE

1

Importance of the COSO Internal Control Framework

IT IS NOT A STANDARD or detailed requirement but only a framework. Some business executives may ask then, "Who or what is COSO?" In our business world of multiple rules and regulations that have been established by numerous governmental and other agencies that often use hard-to-remember acronyms, it is easy to roll our eyes or shrug our shoulders at yet another set of standards. In addition, COSO (Committee of Sponsoring Organizations) internal controls are only a framework model outlining professional practices for establishing preferred business systems and processes that promote efficient and effective internal controls. Also, the "sponsoring organizations" that issue and publish this material are neither governmental nor some other regulatory agencies. Nevertheless, the COSO internal control framework is an important set or model of guidance materials that enterprises should follow when developing their systems and procedures, as well as when establishing Sarbanes-Oxley Act (SOx) compliance.

This COSO internal control framework was originally launched in the United States in 1992, now a long time ago. This was yet another period of notable fraudulent business practices in the United States and elsewhere that identified a well-recognized need for improved internal control processes and procedures to help and guide. The 1992 COSO internal control framework soon became a fundamental element of American Institute of Certified Public Accountants (AICPA) auditing standards in the United States, and eventually became the standard for enterprise external auditors in their reviews, certifying that enterprise internal controls were adequately following the Sarbanes-Oxley Act (SOx) rules. Because of its general nature describing good internal control practices, the COSO framework had never been revised until the present.

Since the release of that original COSO framework, a whole lot has changed for business organizations and particularly for their IT processes during these interim years. For example, mainframe computer systems with lots of batch-processing procedures were common then but have all but gone away, to be replaced by client-server systems. Also,

while the World Wide Web was just getting started then, it was not nearly as developed as it is today. Because of the Internet, enterprises' organization structures have become much more fluid, flexible, and international. In addition, things such as social network computing, powerful handheld devices, and cloud computing did not exist back then.

Although some might wonder why it took so long, COSO announced in 2011 that it was revising its internal control framework with a draft version, which was issued in early 2012. That COSO internal control draft was circulated to a wide range of internal and external auditors, academics, and enterprise financial management, and it went through an extensive public comment period. The final revised COSO internal control framework description was released in mid-May 2013.

The following chapters describe the revised COSO internal control framework in some detail and explain why its concepts are very important for enterprise management today. This chapter begins with some background information on the COSO internal control framework from a senior executive management perspective. The COSO internal control framework sets the stage for achieving SOx compliance and will continue to be even more important with its new revised version. This book will conclude with some guidance and rules for implementing the new revised COSO internal control framework.

THE IMPORTANCE OF ENTERPRISE INTERNAL CONTROLS

An effective internal control system is one of the best defenses against business failure. An internal control system is an important driver of business performance, which manages risk and enables the creation and preservation of enterprise value. Internal controls are an integral part of an enterprise's governance system and ability to manage risk, which is understood, effected, and actively monitored by an enterprise governing body, its management, and other personnel to take advantage of the opportunities and to counter the threats to achieving an enterprise's objectives. On a very high-level conceptual manner, Exhibit 1.1 shows the relationship of internal controls as a component of risk-management processes and as a key element of enterprise governance.

Internal controls are a crucial component of an enterprise's governance system and ability to manage risk, and it is fundamental to supporting the achievement of an enterprise's objectives and creating, enhancing, and protecting stakeholder value. High-profile organizational failures typically lead to the imposition of additional rules

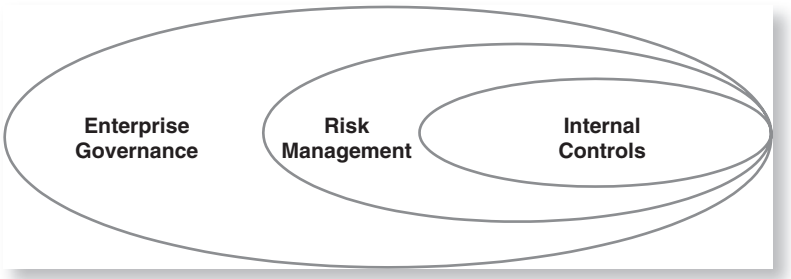

EXHIBIT 1.1 Importance of Enterprise Internal Controls

and requirements, as well as to subsequent time-consuming and costly compliance efforts. However, this obscures the fact that the right kind of internal controls—which enable an enterprise to capitalize on opportunities, while offsetting threats—can actually save time and money and promote the creation and preservation of value. Effective internal controls also create a competitive advantage, because an enterprise with effective controls can take on additional risks.

Internal controls are designed to protect an enterprise and its related business units from the loss or misuse of its assets. Sound internal controls help ensure that transactions are properly authorized, that supporting IT systems are well-managed, and that the information contained in financial reports is reliable. An internal control is a process through which an enterprise and one of its operating units attempts to minimize the likelihood of accounting-related errors, irregularities, and illegal acts. Internal controls help safeguard funds, provide for efficient and effective management of assets, and permit accurate financial accounting. Internal controls cannot eliminate all errors and irregularities, but they can alert management to potential problems.

WHAT ARE ENTERPRISE INTERNAL CONTROLS?

A classic definition states that *internal controls* consist of the plan of organization and all of the coordinate methods adopted within 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. This definition recognizes that a system of internal controls extends beyond those matters that relate directly just to the functions of the accounting and financial departments. Rather, an internal control is a business practice, policy, or procedure that is established within an enterprise to create value or minimize risk. Although enterprises first thought of internal controls in terms of fair and accurate accounting processes and effective operational management, information technology (IT) controls are also a very important subset of internal controls today. They are designed to ensure that the information within an enterprise operates as intended, that data is reliable, and that the enterprise is in compliance with all applicable laws and regulations.

We should think of internal controls not as just one solitary activity but as a series of related internal system actions. For example, a requirement that all sales receipts must be accurate and assigned to correct accounts may be an important internal control, but processes should also be in place to correct out-of-balance sales receipts and to make related adjustments as necessary. Together, these requirements and processes represent an internal control system. These internal control systems are often complex, and it is not practical or profitable to attempt to independently review every transaction. Instead, management should be alert to conditions that could indicate potential problems.

Enterprise personnel at all levels, and senior executives in particular, should be responsible for understanding internal control concepts and helping to manage and implement effective internal control systems in their enterprises. This is particularly important for senior-level enterprise internal controls, in which different business units and subsidiaries must interact and IT systems must connect through often complex business and international interconnections. In addition, an enterprise must establish

overall governance practices and operate in compliance with the numerous laws, regulations, and standards that affect its operations.

In a business operation, finance and accounting personnel have certain internal control responsibilities, a purchasing executive has others, and an IT systems developer has different responsibilities, but a senior executive should have an overall understanding of all aspects of internal controls throughout an enterprise, as well as of the top-level internal control concepts that affect overall enterprise operations and governance processes. The COSO internal control framework ties these all together, and an objective of this book is to help the senior executive understand these internal control concepts and, at a minimum, ask the right questions.

UNDERSTANDING THE COSO INTERNAL CONTROL FRAMEWORK: HOW TO USE THIS BOOK

Internal controls are important enterprise tools and concepts to ensure accurate financial reporting and management. However, in past years, *internal controls* was only a nice-sounding term by which professionals at all levels acknowledged that having effective internal controls was important. That was a long time ago, and matters were very much resolved with the introduction of the COSO internal control framework back in 1992. That best practices guide stood the test of time until it was recently updated.

This book will introduce the revised new COSO internal control framework from the perspective of senior enterprise executives. Chapter 2 will introduce the original framework that has been important for achieving SOx financial reporting compliance. Then, starting with Chapter 3, we will introduce and explain the new revised COSO internal control framework. This approach outlines and explains COSO's complex-looking three-dimensional model for building and establishing enterprise internal controls. The chapters following take COSO's three-dimensional framework and look at it from each of its dimensions to help the enterprise executive understand this internal control framework.

Other chapters cover supplementary standards or frameworks that are closely related to the COSO internal control framework, such as the continuing relationship of this framework to SOx internal control requirements, its relationship with the COBIT framework, and the current status of the related COSO enterprise risk management framework.

This book will conclude with guidance for implementing this revised framework. Although much of the COSO framework describes general practices that are applicable in many dimensions, there are some subtle differences between this new revised framework and the original edition. Following the transition rules outlined in Chapter 20, an enterprise must specify the version of the COSO internal control framework used when releasing its SOx financial reports.

The original COSO framework was with us for many years, and we expect these revisions will also be in place for years into the future. A goal of this book is to provide sufficient summary information about the revised COSO internal control framework such that a senior executive can brief members of the audit committee about the nature of this new revision and can also help members of the enterprise management team understand and implement enterprise internal controls that are consistent with these new revisions.