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

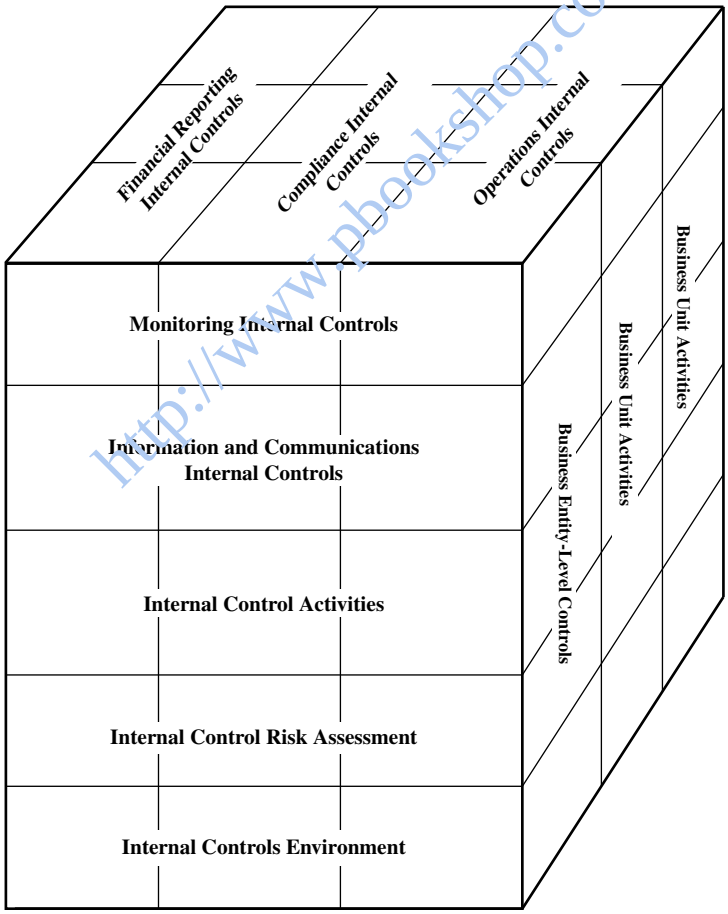

EXHIBIT 1.1 COSO Internal Controls Framework

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

previous parent but 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 when the free-standing business is built and financial structure details are established.

6. **Control Environment Factors: Assignment of Authority and Responsibility.** This COSO-defined area of the control environment is similar to the enterprise structure factors previously discussed. An enterprise'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 enterprise 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 enterprises 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 department 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 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 an individual's actions interrelate to achieve those objectives. The framework section of the previously referenced COSO internal controls 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 systems.

7. **Control Environment Factors: Human Resources Policies and Practices.** Human resource practices cover such areas as hiring, orientation, training, valuating, 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 ignoring a plant smoking ban, quickly sends a message to others in the enterprise. 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 enterprise should take steps to hire the best, most qualified candidates. Potential employee backgrounds should be checked to verify such matters as their education backgrounds and prior work experience. 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 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 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 members of the enterprise. 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 at least 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 this 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. 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 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 enterprise that is building a strong internal control structure should give special attention to placing these solid foundation bricks in their control environment structure.

COSO Internal Control Elements: Risk Assessment

Again with a reference back to the Exhibit 1.1 COSO internal control framework, the next level or layer above the control foundation is called risk assessment. An enterprise'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 enterprise 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, which will be introduced in Chapter 3, there should be at least a minimum understanding of the risk assessment process. An enterprise 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 enterprises have found that the best time and place to assess their various levels of risks is during the annual or periodic planning process. This risk-assessment process should be performed at all levels and for virtually all activities within the enterprise. The COSO internal controls 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 introduced starting in Chapter 4, retains these same factors but treats the 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, as will be discussed in many chapters that follow, leads to a far more comprehensive, integrated approach to understanding an enterprise's risks as part of their internal control environment.

The COSO internal controls framework—released over 10 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 enterprise as well as the risks over various enterprise activities or entities. A variety of risks, caused by either internal or external sources, may affect the overall enterprise. COSO ERM has defined some essential components, suggested a common language, and has introduced a common language to allow an enterprise to better manage its enterprise-level risks.

Other COSO Internal Control Components and Activities

The control environment as well as risk assessment are only two components of the 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 also are very important for understanding the overall

COSO internal control framework. An understanding of the COSO internal control framework is essential for today's managers in all levels and components of an enterprise. If for no other reason, that understanding is required for an enterprise to achieve their SOx Section 404 internal control compliance requirements, as will be summarized in Chapter 10. However, the objective of this book is not to provide a detailed description of the entire COSO internal controls framework but rather to introduce it as a precursor to COSO ERM.

Internal controls and enterprise risk management each take a different perspective to understanding and evaluating activities in an enterprise. While COSO internal controls focus on an enterprise's daily activities, enterprise risk management focuses on activities that an enterprise 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 enterprise. However, that same manager may be concerned about such enterprise risks as the financial impacts on the enterprise 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 controls framework but involve enterprise risk.

COSO INTERNAL CONTROLS: THE PRINCIPAL RECOGNIZED INTERNAL CONTROLS STANDARD

The COSO internal controls framework was released in 1992 as a three-volume publication describing this internal control standard. Although there initially was limited recognition of the COSO framework beyond comments in AICPA and IIA publications, the then major public accounting firms and others soon began to see its value. Over the years the COSO internal controls framework has become the worldwide guidance standard for defining, describing, and assessing internal controls.

Public accounting auditing standards were once the responsibility of the AICPA's Auditing Standards Board (ASB), but since the activation of SOx in 2002, the Public Company Accounting Oversight Board (PCAOB) has been established to supervise all independent auditing firms and to take responsibility for the release of auditing standards. The PCAOB has issued auditing standards that recognize and accept the COSO internal controls framework.[4]

AN INTRODUCTION TO COSO ERM

The release of the COSO internal controls framework with its definitions pointed to other related areas where consistent definitions were lacking. One of these was risk management, a concept that had been receiving multiple definitions and interpretations by various industry groups. This was the era prior to 2002-era SOx rules, when some public accounting firms began to call themselves risk management professionals,

although many did not appear to have a clear understanding of what was meant by risk management. To try to develop such a consistent risk management definition, COSO contracted with the public accounting firm PricewaterhouseCoopers (PwC) in 2001 to develop a common consistent definition for risk management. The result was the COSO Enterprise Risk Management or COSO ERM framework, our main topic. COSO ERM will be more thoroughly introduced and discussed in subsequent chapters of this book.

While we will be discussing many aspects of COSO ERM and how to use this framework, business professionals should also have a detailed understanding of the COSO internal controls framework just introduced. We have only provided a brief introduction to COSO internal controls, but a more detailed description of this framework can found in many Web references and in our book, *Brink's Modern Internal Auditing.*[5] For virtually all persons involved in modern business today, an understanding of that COSO definition of internal controls is essential.

GOVERNANCE, RISK, AND COMPLIANCE

Enterprise risk management and COSO ERM are only one of three major issues that are very much impacting all enterprises worldwide today. The other two are importance of good enterprise governance processes, and the need for effective enterprise-wide compliance programs. Taken together along with risk management, these three issues are usually referenced by their initials, GRC. While much of our emphasis will be on the importance of managing and understanding all aspects of enterprise risk through COSO ERM, other chapters will discuss important governance and compliance issues in enterprise.

Corporate or enterprise governance is the set of processes, customs, policies, laws, and institutions affecting the way an enterprise or corporation is directed, administered, or controlled. It is much more than a policy statement published in an annual report or a public relations type of advertisement in the *Wall Street Journal*. Corporate governance includes the manner of the relationships among the many stakeholders involved in the enterprise and the goals for which the enterprise is governed. The principal stakeholders are the shareholders, the board of directors, employees, customers, creditors, suppliers, and the community at large.

Enterprise governance is a multifaceted subject, with an important theme to ensure the accountability of certain individuals in an enterprise through mechanisms that try to reduce or eliminate the conflicts that will exist between their overall goals and individual stakeholders' self-interest. In many enterprise activities, there is a continuing need to focus any governance system on economic efficiency along with a strong emphasis on shareholder and stakeholder welfare.

There has been renewed interest in the corporate or enterprise governance practices in modern corporations since 2001, particularly due to the high-profile collapses of a number of large U.S. firms such as Enron Corporation at that time and the failure of many financial institutions in the years starting about 2008. When Enron failed, the U.S. federal government passed the Sarbanes-Oxley Act (SOx) in 2002 with an objective to restore public confidence in corporate or enterprise governance.

The collapse of the banks and other financial institutions in 2008 and beyond in the United States led to massive taxpayer bailouts and increased legal rules. An enterprise today needs to establish policies to effectively handle its governance issues as well as a culture to allow it to build an effective system of governance.

After governance, risk issues, and management, the third key component of GRC is enterprise compliance. Compliance is either a state of being in accordance with some established guidelines, specifications, or legislation or the process of becoming so. Internal audits, for example, should be developed in compliance with the International Standards for the Professional Practice of Internal Auditing, as will be discussed in Chapter 14. Software, as another example, may be developed in compliance with specifications created by some standards body and should be installed and used in compliance with the vendor's licensing agreement. In the legal system, compliance usually refers to behavior in accordance with legislation, such as the Sarbanes-Oxley Act (SOx) or any of a large and growing body of other laws and rules.

An enterprise must develop systems to monitor and manage their levels of compliance with various rules and regulations as well as to take appropriate actions to detect and act on any violations. With an emphasis on COSO ERM, the chapters following will introduce and discuss how an enterprise today should develop appropriate GRC processes.

GLOBAL COMPUTER PRODUCTS: OUR EXAMPLE COMPANY

The following chapters will include multiple examples of forms and procedures as well as discussions of COSO ERM and other GRC processes that can be effectively launched and implemented in an enterprise. Starting here and throughout our discussion of the COSO ERM components as well as in other GRC materials when appropriate, we will be referring to a hypothetical computer products manufacturer called Global Computer Products. Exhibit 1.3 gives an overview and background of this example company while Exhibit 1.4 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.

Following a discussion in Chapter 2 on the importance of general enterprise mission statements and with the introduction of this example company, Exhibit 1.5 shows an example mission statement for Global Computer Products with linkages to strategic and specific related objectives. Our discussion here—and certainly not a goal of COSO ERM and GRC principles—is not to suggest approaches to developing organization mission statements and formal strategic objectives. Rather, the message here is that any and every enterprise should develop a mission statement and then have some formal objectives to achieve that mission. In addition, the enterprise should develop some units of measure to allow them to assess whether they are achieving those risk management objectives.

We will be referencing this example company in the chapters to follow as we introduce various elements of COSO ERM and overall GRC principles. These are at least as important as the need to comply with the COSO internal controls framework.

Lobal Computer Products 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 of the book as an example of how an enterprise can assess its risks and develop both effective ERM and GRC strategies. This description represents the type of medium-sized organization today that is operating internationally in more advanced technology but sales-driven areas.

Some key characteristics of Global Computer Products include:

- *Locations and Operations.* The company has a headquarters office in the Chicago area with a computer security development facility in San Jose, CA, and four product distribution centers in smaller U.S. locations 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.
- *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 employees. Reporting to the chief audit executive (CAE), Global has a relatively small internal audit department as well as a single general counsel.
- *Product Description.* Global had developed a computer security product that consists of both a hardware device plugged into a standard laptop or desktop computer along with software drivers. The hardware device plug-in card is 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 descriptions in professional publications as well as through a team of sales representatives. On a worldwide basis, 80 percent of sales are to individuals with the balance to smaller businesses. The United States accounts for about 75 percent of product sales with the balance in 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 percent of the shares and management holds 3 percent. Long-term debt totals $450,000,000 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 1.3 Example Company Background: Global Computer Products

The following are some—but certainly not all—of the key risks that could impact the example company referenced throughout these chapters, Global Computer Products. These risks may be expanded or modified over time as this 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 introduced in Chapter 4. They should be considered just risks that impact this example enterprise.

- Organization Strategic Risks that could impact the effectiveness of products or operations:
  - Changes in technology that impact effectiveness of company products.
  - A trend away from computer-based applications and a move to Internet-based Software-as-a-Service (SaaS) applications.
  - 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 an earthquake, or military actions.
  - New competitors offering attractive alternative products.
  - Interest rate increases or other factors limiting ability to finance expansion.
  - The failure of a major key customer or vendor.
- Company Operations Risks
  - A computer server systems or network failure at one or several locations.
  - The unexpected resignation of a key management person 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 significant loss in stock market capitalization value due to reported operating losses.
- Financial and Operational Reporting Risks
  - Significant internal controls weaknesses identified through a SOx Section 404 review.
  - Failure of one or more subsidiary units to secure a ''clean'' external audit opinion.
  - Financial or operations errors in individual units 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 retain ISO certifications in key areas.
  - Failure to meet product quality standards.

EXHIBIT 1.4 Global Computer Products Corporate Risks Summary

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 Enterprises of the Treadway Commission, published by AICPA, Jersey City, NJ, 1992.
3. A more detailed description of the COSO Internal Controls framework can be found in Robert Moeller, *Brink's Modern Internal Auditing: A Common Body of Knowledge*, 7th ed., Hoboken, NJ: John Wiley & Sons, 2009.
4. PCAOB, Rule 3100, Compliance with Public Accounting and Related Professional Practice Standards, February 15, 2005, www.pcaobus.org.
5. Robert Moeller, *Brink's Modern Internal Auditing: A Common Body of Knowledge*, 7th ed., Hoboken, NJ: John Wiley & Sons, 2009.