1

IMPORTANCE OF ENTERPRISE RISK MANAGEMENT TODAY

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

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

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

COSO RISK MANAGEMENT: HOW DID WE GET HERE?

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

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

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

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

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

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

COSO INTERNAL CONTROL FRAMEWORK

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

> Internal control is a process, affected by an entity's board of directors, man-
> agement, and other personnel, designed to provide reasonable assurance
> regarding the achievement of objectives in the following categories:
>
> Effectiveness and efficiency of operations
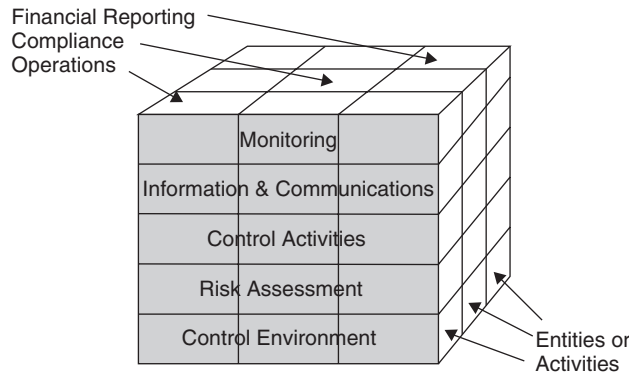>
> Reliability of financial reporting
>
> Compliance with applicable laws and regulations[4]

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

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

COSO Internal Control Elements

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

Financial Reporting
Compliance
Operations

Monitoring

Information & Communications

Control Activities

Risk Assessment

Control Environment

Entities or
Activities

Relationship between Control Components,
Objectives, and Organization Entities

EXHIBIT 1.1 AN ORGANIZATION'S COSO INTERNAL CONTROL MODEL

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

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

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

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

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

Control Environment Factors

Integrity and Ethical Values

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

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

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

- Nonexistent or ineffective controls, such as poor segregation of duties in sensitive areas, that offer temptations to steal or to conceal poor performance

- High decentralization that leaves top management unaware of actions taken at lower organization levels and thereby reduces the chances of getting caught

- A weak management function that has neither the ability nor the authority to detect and report improper behavior

- Penalties for improper behavior that are insignificant or unpublicized and thus lose their value as deterrents

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

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

I.   Introduction.

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

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

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

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

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

II.   Fair Dealing.

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

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

III.   Conduct in the Workplace.

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

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

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

IV.   Conflicts of Interest.

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

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

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

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

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

V.   Company Property and Records.

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

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

EXHIBIT 1.2   CODE OF CONDUCT TOPICS EXAMPLE

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

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

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

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

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

VI.   **Complying with the Law.**

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

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

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

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

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

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

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

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

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

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

Commitment to Competence

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

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

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

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

Board of Directors and Audit Committee

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

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

Management's Philosophy and Operating Style

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

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

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

Organization Structure

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

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

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

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

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

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

Assignment of Authority and Responsibility

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

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

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

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

Human Resources Policies and Practices

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

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

- *Recruitment and hiring.* The organization should take steps to hire the best, most qualified candidates. Potential employee backgrounds should be checked to verify their education credentials and prior work experiences. Interviews should be well organized and in-depth. They should also transmit a message to the prospective candidate about the organization's values, culture, and operating style.

- *New employee orientation.* A clear signal should be given to new employees regarding the organization's value system and the consequences of not complying with those values. This often occurs when new employees are introduced to the code of conduct and asked to formally acknowledge their acceptance of that code. Without these messages, new employees may join the organization lacking an appropriate understanding of its values.

- *Evaluation, promotion, and compensation.* There should be a fair performance evaluation program in place that is not subject to an

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

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

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

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

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

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

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

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

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

Other Components and Activities

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

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

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

COSO INTERNAL CONTROL FRAMEWORK AS A RECOGNIZED STANDARD

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

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

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

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

ORIGINS OF COSO ERM

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

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

NOTES

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

2. Committee of Sponsoring Organizations of the Treadway Commission, published by AICPA, Jersey City, NJ, 1992.

3. For a more detailed reference to the COSO Internal Control–Integrated Framework, see Robert Moeller, *Brink's Modern Internal Auditing,* 6th ed., Hoboken, NJ: John Wiley & Sons, 2005.

4. *Internal Control–Integrated Framework,* The Committee of Sponsoring Organizations of the Treadway Committee, New York, 1992.

5. For more information on the Sarbanes-Oxley Act and its internal control reporting requirements, see Robert Moeller, *Sarbanes-Oxley and the New Internal Auditing Rules,* Hoboken, NJ: John Wiley & Sons, 2004.

6. Committee of Sponsoring Organizations of the Treadway Commission, *Internal Control–Integrated Framework,* New York: AICPA, 1992.

7. SAS 78, Consideration of Internal Control in a Financial Statement Audit: An Amendment to SAS No. 55, New York: AICPA, 1995.

8. PCAOB, Rule 3100, Compliance with Public Accounting and Related Professional Practice Standards, February 15, 2005, www.pcaobus.org.