1994 Edition
In Two Volumes

INTERNAL CONTROL – INTEGRATED FRAMEWORK

COSO

- Executive Summary
- Framework
- Reporting to External Parties
- Addendum to "Reporting to External Parties"

Committee of Sponsoring Organizations of the Treadway Commission (COSO)

Oversight

	Representative
American Institute of Certified Public Accountants	Robert L. May, Chairman
American Accounting Association	Alvin A. Arens
The Institute of Internal Auditors	William G. Bishop, III
Institute of Management Accountants	Thomas M. O'Toole
Financial Executives Institute	P. Norman Roy

Project Advisory Council to COSO

Guidance

Gaylen N. Larson, Chairman
Group Vice President, Chief Accounting Officer
Household International

Andrew D. Bailey
Professor, Department of Accounting
College of Business and Public Administration
The University of Arizona

Roger N. Carolus
Senior Vice President
NationsBank (retired)

C. Perry Colwell
Senior Vice President–Financial Management
AT&T (retired)

William J. Ihlanfeldt
Assistant Controller
Shell Oil Company

David L. Landsittel
Managing Director–Auditing
Arthur Andersen & Co.

John H. Stewart
Assistant Treasurer
IBM Corporation

Howard L. Siers, Consultant
General Auditor
E.I. Du Pont de Nemours and Company, Inc. (retired)

Coopers & Lybrand

Author

Principal Contributors

Vincent M. O'Reilly
Deputy Chairman, Accounting and Auditing

Frank J. Tanki
Director, Accounting and SEC Technical Services

R Malcolm Schwartz
Principal
New York Office

Robert J. Spear
Partner
Boston Office

Richard M. Steinberg
Partner
National Office

Contents

INTERNAL CONTROL – INTEGRATED FRAMEWORK

► Executive Summary

Framework

Reporting to External Parties

Addendum to "Reporting to External Parties"

Executive Summary

Senior executives have long sought ways to better control the enterprises they run. Internal controls are put in place to keep the company on course toward profitability goals and achievement of its mission, and to minimize surprises along the way. They enable management to deal with rapidly changing economic and competitive environments, shifting customer demands and priorities, and restructuring for future growth. Internal controls promote efficiency, reduce risk of asset loss, and help ensure the reliability of financial statements and compliance with laws and regulations.

Because internal control serves many important purposes, there are increasing calls for better internal control systems and report cards on them. Internal control is looked upon more and more as a solution to a variety of potential problems.

What Internal Control Is

Internal control means different things to different people. This causes confusion among businesspeople, legislators, regulators and others. Resulting miscommunication and different expectations cause problems within an enterprise. Problems are compounded when the term, if not clearly defined, is written into law, regulation or rule.

This report deals with the needs and expectations of management and others. It defines and describes internal control to:

- Establish a common definition serving the needs of different parties.
- Provide a standard against which business and other entities—large or small, in the public or private sector, for profit or not—can assess their control systems and determine how to improve them.

Internal control is broadly defined as a process, effected 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 first category addresses an entity's basic business objectives, including performance and profitability goals and safeguarding of resources. The second relates to the preparation of reliable published financial statements, including interim and condensed financial statements and selected financial data derived from such statements, such as earnings releases, reported publicly. The third deals with complying with those laws and regulations to which the entity is subject. These distinct but overlapping categories address different needs and allow a directed focus to meet the separate needs.

Internal control systems operate at different levels of effectiveness. Internal control can be judged effective in each of the three categories, respectively, if the board of directors and management have reasonable assurance that:

- They understand the extent to which the entity's operations objectives are being achieved.
- Published financial statements are being prepared reliably.
- Applicable laws and regulations are being complied with.

While internal control is a process, its effectiveness is a state or condition of the process at one or more points in time.

Internal control consists of five interrelated components. These are derived from the way management runs a business, and are integrated with the management process. Although the components apply to all entities, small and mid-size companies may implement them differently than large ones. Its controls may be less formal and less structured, yet a small company can still have effective internal control. The components are:

- *Control Environment*—The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values and competence of the entity's people; management's philosophy and operating style; the way management assigns authority and responsibility, and organizes and develops its people; and the attention and direction provided by the board of directors.
- *Risk Assessment*—Every entity faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is establishment of objectives, linked at different levels and internally consistent. Risk assessment is the identification and analysis of relevant risks to achievement of the objectives, forming a basis for determining how the risks should be managed. Because economic, industry, regulatory and operating conditions will continue to change, mechanisms are needed to identify and deal with the special risks associated with change.
- *Control Activities*—Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.
- *Information and Communication*—Pertinent information must be identified, captured and communicated in a form and timeframe that enables people to carry out their responsibilities. Information systems produce reports, containing operational, financial and compliance-related information, that make it possible to run and control the business. They deal not only with internally generated data, but also information about

external events, activities and conditions necessary to informed business decision-making and external reporting. Effective communication also must occur in a broader sense, flowing down, across and up the organization. All personnel must receive a clear message from top management that control responsibilities must be taken seriously. They must understand their own role in the internal control system, as well as how individual activities relate to the work of others. They must have a means of communicating significant information upstream. There also needs to be effective communication with external parties, such as customers, suppliers, regulators and shareholders.

- *Monitoring*—Internal control systems need to be monitored—a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two. Ongoing monitoring occurs in the course of operations. It includes regular management and supervisory activities, and other actions personnel take in performing their duties. The scope and frequency of separate evaluations will depend primarily on an assessment of risks and the effectiveness of ongoing monitoring procedures. Internal control deficiencies should be reported upstream, with serious matters reported to top management and the board.

There is synergy and linkage among these components, forming an integrated system that reacts dynamically to changing conditions. The internal control system is intertwined with the entity's operating activities and exists for fundamental business reasons. Internal control is most effective when controls are built into the entity's infrastructure and are a part of the essence of the enterprise. "Built in" controls support quality and empowerment initiatives, avoid unnecessary costs and enable quick response to changing conditions.

There is a direct relationship between the three categories of objectives, which are what an entity strives to achieve, and components, which represent what is needed to achieve the objectives. All components are relevant to each objectives category. When looking at any one category—the effectiveness and efficiency of operations, for instance—all five components must be present and functioning effectively to conclude that internal control over operations is effective.

The internal control definition—with its underlying fundamental concepts of a process, effected by people, providing reasonable assurance—together with the categorization of objectives and the components and criteria for effectiveness, and the associated discussions, constitute this internal control framework.

What Internal Control Can Do

Internal control can help an entity achieve its performance and profitability targets, and prevent loss of resources. It can help ensure reliable financial reporting. And it can help ensure that the enterprise complies with laws and regulations, avoiding damage to its reputation and other consequences. In sum, it can help an entity get to where it wants to go, and avoid pitfalls and surprises along the way.

What Internal Control Cannot Do

Unfortunately, some people have greater, and unrealistic, expectations. They look for absolutes, believing that:

- Internal control can ensure an entity's success—that is, it will ensure achievement of basic business objectives or will, at the least, ensure survival.

  Even effective internal control can only *help* an entity achieve these objectives. It can provide management information about the entity's progress, or lack of it, toward their achievement. But internal control cannot change an inherently poor manager into a good one. And, shifts in government policy or programs, competitors' actions or economic conditions can be beyond management's control. Internal control cannot ensure success, or even survival.

- Internal control can ensure the reliability of financial reporting and compliance with laws and regulations.

  This belief is also unwarranted. An internal control system, no matter how well conceived and operated, can provide only reasonable—not absolute—assurance to management and the board regarding achievement of an entity's objectives. The likelihood of achievement is affected by limitations inherent in all internal control systems. These include the realities that judgments in decision-making can be faulty, and that breakdowns can occur because of simple error or mistake. Additionally, controls can be circumvented by the collusion of two or more people, and management has the ability to override the system. Another limiting factor is that the design of an internal control system must reflect the fact that there are resource constraints, and the benefits of controls must be considered relative to their costs.

Thus, while internal control can help an entity achieve its objectives, it is not a panacea.

Roles and Responsibilities

Everyone in an organization has responsibility for internal control.

- *Management*—The chief executive officer is ultimately responsible and should assume "ownership" of the system. More than any other individual, the chief executive sets the "tone at the top" that affects integrity and ethics and other factors of a positive control environment. In a large company, the chief executive fulfills this duty by providing leadership and direction to senior managers and reviewing the way they're controlling the business. Senior managers, in turn, assign responsibility for establishment of more specific internal control policies and procedures to personnel responsible for the unit's functions. In a smaller entity, the influence of the chief executive, often an owner-manager, is usually more direct. In any event, in a cascading responsibility, a manager is effectively a chief executive of his or her sphere of responsibility. Of particular significance are financial officers and their staffs, whose control activities cut across, as well as up and down, the operating and other units of an enterprise.

- *Board of Directors*—Management is accountable to the board of directors, which provides governance, guidance and oversight. Effective board members are objective, capable and inquisitive. They also have a knowledge of the entity's activities and environment, and commit the time necessary to fulfill their board responsibilities. Management may be in a position to override controls and ignore or stifle communications from subordinates, enabling a dishonest management which intentionally misrepresents results to cover its tracks. A strong, active board, particularly when coupled with effective upward communications channels and capable financial, legal and internal audit functions, is often best able to identify and correct such a problem.
- *Internal Auditors*—Internal auditors play an important role in evaluating the effectiveness of control systems, and contribute to ongoing effectiveness. Because of organizational position and authority in an entity, an internal audit function often plays a significant monitoring role.
- *Other Personnel*—Internal control is, to some degree, the responsibility of everyone in an organization and therefore should be an explicit or implicit part of everyone's job description. Virtually all employees produce information used in the internal control system or take other actions needed to effect control. Also, all personnel should be responsible for communicating upward problems in operations, noncompliance with the code of conduct, or other policy violations or illegal actions.

A number of external parties often contribute to achievement of an entity's objectives. External auditors, bringing an independent and objective view, contribute directly through the financial statement audit and indirectly by providing information useful to management and the board in carrying out their responsibilities. Others providing information to the entity useful in effecting internal control are legislators and regulators, customers and others transacting business with the enterprise, financial analysts, bond raters and the news media. External parties, however, are not responsible for, nor are they a part of, the entity's internal control system.

Organization of this Report

This report is in four volumes.* The first is this *Executive Summary,* a high-level overview of the internal control framework directed to the chief executive and other senior executives, board members, legislators and regulators.

The second volume, the *Framework,* defines internal control, describes its components and provides criteria against which managements, boards or others can assess their control systems.

The third volume, *Reporting to External Parties,* is a supplemental document providing guidance to those entities that report publicly on internal control over preparation of their published financial statements, or are contemplating doing so.

The fourth volume, *Evaluation Tools,* provides materials that may be useful in conducting an evaluation of an internal control system.

* The COSO report was issued in September 1992 as a four-volume set. An addendum to *Reporting to External Parties* was issued in May 1994. In this 1994 edition, the first three volumes and the addendum are combined and printed in one volume and *Evaluation Tools* in a second one.

What to Do

Actions that might be taken as a result of this report depend on the position and role of the parties involved:

- *Senior Management*—Most senior executives who contributed to this study believe they are basically "in control" of their organizations. Many said, however, that there are areas of their company—a division, a department or a control component that cuts across activities—where controls are in early stages of development or otherwise need to be strengthened. They do not like surprises. This study suggests that the chief executive initiate a self-assessment of the control system. Using this framework, a CEO, together with key operating and financial executives, can focus attention where needed. Under one approach, the chief executive could proceed by bringing together business unit heads and key functional staff to discuss an initial assessment of control. Directives would be provided for those individuals to discuss this report's concepts with their lead personnel, provide oversight of the initial assessment process in their areas of responsibility and report back findings. Another approach might involve an initial review of corporate and business unit policies and internal audit programs. Whatever its form, an initial self-assessment should determine whether there is a need for, and how to proceed with, a broader, more in-depth evaluation. It should also ensure that ongoing monitoring processes are in place. Time spent in evaluating internal control represents an investment, but one with a high return.
- *Board Members*—Members of the board of directors should discuss with senior management the state of the entity's internal control system and provide oversight as needed. They should seek input from the internal and external auditors.
- *Other Personnel*—Managers and other personnel should consider how their control responsibilities are being conducted in light of this framework, and discuss with more senior personnel ideas for strengthening control. Internal auditors should consider the breadth of their focus on the internal control system, and may wish to compare their evaluation materials to the evaluation tools.
- *Legislators and Regulators*—Government officials who write or enforce laws recognize that there can be misconceptions and different expectations about virtually any issue. Expectations for internal control vary widely in two respects. First, they differ regarding what control systems can accomplish. As noted, some observers believe internal control systems will, or should, prevent economic loss, or at least prevent companies from going out of business. Second, even when there is agreement about what internal control systems can and can't do, and about the validity of the "reasonable assurance" concept, there can be disparate views of what that concept means and how it will be applied. Corporate executives have expressed concern regarding how regulators might construe public reports asserting "reasonable assurance" in hindsight after an alleged control failure has occurred. Before legislation or regulation dealing with management reporting on internal control is acted upon, there should be agreement on a common internal

control framework, including limitations of internal control. This framework should be helpful in reaching such agreement.

- *Professional Organizations*—Rule-making and other professional organizations providing guidance on financial management, auditing and related topics should consider their standards and guidance in light of this framework. To the extent diversity in concept and terminology is eliminated, all parties will benefit.
- *Educators*—This framework should be the subject of academic research and analysis, to see where future enhancements can be made. With the presumption that this report becomes accepted as a common ground for understanding, its concepts and terms should find their way into university curricula.

We believe this report offers a number of benefits. With this foundation for mutual understanding, all parties will be able to speak a common language and communicate more effectively. Business executives will be positioned to assess control systems against a standard, and strengthen the systems and move their enterprises toward established goals. Future research can be leveraged off an established base. Legislators and regulators will be able to gain an increased understanding of internal control, its benefits and limitations. With all parties utilizing a common internal control framework, these benefits will be realized.

INTERNAL CONTROL – INTEGRATED FRAMEWORK

Executive Summary

► Framework

Reporting to External Parties

Addendum to "Reporting to External Parties"

Definition

Chapter Summary: Internal control is defined as a process, effected by an entity's people, designed to accomplish specified objectives. The definition is broad, encompassing all aspects of controlling a business, yet facilitates a directed focus on specific objectives. Internal control consists of five interrelated components, which are inherent in the way management runs the enterprise. The components are linked, and serve as criteria for determining whether the system is effective.

A key objective of this study is to help management of businesses and other entities better control their organizations' activities. But internal control means different things to different people. And the wide variety of labels and meanings prevents a common understanding of internal control. An important goal, then, is to integrate various internal control concepts into a framework in which a common definition is established and control components are identified. This framework is designed to accommodate most viewpoints and provide a starting point for individual entities' assessments of internal control, for future initiatives of rule-making bodies and for education.

Internal Control

Internal control is defined as follows:

> Internal control is a process, effected 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.

This definition reflects certain fundamental concepts:

- Internal control is *a process.* It's a means to an end, not an end in itself.
- Internal control is effected by *people.* It's not merely policy manuals and forms, but people at every level of an organization.
- Internal control can be expected to provide only *reasonable assurance*, not absolute assurance, to an entity's management and board.
- Internal control is geared to the achievement of *objectives* in one or more separate but overlapping categories.

This definition of internal control is broad for two reasons. First, it is the way most senior executives interviewed view internal control in managing their businesses.[1] In fact, they often speak in terms of "control" and being "in control."

[1] The term "business" as used here pertains to the activities of any entity, including government and other not-for-profit organizations.

Second, it accommodates subsets of internal control. Those who want to can focus separately, for example, on controls over financial reporting or controls related to compliance with laws and regulations. Similarly, a directed focus on controls in particular units or activities of an entity can be accommodated.

The definition also provides a basis for defining internal control effectiveness, discussed later in this chapter. The fundamental concepts outlined above are discussed in the following paragraphs.

A Process[2]

Internal control is not one event or circumstance, but a series of actions that permeate an entity's activities. These actions are pervasive, and are inherent in the way management runs the business.

Business processes, which are conducted within or across organization units or functions, are managed through the basic management processes of planning, executing and monitoring. Internal control is a part of these processes and is integrated with them. It enables them to function and monitors their conduct and continued relevancy. It is a tool used by management, not a substitute for management.

This conceptualization of internal control is very different from the perspective of some observers who view internal control as something added on to an entity's activities, or as a necessary burden, imposed by regulators or by the dictates of overzealous bureaucrats. The internal control system is intertwined with an entity's operating activities and exists for fundamental business reasons. Internal controls are most effective when they are built into the entity's infrastructure and are part of the essence of the enterprise. They should be "built in" rather than "built on."

"Building in" controls can directly affect an entity's ability to reach its goals, and supports businesses' quality initiatives. The quest for quality is directly linked to how businesses are run, and how they are controlled. Quality initiatives become part of the operating fabric of an enterprise, as evidenced by:

- Senior executive leadership ensuring that quality values are built into the way a company does business.
- Establishing quality objectives linked to the entity's information collection and analysis and other processes.
- Using the knowledge of competitive practices and customer expectations to drive continuous quality improvement.

These quality factors parallel those in effective internal control systems. In fact, internal control not only is integrated with quality programs, it usually is critical to their success.

[2] Although referred to as "a process," internal control may be viewed as a multiplicity of processes.

Building in controls also has important implications to cost containment and response time:

- Most enterprises are faced with highly competitive marketplaces and a need to contain costs. Adding new procedures separate from existing ones adds costs. By focusing on existing operations and their contribution to effective internal control, and building controls into basic operating activities, an enterprise often can avoid unnecessary procedures and costs.
- A practice of building controls into the fabric of operations helps trigger development of new controls necessary to new business activities. Such automatic reaction makes entities more nimble and competitive.

People

Internal control is effected by a board of directors, management and other personnel in an entity. It is accomplished by the people of an organization, by what they do and say. People establish the entity's objectives and put control mechanisms in place.

Similarly, internal control affects people's actions. Internal control recognizes that people do not always understand, communicate or perform consistently. Each individual brings to the workplace a unique background and technical ability, and has different needs and priorities.

These realities affect, and are affected by, internal control. People must know their responsibilities and limits of authority. Accordingly, a clear and close linkage needs to exist between people's duties and the way in which they are carried out, as well as with the entity's objectives.

The organization's people include the board of directors, as well as management and other personnel. Although directors might be viewed as primarily providing oversight, they also provide direction and approve certain transactions and policies. As such, boards of directors are an important element of internal control.

Reasonable Assurance

Internal control, no matter how well designed and operated, can provide only reasonable assurance to management and the board of directors regarding achievement of an entity's objectives. The likelihood of achievement is affected by limitations inherent in all internal control systems. These include the realities that human judgment in decision-making can be faulty, persons responsible for establishing controls need to consider their relative costs and benefits, and breakdowns can occur because of human failures such as simple error or mistake. Additionally, controls can be circumvented by collusion of two or more people. Finally, management has the ability to override the internal control system.

Objectives

Every entity sets out on a mission, establishing objectives it wants to achieve and strategies for achieving them. Objectives may be set for an entity as a whole, or be targeted to specific activities within the entity. Though many objectives are specific to a particular entity, some are widely shared. For example, objectives common to virtually all entities are achieving and

maintaining a positive reputation within the business and consumer communities, providing reliable financial statements to stakeholders, and operating in compliance with laws and regulations.

For this study, objectives fall into three categories:

- Operations — relating to effective and efficient use of the entity's resources.
- Financial reporting — relating to preparation of reliable published financial statements.
- Compliance — relating to the entity's compliance with applicable laws and regulations.

This categorization allows focusing on separate aspects of internal control. These distinct but overlapping categories (a particular objective can fall under more than one category) address different needs and may be the direct responsibility of different executives. This categorization also allows distinguishing between what can be expected from each category of internal control.

An internal control system can be expected to provide reasonable assurance of achieving objectives relating to the reliability of financial reporting and compliance with laws and regulations. Achievement of those objectives, which are based largely on standards imposed by external parties, depends on how activities within the entity's control are performed.

However, achievement of operations objectives — such as a particular return on investment, market share or entry into new product lines — is not always within the entity's control. Internal control cannot prevent bad judgments or decisions, or external events that can cause a business to fail to achieve operations goals. For these objectives, the internal control system can provide reasonable assurance only that management and, in its oversight role, the board are made aware, in a timely manner, of the extent to which the entity is moving toward those objectives.

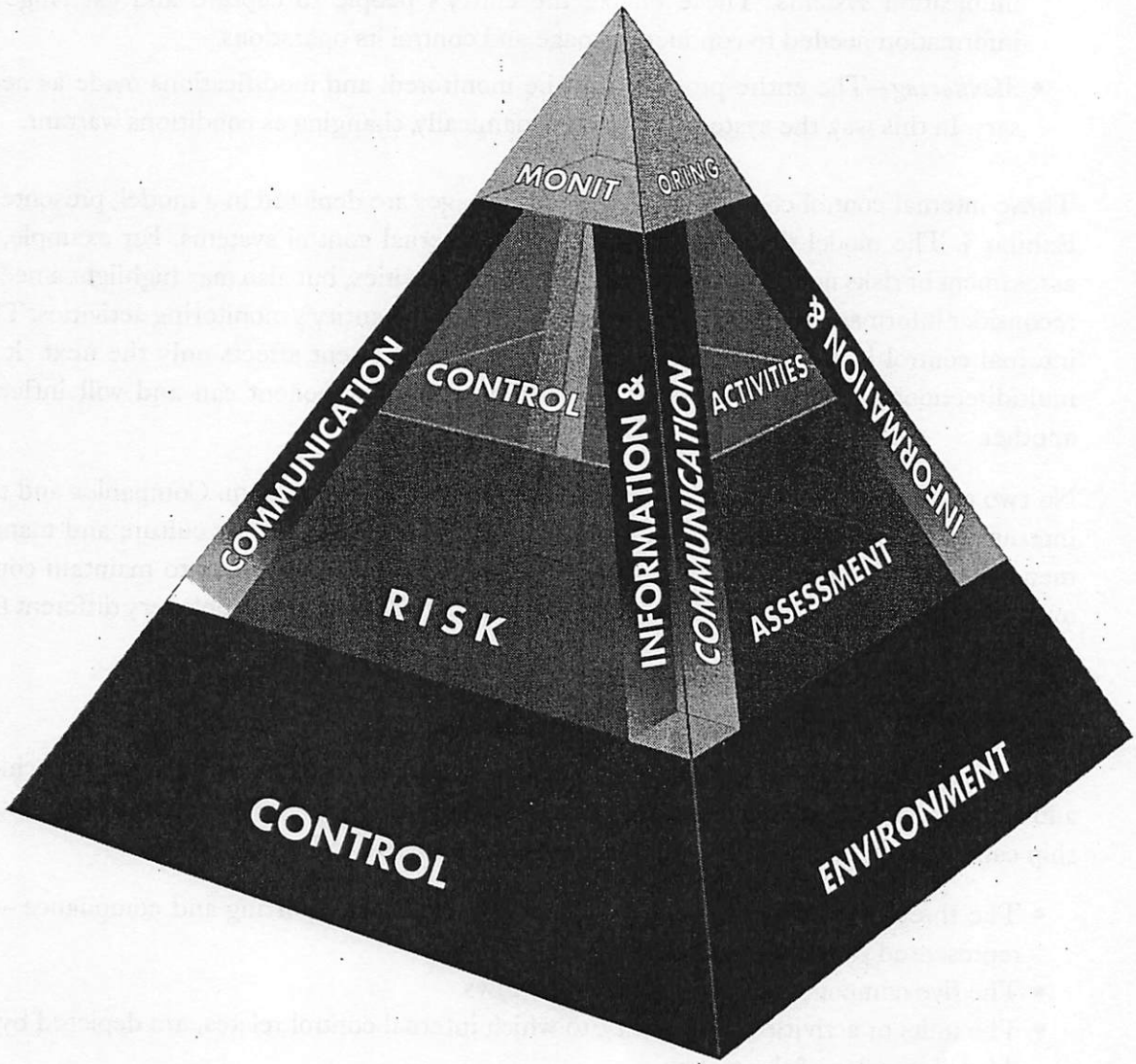
Components

Internal control consists of five interrelated components. These are derived from the way management runs a business, and are integrated with the management process. The components are:

- *Control Environment*—The core of any business is its people — their individual attributes, including integrity, ethical values and competence — and the environment in which they operate. They are the engine that drives the entity and the foundation on which everything rests.
- *Risk Assessment*—The entity must be aware of and deal with the risks it faces. It must set objectives, integrated with the sales, production, marketing, financial and other activities so that the organization is operating in concert. It also must establish mechanisms to identify, analyze and manage the related risks.

Exhibit 1

Internal Control Components



The *control environment* provides an atmosphere in which people conduct their activities and carry out their control responsibilities. It serves as the foundation for the other components. Within this environment, management *assesses risks* to the achievement of specified objectives. *Control activities* are implemented to help ensure that management directives to address the risks are carried out. Meanwhile, relevant *information* is captured and *communicated* throughout the organization. The entire process is *monitored* and modified as conditions warrant.

- *Control Activities*— Control policies and procedures must be established and executed to help ensure that the actions identified by management as necessary to address risks to achievement of the entity's objectives are effectively carried out.
- *Information and Communication*— Surrounding these activities are information and communication systems. These enable the entity's people to capture and exchange the information needed to conduct, manage and control its operations.
- *Monitoring*—The entire process must be monitored, and modifications made as necessary. In this way, the system can react dynamically, changing as conditions warrant.

These internal control components and their linkages are depicted in a model, presented in Exhibit 1. The model depicts the dynamism of internal control systems. For example, the assessment of risks not only influences the control activities, but also may highlight a need to reconsider information and communication needs, or the entity's monitoring activities. Thus, internal control is not a serial process, where one component affects only the next. It is a multidirectional iterative process in which almost any component can and will influence another.

No two entities will, or should, have the same internal control system. Companies and their internal control needs differ dramatically by industry and size, and by culture and management philosophy. Thus, while all entities need each of the components to maintain control over their activities, one company's internal control system often will look very different from another's.

Relationship of Objectives and Components

There is a direct relationship between objectives, which are what an entity strives to achieve, and the components, which represent what is needed to achieve the objectives. The relationship can be depicted by a three-dimensional matrix, shown in Exhibit 2:

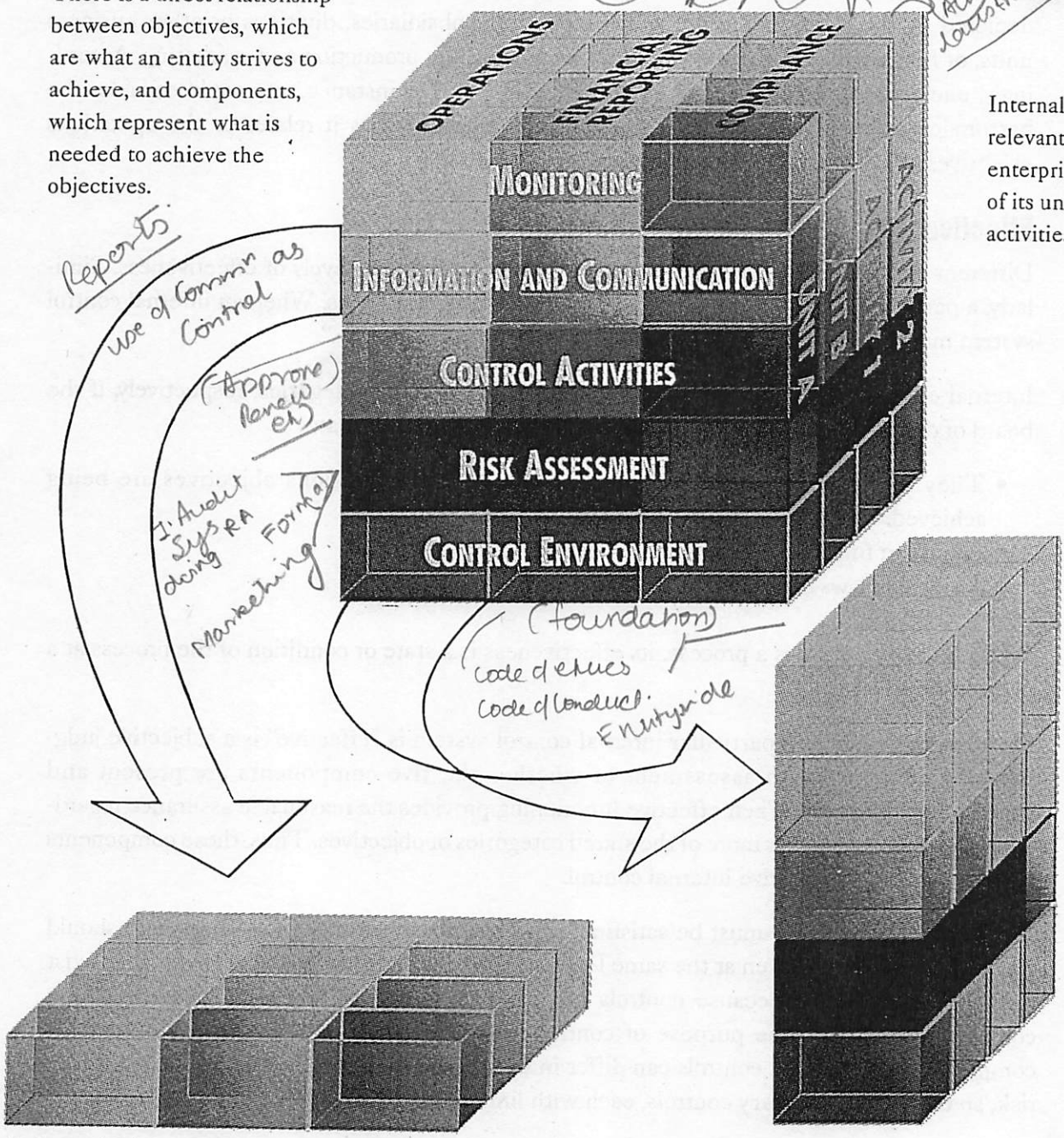
- The three objectives categories — operations, financial reporting and compliance — are represented by the vertical columns.
- The five components are represented by rows.
- The units or activities of an entity, to which internal control relates, are depicted by the third dimension of the matrix.

Each component row "cuts across" and applies to all three objectives categories. An example is depicted separately at the bottom left of the exhibit, as a "pull out" section: Financial and non-financial data generated from internal and external sources, which is part of the information and communication component, is needed to effectively manage business operations, develop reliable financial statements and determine that the entity is complying with applicable laws. Another example (not depicted separately), the establishment and execution of control policies and procedures to ensure that management plans, programs and other directives are carried out—representing the control activities component— is also relevant to all three objectives categories.

Exhibit 2

Relationship of Objectives and Components

There is a direct relationship between objectives, which are what an entity strives to achieve, and components, which represent what is needed to achieve the objectives.



Internal control is relevant to an entire enterprise, or to any of its units or activities.

Information is needed for all three objectives categories — to effectively manage business operations, prepare financial statements reliably and determine compliance.

All five components are applicable and important to achievement of operations objectives.

Similarly, looking at the objectives categories, all five components are relevant to each. Taking one category, effectiveness and efficiency of operations, for example, all five components are applicable and important to its achievement. This is illustrated separately at the bottom right of the exhibit.

Internal control is relevant to an entire enterprise, or to one of its parts. This relationship is depicted by the third dimension, which represents subsidiaries, divisions or other business units, or functional or other activities such as purchasing, production and marketing. Accordingly, one could focus on any one of the matrix's cells. For instance, one could consider the bottom-left-front cell, representing the control environment as it relates to the operations objectives of a particular company division.

Effectiveness

Different entities' internal control systems operate at different levels of effectiveness. Similarly, a particular system may operate differently at different times. When an internal control system meets the following standard, it can be deemed "effective."

Internal control can be judged effective in each of the three categories, respectively, if the board of directors and management have reasonable assurance that:

- They understand the extent to which the entity's operations objectives are being achieved.
- Published financial statements are being prepared reliably.
- Applicable laws and regulations are being complied with.

While internal control is a process, its effectiveness is a state or condition of the process at a point in time.

Determining whether a particular internal control system is "effective" is a subjective judgment resulting from an assessment of whether the five components are present and functioning effectively. Their effective functioning provides the reasonable assurance regarding achievement of one or more of the stated categories of objectives. Thus, these components are also criteria for effective internal control.

Although all five criteria must be satisfied, this does not mean that each component should function identically, or even at the same level, in different entities. Some trade-offs may exist between components. Because controls can serve a variety of purposes, controls in one component can serve the purpose of controls that might normally be present in another component. Additionally, controls can differ in the degree to which they address a particular risk, so that complementary controls, each with limited effect, together can be satisfactory.

These components and criteria apply to an entire internal control system, or to one or more objectives categories. When considering any one category — controls over financial reporting, for example — all five criteria must be satisfied in order to conclude that internal control over financial reporting is effective.

The following chapters should be considered when determining whether an internal control system is effective. It should be recognized:

- Because internal control is a part of the management process, the components are discussed in the context of what management does in running a business. Not everything management does, however, is an element of internal control. Establishment of objectives, for example, while an important management responsibility, is a precondition to internal control. Similarly, many decisions and actions by management do not represent internal control. Exhibit 3 lists common management actions and indicates which ones are considered components of internal control. (This listing purports neither to be all-inclusive nor to depict the only way to describe management activities.)
- The principles discussed apply to all entities, regardless of size. While some small and mid-size entities may implement component factors differently than large ones, they still can have effective internal control. Each component chapter has a section illustrating such circumstances.
- Each component chapter contains an "evaluation" section with factors one might consider in evaluating the component. Those factors are not intended to be all-inclusive, nor are all of them relevant to every circumstance. They are offered as illustrations for developing a more comprehensive or tailored evaluation program.

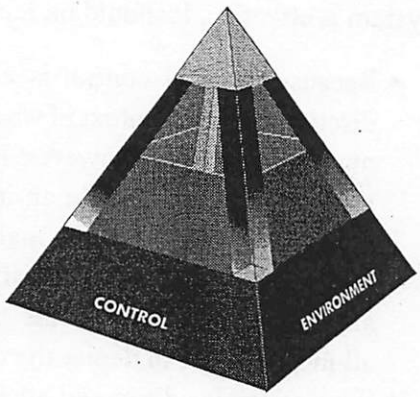
Exhibit 3

Internal Control and the Management Process

Management Activities	Internal Control
Entity-level objective setting—mission, value statements	
Strategic planning	
Establishing control environment factors	✓
Activity-level objective setting	
Risk identification and analysis	✓
Risk management	
Conducting control activities	✓
Information identification, capture and communication	✓
Monitoring	✓
Corrective actions	

Control Environment

Chapter Summary: The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values and competence of the entity's people; management's philosophy and operating style; the way management assigns authority and responsibility, and organizes and develops its people; and the attention and direction provided by the board of directors.



The control environment has a pervasive influence on the way business activities are structured, objectives established and risks assessed. It also influences control activities, information and communication systems, and monitoring activities. This is true not only of their design, but also the way they work day to day. The control environment is influenced by the entity's history and culture. It influences the control consciousness of its people. Effectively controlled entities strive to have competent people, instill an enterprise-wide attitude of integrity and control consciousness, and set a positive "tone at the top." They establish appropriate policies and procedures, often including a written code of conduct, which foster shared values and teamwork in pursuit of the entity's objectives.

Control Environment Factors

The control environment encompasses factors discussed below. Although all are important, the extent to which each is addressed will vary with the entity. For example, the chief executive of an entity with a small workforce and centralized operations may not establish formal lines of responsibility and detailed operating policies, but could nevertheless have an appropriate control environment.

Integrity and Ethical Values

An entity's objectives and the way they are achieved are based on preferences, value judgments and management styles. Those preferences and value judgments, which are translated into standards of behavior, reflect management's integrity and its commitment to ethical values.

Because an entity's good reputation is so valuable, the standard of behavior must go beyond mere compliance with law. In awarding reputation to the best companies, society expects more than that.

The effectiveness of internal controls cannot rise above the integrity and ethical values of the people who create, administer and monitor them. Integrity and ethical values are essential elements of the control environment, affecting the design, administration and monitoring of other internal control components.

Integrity is a prerequisite for ethical behavior in all aspects of an enterprise's activities. As the Treadway Commission reported, "A strong corporate ethical climate at all levels is vital to the well-being of the corporation, all of its constituencies, and the public at large. Such a climate contributes importantly to the effectiveness of company policies and control systems, and helps influence behavior that is not subject to even the most elaborate system of controls."[1]

Establishing ethical values often is difficult because of the need to consider the concerns of several parties. Top management's values must balance the concerns of the enterprise, its employees, suppliers, customers, competitors and the public. Balancing these concerns can be a complex and frustrating effort because interests often are at odds. For example, providing an essential product (petroleum, lumber or food) may cause some environmental concerns.

Managers of well-run enterprises have increasingly accepted the view that "ethics pays"—that ethical behavior is good business. Positive and negative examples abound. The well-publicized handling by a pharmaceutical company of a crisis involving tampering with one of its major products was both sound ethics and sound business. The impact on customer relations or stock prices of slowly leaked bad news, such as profit shortfalls or illegal acts, generally is worse than if full disclosures are made as quickly as possible.

Focusing solely on short-term results can hurt even in the short term. Concentration on the bottom line—sales or profit at any cost—often evokes unsought actions and reactions. High-pressure sales tactics, ruthlessness in negotiations or implicit offers of kickbacks, for instance, may evoke reactions that can have immediate (as well as lasting) effects.

Ethical behavior and management integrity are a product of the "corporate culture." Corporate culture includes ethical and behavioral standards, how they are communicated and how they are reinforced in practice. Official policies specify what management wants to happen. Corporate culture determines what actually happens, and which rules are obeyed, bent or ignored. Top management—starting with the CEO—plays a key role in determining the corporate culture. The CEO usually is the dominant personality in an organization, and individually often sets its ethical tone.

Incentives and Temptations. A study[2] several years ago suggested that certain organizational factors can influence the likelihood of fraudulent and questionable financial reporting practices. Those same factors also are likely to influence ethical behavior.

Individuals may engage in dishonest, illegal or unethical acts simply because their organizations give them strong incentives or temptations to do so. Emphasis on "results," particularly in the short term, fosters an environment in which the price of failure becomes very high.

[1] *Report of the National Commission on Fraudulent Financial Reporting* (National Commission on Fraudulent Financial Reporting, 1987).

[2] Kenneth A. Merchant, *Fraudulent and Questionable Financial Reporting: A Corporate Perspective* (Morristown, NJ: Financial Executives Research Foundation, 1987).

Incentives cited for engaging in fraudulent or questionable financial reporting practices and, by extension, other forms of unethical behavior are:

- Pressure to meet unrealistic performance targets, particularly for short-term results,
- High performance-dependent rewards, and
- Upper and lower cutoffs on bonus plans.

The study also cites "temptations" for employees to engage in improper acts:

- 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 organizational levels and thereby reduces the chances of getting caught.
- A weak internal audit function that does not have the ability to detect and report improper behavior.
- An ineffective board of directors that does not provide objective oversight of top management.
- Penalties for improper behavior that are insignificant or unpublicized and thus lose their value as deterrents.

Removing or reducing these incentives and temptations can go a long way toward diminishing undesirable behavior. As suggested, this can be achieved following sound and profitable business practices. For example, performance incentives—accompanied by appropriate controls—can be a useful management technique as long as the performance targets are realistic. Setting realistic performance targets is a sound motivational practice; it reduces counterproductive stress as well as the incentive for fraudulent financial reporting that unrealistic targets create. Similarly, a well-controlled reporting system can serve as a safeguard against temptation to misstate performance.

Providing and Communicating Moral Guidance. In addition to the incentives and temptations just discussed, the aforementioned study found a third cause of fraudulent and questionable financial reporting practices: ignorance. The study found that "in many of the companies that have suffered instances of deceptive financial reporting, the people involved either did not know what they were doing was wrong or erroneously believed they were acting in the organization's best interest." This ignorance is often caused by poor moral background or guidance, rather than by an intent to deceive. Thus, not only must ethical values be communicated, but explicit guidance must be given regarding what is right and wrong.

The most effective way of transmitting a message of ethical behavior throughout the organization is by example. People imitate their leaders. Employees are likely to develop the same attitudes about what's right and wrong—and about internal control—as those shown by top management. Knowledge that the CEO has "done the right thing" ethically when faced with a tough business decision sends a strong message to all levels of the organization.

Setting a good example is not enough. Top management should verbally communicate the entity's values and behavioral standards to employees. A study[3] some years ago noted that a formal code of corporate conduct is "a widely used method of communicating to employees the company's expectations about duty and integrity." Codes address a variety of behavioral issues, such as integrity and ethics, conflicts of interest, illegal or otherwise improper payments, and anti-competitive arrangements. Spurred in part by revelations of scandals in the defense industry, many companies have adopted such codes in recent years, along with necessary communications channels and monitoring. While codes of conduct can be helpful, they are not the only way to transmit an organization's ethical values to employees, suppliers and customers.

Existence of a written code of conduct, and even documentation that employees received and understand it, does not ensure that it is being followed. Compliance with ethical standards, whether or not embodied in a written code of conduct, is best ensured by top management's actions and examples. Of particular importance are resulting penalties to employees who violate such codes, mechanisms that exist to encourage employee reporting of suspected violations, and disciplinary actions against employees who fail to report violations. Messages sent by management's actions in these situations quickly become embodied in the corporate culture.

Commitment to Competence

Competence should reflect the knowledge and skills needed to accomplish tasks that define the individual's job. How well these tasks need to be accomplished generally is a management decision which should be made considering the entity's objectives and management's strategies and plans for achievement of the objectives. There often is a trade-off between competence and cost—it is not necessary, for instance, to hire an electrical engineer to change a light bulb.

Management needs to specify the competence levels for particular jobs and to translate those levels into requisite knowledge and skills. The necessary knowledge and skills may in turn depend on individuals' intelligence, training and experience. Among the many factors considered in developing knowledge and skill levels are the nature and degree of judgment to be applied to a specific job. There often can be a trade-off between the extent of supervision and the requisite competence level of the individual.

Board of Directors or Audit Committee

The control environment and "tone at the top" are influenced significantly by the entity's board of directors and audit committee. Factors include the board or audit committee's independence from management, experience and stature of its members, extent of its involvement and scrutiny of activities, and the appropriateness of its actions. Another factor is the degree to which difficult questions are raised and pursued with management regarding

[3] R.K. Mautz and J. Winjum, *Criteria for Management Control Systems* (New York: Financial Executives Research Foundation, 1981).

plans or performance. Interaction of the board or audit committee with internal and external auditors is another factor affecting the control environment.

Because of its importance, an active and involved board of directors, board of trustees or comparable body—possessing an appropriate degree of management, technical and other expertise coupled with the necessary stature and mind set so that it can adequately perform the necessary governance, guidance and oversight responsibilities—is critical to effective internal control. And, because a board must be prepared to question and scrutinize management's activities, present alternative views and have the courage to act in the face of obvious wrongdoing, it is necessary that the board contain outside directors. Certainly, officers and employees often are highly effective and important board members, bringing knowledge of the company to the table. But there must be a balance. Although small and even mid-size companies may find it difficult to attract or incur the cost of having a majority of outside directors—usually not the case with large organizations—it is important that the board contain at least a critical mass of outside directors. The number should suit the entity's circumstances, but more than one outside director normally would be needed for a board to have the requisite balance.

The need for and responsibilities of boards of directors and audit committees are discussed further below under "Application to Small and Mid-Size Entities," and in Chapter 8.

Management's Philosophy and Operating Style

Management's philosophy and operating style affect the way the enterprise is managed, including the kinds of business risks accepted. An entity that has been successful taking significant risks may have a different outlook on internal control than one that has faced harsh economic or regulatory consequences as a result of venturing into dangerous territory. An informally managed company may control operations largely by face-to-face contact with key managers. A more formally managed one may rely more on written policies, performance indicators and exception reports.

Other elements of management's philosophy and operating style include attitudes toward financial reporting, conservative or aggressive selection from available alternative accounting principles, conscientiousness and conservatism with which accounting estimates are developed, and attitudes toward data processing and accounting functions and personnel. How management meets its responsibilities is discussed further in Chapter 8.

Organizational Structure

An entity's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled and monitored. Activities may relate to what is sometimes referred to as the value chain: inbound (receiving) activities, operations or production, outbound (shipping), marketing, sales and service. There may be support functions, relating to administration, human resources or technology development.[4]

[4] Michael E. Porter, *Competitive Advantage* (New York: Free Press, 1985).

Significant aspects of establishing a relevant organizational structure include defining key areas of authority and responsibility and establishing appropriate lines of reporting. For example, the internal audit department should have unrestricted access to a senior officer who is not directly responsible for preparing the company's financial statements and has sufficient authority to ensure appropriate audit coverage and to follow up on findings and recommendations.

An entity develops an organizational structure suited to its needs. Some are centralized, others decentralized. Some have direct reporting relationships, others are more of a matrix organization. Some entities are organized by industry or product line, by geographical location or by a particular distribution or marketing network. Other entities, including many state and local governmental units and not-for-profit institutions, are organized on a functional basis.

The appropriateness of an entity's organizational structure depends, in part, on its size and the nature of its activities. A highly structured organization, including formal reporting lines and responsibilities, may be appropriate for a large entity with numerous operating divisions, including foreign operations. However, it could impede the necessary flow of information in a small entity. Whatever the structure, an entity's activities will be organized to carry out the strategies designed to achieve particular objectives.

Assignment of Authority and Responsibility

This includes assignment of authority and responsibility for operating activities, and establishment of reporting relationships and authorization protocols. It involves the degree to which individuals and teams are encouraged to use initiative in addressing issues and solving problems, as well as limits of their authority. It also deals with policies describing appropriate business practices, knowledge and experience of key personnel, and resources provided for carrying out duties.

There is a growing tendency to push authority downward to bring decision-making closer to front-line personnel. An entity may take this tack to become more market-driven or quality focused—perhaps to eliminate defects, reduce cycle time or increase customer satisfaction. To do so, the enterprise needs to recognize and respond to changing priorities in market opportunities, business relationships and public expectations. Alignment of authority and accountability often is designed to encourage individual initiatives, within limits. Delegation of authority, or "empowerment," means surrendering central control of certain business decisions to lower echelons—to the individuals who are closest to everyday business transactions. This may involve empowerment to sell products at discount prices; negotiate long-term supply contracts, licenses or patents; or enter alliances or joint ventures.

A critical challenge is to delegate only to the extent required to achieve objectives. This requires ensuring that risk acceptance is based on sound practices for identification and minimization of risk, including sizing risks and weighing potential losses versus gains in arriving at good business decisions.

Another challenge is ensuring that all personnel understand the entity's objectives. It is essential that each individual knows how his or her actions interrelate and contribute to achievement of the objectives.

Increased delegation sometimes is accompanied by or the result of streamlining or "flattening" of an entity's organizational structure, and is intentional. Purposeful structural change to encourage creativity, initiative and the capability to react quickly can enhance competitiveness and customer satisfaction. Such increased delegation may carry an implicit requirement for a higher level of employee competence, as well as greater accountability. It also requires effective procedures for management to monitor results. Along with better, market-driven decisions, empowerment may increase the number of undesirable or unanticipated decisions. If a district sales manager decides that authorization to sell at 35% off list justifies a temporary 45% discount to gain market share, management may need to know so that it can overrule or accept such decisions going forward.

The control environment is greatly influenced by the extent to which individuals recognize that 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 the internal control system.

Human Resource Policies and Practices

Human resource practices send messages to employees regarding expected levels of integrity, ethical behavior and competence. Such practices relate to hiring, orientation, training, evaluating, counseling, promoting, compensating and remedial actions. For example, standards for hiring the most qualified individuals, with emphasis on educational background, prior work experience, past accomplishments and evidence of integrity and ethical behavior, demonstrate an entity's commitment to competent and trustworthy people. Recruiting practices that include formal, in-depth employment interviews and informative and insightful presentations on the entity's history, culture and operating style send a message that the entity is committed to its people. Training policies that communicate prospective roles and responsibilities and include practices such as training schools and seminars, simulated case studies and role-play exercises, illustrate expected levels of performance and behavior. Rotation of personnel and promotions driven by periodic performance appraisals demonstrate the entity's commitment to the advancement of qualified personnel to higher levels of responsibility. Competitive compensation programs that include bonus incentives serve to motivate and reinforce outstanding performance. Disciplinary actions send a message that violations of expected behavior will not be tolerated.

It is essential that personnel be equipped for new challenges as issues that enterprises face change and become more complex—driven in part by rapidly changing technologies and increasing competition. Education and training, whether classroom instruction, self-study or on-the-job training, must prepare an entity's people to keep pace and deal effectively with the evolving environment. They will also strengthen the entity's ability to effect quality initiatives. Hiring of competent people and one-time training are not enough. The education process must be ongoing.

Differences and Implications

The control environment of an entity's autonomous operating divisions and foreign and domestic subsidiaries can vary widely due to differences in senior operating management's preferences, value judgments and management styles. These control environments may vary for any number of reasons. Since no two operating divisions or foreign or domestic subsidiaries are managed in the same way, it is unlikely that control environments will be the same. It is important, therefore, to recognize the effect that varying control environments can have on the other components of a system of internal control.

The impact of an ineffective control environment could be far reaching, possibly resulting in a financial loss, a tarnished public image or a business failure. Consider, for example, the case of a defense contractor generally considered to have effective internal control. The company had well-designed information systems and control activities, extensive policy manuals prescribing control functions, and extensive reconciling and supervisory routines. It underwent frequent government audits. The control environment, however, was significantly flawed. Senior management did not want to know if wrongdoing occurred. Even when signs of fraudulent activities became strong, senior management officials practiced denial. The defense contractor was found to have engaged in fraudulent activities at the Pentagon, was assessed a significant fine and suffered public embarrassment from extensive media coverage.

The attitude and concern of top management for effective internal control must permeate the organization. It is not sufficient to say the right words. An attitude of "do as I say, not as I do" surely will bring about an unhealthy environment.

Application to Small and Mid-Size Entities

While every entity should embrace the concepts underlying the discussion in this chapter, small and mid-size entities may implement the control environment factors differently than larger entities. For example, a small company might not have a written code of conduct, but that does not necessarily mean the company could not have a culture that emphasizes the importance of integrity and ethical behavior. Through the visibility and direct involvement of the CEO or owner-manager and top managers, their commitment to integrity and ethical behavior can be communicated orally—in staff meetings, one-on-one meetings and dealings with vendors and customers. Their own integrity and behavior, however, is critical and must be consistent with the oral message because of the first-hand contact that employees have with them. Usually, the fewer the levels of management, the faster the message is carried through an organization of what conduct is acceptable.

Similarly, human resource policies may not be formalized, as one would expect in a larger entity. Policies and practices can nevertheless exist and be communicated. The CEO can orally make explicit his or her expectations about the type of person to be hired to fill a particular job, and may even be active in the hiring process. Formal documentation is not always necessary for a policy to be in place and operating effectively.

Because of the critical importance of a board of directors or comparable body, even small entities generally need the benefit of such a body for effective internal control. As noted, often it is more difficult and costly for a small company to maintain a majority of outside directors — and it may be unnecessary to do so. The needed independence often can be gained with a smaller number of outside directors. The overriding factor is that there exist what can be termed a "critical mass," which, simply, is enough outside directors to see that the board raises the tough issues and takes the difficult actions when necessary. There is one exception to the general need for such a board. Where an entity is owner-managed, and does not go outside for capital, a board, though perhaps still useful, usually is not essential to effective internal control.

Evaluation

An evaluator should consider each control environment factor in determining whether a positive control environment exists. Listed below are issues on which one might focus. This list is not all-inclusive, nor will every item apply to every entity; it can, however, serve as a starting point. Although some of the items are highly subjective and require considerable judgment, they generally are relevant to control environment effectiveness.

Integrity and Ethical Values

- Existence and implementation of codes of conduct and other policies regarding acceptable business practice, conflicts of interest, or expected standards of ethical and moral behavior.
- Dealings with employees, suppliers, customers, investors, creditors, insurers, competitors, and auditors, etc. (e.g., whether management conducts business on a high ethical plane, and insists that others do so, or pays little attention to ethical issues).
- Pressure to meet unrealistic performance targets — particularly for short-term results — and extent to which compensation is based on achieving those performance targets.

Commitment to Competence

- Formal or informal job descriptions or other means of defining tasks that comprise particular jobs.
- Analyses of the knowledge and skills needed to perform jobs adequately.

Board of Directors or Audit Committee

- Independence from management, such that necessary, even if difficult and probing, questions are raised.
- Frequency and timeliness with which meetings are held with chief financial and/or accounting officers, internal auditors and external auditors.
- Sufficiency and timeliness with which information is provided to board or committee members, to allow monitoring of management's objectives and strategies, the entity's financial position and operating results, and terms of significant agreements.
- Sufficiency and timeliness with which the board or audit committee is apprised of sensitive information, investigations and improper acts (e.g., travel expenses of senior

officers, significant litigation, investigations of regulatory agencies, defalcations, embezzlement or misuse of corporate assets, violations of insider trading rules, political payments, illegal payments).

Management's Philosophy and Operating Style

- Nature of business risks accepted, e.g., whether management often enters into particularly high-risk ventures, or is extremely conservative in accepting risks.
- Frequency of interaction between senior management and operating management, particularly when operating from geographically removed locations.
- Attitudes and actions toward financial reporting, including disputes over application of accounting treatments (e.g., selection of conservative versus liberal accounting policies; whether accounting principles have been misapplied, important financial information not disclosed, or records manipulated or falsified).

Organizational Structure

- Appropriateness of the entity's organizational structure, and its ability to provide the necessary information flow to manage its activities.
- Adequacy of definition of key managers' responsibilities, and their understanding of these responsibilities.
- Adequacy of knowledge and experience of key managers in light of responsibilities.

Assignment of Authority and Responsibility

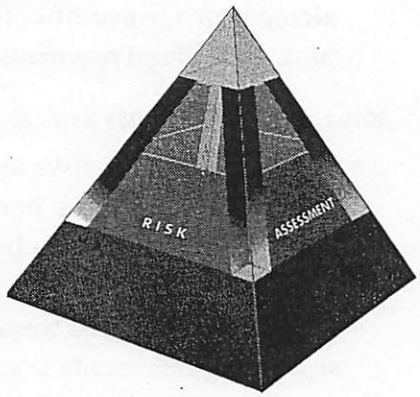
- Assignment of responsibility and delegation of authority to deal with organizational goals and objectives, operating functions and regulatory requirements, including responsibility for information systems and authorizations for changes.
- Appropriateness of control-related standards and procedures, including employee job descriptions.
- Appropriate numbers of people, particularly with respect to data processing and accounting functions, with the requisite skill levels relative to the size of the entity and nature and complexity of activities and systems.

Human Resource Policies and Practices

- Extent to which policies and procedures for hiring, training, promoting and compensating employees are in place.
- Appropriateness of remedial action taken in response to departures from approved policies and procedures.
- Adequacy of employee candidate background checks, particularly with regard to prior actions or activities considered to be unacceptable by the entity.
- Adequacy of employee retention and promotion criteria and information-gathering techniques (e.g., performance evaluations) and relation to the code of conduct or other behavioral guidelines.

Risk Assessment

Chapter Summary: Every entity faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is establishment of objectives, linked at different levels and internally consistent. Risk assessment is the identification and analysis of relevant risks to achievement of the objectives, forming a basis for determining how the risks should be managed. Because economic, industry, regulatory and operating conditions will continue to change, mechanisms are needed to identify and deal with the special risks associated with change.



All entities, regardless of size, structure, nature or industry, encounter risks at all levels within their organizations. Risks affect each entity's ability to survive; successfully compete within its industry; maintain its financial strength and positive public image; and maintain the overall quality of its products, services and people. There is no practical way to reduce risk to zero. Indeed, the decision to be in business creates risk. Management must determine how much risk is to be prudently accepted, and strive to maintain risk within these levels.

Objective setting is a precondition to risk assessment. There must first be objectives before management can identify risks to their achievement and take necessary actions to manage the risks. Objective setting, then, is a key part of the management process. While not an internal control component, it is a prerequisite to and enabler of internal control. This chapter first discusses objectives, followed by the discussion of risks.

Objectives

Objective setting can be a highly structured or an informal process. Objectives may be explicitly stated, or be implicit, such as to continue a past level of performance. At the entity level, objectives often are represented by the entity's mission and value statements. Along with assessments of the entity's strengths and weaknesses, and of opportunities and threats, they lead to an overall strategy. Generally, the strategic plan is broadly stated, dealing with high-level resource allocations and priorities.

More-specific objectives flow from the entity's broad strategy. Entity-level objectives are linked and integrated with more-specific objectives established for various "activities," such as sales, production and engineering, making sure they are consistent. These subobjectives, or activity-level objectives, include establishing goals and may deal with product line, market, financing and profit objectives.

By setting objectives at the entity and activity levels, an entity can identify critical success factors. These are key things that must go right if goals are to be attained. Critical success

factors exist for the entity, a business unit, a function, a department or an individual. Objective setting enables management to identify measurement criteria for performance, with focus on critical success factors.

Categories of Objectives

Despite the diversity of objectives, certain broad categories can be established:

- *Operations Objectives*—These pertain to effectiveness and efficiency of the entity's operations, including performance and profitability goals and safeguarding resources against loss. They vary based on management's choices about structure and performance.
- *Financial Reporting Objectives*—These pertain to the preparation of reliable published financial statements, including prevention of fraudulent public financial reporting. They are driven primarily by external requirements.
- *Compliance Objectives*—These objectives pertain to adherence to laws and regulations to which the entity is subject. They are dependent on external factors, such as environmental regulation, and tend to be similar across all entities in some cases and across an industry in others.

Certain objectives follow from the business an entity is in. A mutual fund must value its holdings daily, whereas another business might do this quarterly. All publicly traded businesses must make certain filings with the SEC. These externally imposed objectives are established by law or regulation, and fall in the category of compliance, and perhaps financial reporting.

Conversely, operations objectives are based more on preferences, judgments and management style. They vary widely among entities simply because informed, competent and honest people may select different objectives. Regarding product development, for example, one entity might choose to be an early adapter, another a quick follower, and yet another a slow lagger. These choices will affect the structure, skills, staffing and controls of the research and development function. Consequently, no one formulation of objectives can be optimal for all entities.

Operations Objectives. Operations objectives relate to achievement of an entity's basic mission—the fundamental reason for its existence. They include related subobjectives for operations, directed at enhancing effectiveness and efficiency in moving the enterprise toward its ultimate goal.

Operations objectives need to reflect the particular business, industry and economic environments in which the entity functions. The objectives need, for example, to be relevant to competitive pressures for quality, reduced cycle times to bring product to market, or changes in technology. Management must see to it that objectives are based on the reality and demands of the marketplace and are expressed in terms that allow meaningful performance measurements.

A clear set of operations objectives and strategies, linked to subobjectives, is fundamental to success. They provide a focal point toward which the entity will commit substantial resources. If an entity's operations objectives are not clear or well conceived, its resources may be misdirected.

Financial Reporting Objectives. Financial reporting objectives address the preparation of reliable published financial statements, including interim and condensed financial statements and selected financial data derived from such statements, such as earnings releases, reported publicly. Entities need to achieve financial reporting objectives to meet external obligations. Reliable financial statements are a prerequisite to obtaining investor or creditor capital, and may be critical to the award of certain contracts or to dealing with certain suppliers. Investors, creditors, customers and suppliers often rely on financial statements to assess management's performance and to compare it with peers and alternative investments.

The term "reliability" as used with financial reporting objectives involves the preparation of financial statements that are fairly presented in conformity with generally accepted or other relevant and appropriate accounting principles and regulatory requirements for external purposes. Fair presentation is defined[1] as:

- The accounting principles selected and applied have general acceptance,
- The accounting principles are appropriate in the circumstances,
- The financial statements are informative of matters that may affect their use, understanding and interpretation,
- The information presented is classified and summarized in a reasonable manner, that is, it is neither too detailed nor too condensed, and
- The financial statements reflect the underlying transactions and events[2] in a manner that presents the financial position, results of operations and cash flows stated within a range

[1] Statement on Auditing Standards No. 69, *The Meaning of "Present Fairly in Conformity With Generally Accepted Accounting Principles" in the Independent Auditor's Report* (New York: AICPA, 1992).

[2] A transaction is an exchange between the entity and an outside party. The sale of products or services to customers, and the purchase of products or services from suppliers, are examples of transactions. An event is another occurrence that can affect financial reporting. For example, a decline in market value of short-term investments below cost, and a ban on the future sale of certain pharmaceuticals in product inventory, are events that affect financial reporting. Such events include transfers within an entity, and allocations and amortization of costs on either a time basis or a measurement of effort or usage. Applying direct costs during production, and allocating manufacturing overhead costs and costs of depreciable assets, are occurrences that affect financial reporting.

Events differ from transactions in that they do not involve an exchange between the entity and an outside party. The primary purpose of distinguishing among these occurrences is to recognize that exchanges with outside parties are not the only matters that can affect financial reporting. Often, special attention must be given to identifying these events, since they will not always be evident from daily operations.

It should be recognized that often considerable judgment, estimates and forecasting future activities are represented in the financial reporting process.

of acceptable limits, that is, limits that are reasonable and practical to attain in financial statements.

Also inherent in fair presentation is the concept of financial statement materiality.

Supporting these objectives is a series of assertions that underlie an entity's financial statements[3]:

- *Existence or Occurrence*—Assets, liabilities and ownership interests exist at a specific date, and recorded transactions represent events that actually occurred during a certain period.
- *Completeness*—All transactions and other events and circumstances that occurred during a specific period, and should have been recognized in that period, have, in fact, been recorded.
- *Rights and Obligations*—Assets are the rights, and liabilities are the obligations, of the entity at a given date.
- *Valuation or Allocation*—Asset, liability, revenue and expense components are recorded at appropriate amounts in conformity with relevant and appropriate accounting principles. Transactions are mathematically correct and appropriately summarized, and recorded in the entity's books and records.
- *Presentation and Disclosure*—Items in the statements are properly described, sorted and classified.

As with the other objectives categories, a series of objectives and related subobjectives exists. The factors representing fair presentation can be viewed as basic financial reporting objectives. These would be supported by subobjectives represented by the financial statement assertions, which in turn are supported by related objectives identified with respect to an entity's various activities.

While these definitions of fair presentation and assertions were set forth for financial statements, they also, at least conceptually, underlie the development of other published financial reports derived from financial statements, such as interim financial information and press releases of earnings reports. Certain of these factors, however, would not be applicable to other published financial reports. For example, the presentation and disclosure assertion generally would not be applicable to an earnings release.

Compliance Objectives. Entities must conduct their activities, and often take specific actions, in accordance with applicable laws and regulations. These requirements may relate, for example, to markets, pricing, taxes, the environment, employee welfare and international trade. These laws and regulations establish minimum standards of behavior which the entity

[3] Statement on Auditing Standards No. 31, *Evidential Matter* (New York: AICPA, 1980).

integrates into its compliance objectives. For example, occupational safety and health regulations might cause a company to define its objective as, "Package and label all chemicals in accordance with regulations." In this case, policies and procedures would deal with communications programs, site inspections and training.

An entity's compliance record with laws and regulations can significantly — either positively or negatively — affect its reputation in the community.

Overlap of Objectives

An objective in one category may overlap or support an objective in another. For example, "Close quarterly within 10 workdays" may be a goal supporting primarily an operations objective — to support management meetings for reviewing business performance. But it also supports timely financial reporting as well as timely filings with regulatory agencies. An objective, "Provide plant management pertinent data on raw material production mix on a timely basis," might relate to all three categories of objectives. The data support decisions on desired changes to the mix (operations), facilitate monitoring hazardous waste (compliance), and provide input for cost accounting (financial reporting as well as operations).

Another set of objectives relates to "safeguarding of resources." Although these are primarily operations objectives, certain aspects of safeguarding can fall under the other categories. Under the operations category is the efficient use of an entity's recorded assets and other resources, and prevention of their loss through theft, waste, inefficiency or what turns out to be simply bad business decisions — such as selling product at too low a price, extension of credit to bad risks, failing to retain key employees or prevent patent infringement, or incurring unforeseen liabilities. Where legal or regulatory requirements apply, these become compliance issues. On the other hand, the goal of ensuring that any such asset losses are properly reflected in the entity's financial statements represents a financial reporting objective.

The category in which an objective falls can sometimes depend on circumstances. Continuing the discussion of safeguarding of assets, controls to prevent theft of assets — such as maintaining a fence around inventory, and a gatekeeper verifying proper authorization of requests for movement of goods — fall under the operations category. These controls normally would not be relevant to the reliability of financial statement preparation, because any inventory losses would be detected pursuant to periodic physical inspection and recorded in the financial statements. However, if for financial reporting purposes management relies solely on perpetual inventory records, as may be the case for interim reporting, the physical security controls would then also fall within the financial reporting category. This is because these physical security controls, along with controls over the perpetual inventory records, would be needed to ensure reliable financial reporting.

The distinction and interrelationship among the categories can further be illustrated in the context of a bank's commercial lending activity. For purposes of illustration, assume that controls exist to ensure credit files contain current customer credit histories and performance data. Further assume in this example that the bank's lending officers do not use that

information in making credit decisions. Instead, approvals of draw downs against existing credit lines, and even increases in limits, are made intuitively. Financial management, however, periodically conducts thorough reviews to determine appropriate levels of loan loss reserves. Under this scenario, controls over operations have significant weaknesses, whereas controls over financial reporting do not. Practically speaking, such lax control over operations likely would result in unacceptable profit performance. The first evidence would show up in performance indicators and later in lower reported profits or even losses — signaling to top management and, if sufficiently serious, to the board, a need for investigation and action. In this way, financial reporting controls may help address the operations weakness, evidencing their interrelationship, but the weakness is in the operations controls alone.

Linkage

Objectives should be complementary and linked. Not only must entity-wide objectives be consistent with the entity's capabilities and prospects, they also must be consistent with the objectives of its business units and functions. Entity-wide objectives must be broken down into subobjectives, consistent with the overall strategy, and linked to activities throughout the organization.

Where entity-wide objectives are consistent with prior practice and performance, the linkage among activities is known. Where, however, objectives depart from an entity's past practices, management must address the linkages or run increased risks. Because they depart from past practice, the need for business-unit or functional subobjectives that are consistent with the new direction is even more important.

An objective to "Fill more management roles internally through promotions" will depend heavily on linked subobjectives for human resource processes dealing with succession planning, appraising, training and development. The subobjectives might be substantially changed if past practice relied on heavy external recruiting.

Activity objectives also need to be clear, that is, readily understood by the people taking the actions toward their achievement. They must also be measurable. Personnel and management must have a mutual understanding of what is to be accomplished, and a means of determining to what extent it is accomplished.

The scope and effort involved in an activity's objectives are also relevant. Most entities establish a number of objectives for each activity, flowing both from the entity-wide objectives and from standards relating to the compliance and financial reporting objectives. For procurement, for example, operations objectives may be established to:

- Purchase goods that meet established engineering specifications;
- Negotiate acceptable prices and other terms;
- Review and re-certify all key vendors annually.

Achieving all of the objectives that could be set for an activity might tax the resources committed to it; so it is useful to relate an activity's overall set of objectives to resources

available. A way to relieve further resource constraint is to question activity objectives that do not support entity-wide objectives and the entity's business processes. Often, a function will have an irrelevant objective that is carried over from past practices (producing routine but unutilized monthly reports, for example).

Another means of balancing objectives and resources is to identify activity objectives that are very important or critical to achieving entity-wide objectives. Not all objectives are equal, so some entities prioritize objectives. Entities may identify certain activity objectives as being critical, and closely monitor activities related to those objectives. This notion reflects the concept of the "critical success factors" discussed earlier, where "things must go right" to achieve the entity's objectives.

Achievement of Objectives

As noted, establishing objectives is a prerequisite to effective internal control. Objectives provide the measurable targets toward which the entity moves in conducting its activities. However, although an entity should have reasonable assurance that certain objectives are achieved, that may not be the case for all objectives.

As discussed in Chapter 1, an effective internal control system should provide reasonable assurance that an entity's financial reporting objectives are being achieved. Similarly, there should be reasonable assurance that compliance objectives are being achieved. Both of these categories are primarily based on external standards established independently of the entity's purposes, and achieving them is largely within the entity's control.

But there is a difference when it comes to operations objectives. First, they are not based on external standards. Second, an entity may perform as intended, yet be out-performed by a competitor. It could also be subject to outside events — a change in government, poor weather and the like — that it cannot control. It may even have considered some of these events in its objective-setting process and treated them as low probability, with a contingency plan in case they occurred. However, such a plan only mitigates the impact of outside events. It does not ensure that the objectives are achieved. Good operations consistent with the intent of objectives do not ensure success.

The goal of internal control in this area focuses primarily on: developing consistency of objectives and goals throughout the organization, identifying key success factors and timely reporting to management of performance and expectations. Although success cannot be ensured, management should have reasonable assurance of being alerted when objectives are in danger of not being achieved.

Risks

The process of identifying and analyzing risk is an ongoing iterative process and is a critical component of an effective internal control system. Managements must focus carefully on risks at all levels of the entity and take the necessary actions to manage them.

Risk Identification

An entity's performance can be at risk due to internal or external factors. These factors, in turn, can affect either stated or implied objectives. Risk increases as objectives increasingly differ from past performance. In a number of areas of performance, an entity often does not set explicit entity-wide objectives because it considers its performance to be acceptable. Although there might not be an explicit or written objective in these circumstances, there is an implied objective of "no change," or "as is." This does not mean that an implied objective is without either internal or external risk. For example, an entity might view its service to customers as acceptable, yet, due to a change in a competitor's practices, its service, as viewed by its customers, might deteriorate.

Regardless of whether an objective is stated or implied, an entity's risk-assessment process should consider risks that may occur. It is important that risk identification be comprehensive. It should consider all significant interactions — of goods, services and information — between an entity and relevant external parties. These external parties include potential and current suppliers, investors, creditors, shareholders, employees, customers, buyers, intermediaries and competitors, as well as public bodies and news media.

Risk identification is an iterative process and often is integrated with the planning process. It also is useful to consider risk from a "clean sheet of paper" approach, and not merely relate the risk to the previous review.

Entity Level. Risks at the entity-wide level can arise from external or internal factors. Examples include:

External Factors

- Technological developments can affect the nature and timing of research and development, or lead to changes in procurement.
- Changing customer needs or expectations can affect product development, production process, customer service, pricing or warranties.
- Competition can alter marketing or service activities.
- New legislation and regulation can force changes in operating policies and strategies.
- Natural catastrophes can lead to changes in operations or information systems and highlight the need for contingency planning.
- Economic changes can have an impact on decisions related to financing, capital expenditures and expansion.

Internal Factors

- A disruption in information systems processing can adversely affect the entity's operations.
- The quality of personnel hired and methods of training and motivation can influence the level of control consciousness within the entity.

- A change in management responsibilities can affect the way certain controls are effected.
- The nature of the entity's activities, and employee accessibility to assets, can contribute to misappropriation of resources.
- An unassertive or ineffective board or audit committee can provide opportunities for indiscretions.

Many techniques have been developed to identify risks. The majority—particularly those developed by internal and external auditors to determine the scope of their activities—involve qualitative or quantitative methods to prioritize and identify higher-risk activities. Other practices include: periodic reviews of economic and industry factors affecting the business, senior management business-planning conferences and meetings with industry analysts. Risks may be identified in connection with short- and long-range forecasting and strategic planning. Which methods an entity selects to identify risks is not particularly important. What is important is that management considers carefully the factors that may contribute to or increase risk. Some factors to consider include: past experiences of failure to meet objectives; quality of personnel; changes affecting the entity such as competition, regulations, personnel, and the like; existence of geographically distributed, particularly foreign, activities; significance of an activity to the entity; and complexity of an activity.

To illustrate, an importer of apparel and footwear established an entity-wide objective of becoming an industry leader in high-quality fashion merchandise. Risks considered at the entity-wide level included: supply sources, including the quality, number and stability of foreign manufacturers; exposures to fluctuations in the value of foreign currencies; timeliness of receiving shipments and effect of delays in customs inspections; availability and reliability of shipping companies and costs; likelihood of international hostilities and trade embargoes; and pressures from customers and investors to boycott doing business in a foreign country whose government adopts unacceptable policies. These were in addition to the more generic risks considered, such as the impact of a deterioration in economic conditions, market acceptance of products, new competitors in the entity's market, and changes in environmental or regulatory laws and regulations.

Identifying external and internal factors that contribute to risk at an entity-wide level is critical to effective risk assessment. Once the major contributing factors have been identified, management can then consider their significance and, where possible, link risk factors to business activities.

Activity Level. In addition to identifying risk at the entity level, risks should be identified at the activity level. Dealing with risks at this level helps focus risk assessment on major business units or functions such as sales, production, marketing, technology development, and research and development. Successfully assessing activity-level risk also contributes to maintaining acceptable levels at the entity-wide level.

In most instances, for any stated or implied objective, many different risks can be identified. In a procurement process, for example, an entity may have an objective related to maintaining adequate raw materials inventory. The risks to not achieving the activity objective might include goods not meeting specifications, or not being delivered in needed quantities, on time or at acceptable prices. These risks might affect the way specifications for purchased goods are communicated to vendors, the use and appropriateness of production forecasts, identification of alternative supply sources and negotiation practices.

Potential causes of failing to achieve an objective range from the obvious to the obscure, and from the significant to the insignificant in potential effect. Certainly, readily apparent risks that significantly affect the entity should be identified. To avoid overlooking relevant risks, this identification is best made apart from assessment of the likelihood of the risk occurring. There are, however, practical limitations to the identification process, and often it is difficult to determine where to draw the line. It doesn't make much sense to consider the risk of a meteor falling from space onto a company's production facility, while it may be reasonable to consider the risk of an airplane crash for a facility located near an airport runway.

Risk Analysis

After the entity has identified entity-wide and activity risks, a risk analysis needs to be performed. The methodology for analyzing risks can vary, largely because many risks are difficult to quantify. Nonetheless, the process—which may be more or less formal—usually includes:

- Estimating the significance of a risk;
- Assessing the likelihood (or frequency) of the risk occurring;
- Considering how the risk should be managed—that is, an assessment of what actions need to be taken.

A risk that does not have a significant effect on the entity and that has a low likelihood of occurrence generally does not warrant serious concern. A significant risk with a high likelihood of occurrence, on the other hand, usually demands considerable attention. Circumstances in between these extremes usually require difficult judgments. It is important that the analysis be rational and careful.

There are numerous methods for estimating the cost of a loss from an identified risk. Management should be aware of them and apply them as appropriate. However, many risks are indeterminate in size. At best they can be described as "large," "moderate" or "small."

Once the significance and likelihood of risk have been assessed, management needs to consider how the risk should be managed. This involves judgment based on assumptions about the risk, and reasonable analysis of costs associated with reducing the level of risk. Actions that can be taken to reduce the significance or likelihood of the risk occurring include a myriad of decisions management may make every day. These range from identifying alternative supply sources or expanding product lines to obtaining more relevant operating

reports or improving training programs. Sometimes actions can virtually eliminate the risk, or offset its effect if it does occur. Examples are vertical integration to reduce supplier risk, hedging financial exposures and obtaining adequate insurance coverage.

Note that there is a distinction between risk assessment, which is part of internal control, and the resulting plans, programs or other actions deemed necessary by management to address the risks. The actions undertaken, as discussed in the prior paragraph, are a key part of the larger management process, but not an element of the internal control system.

Along with actions for managing risk is the establishment of procedures to enable management to track the implementation and effectiveness of the actions. For example, one action an organization might take to manage the risk of loss of critical computer services is to formulate a disaster recovery plan. Procedures then would be effected to ensure that the plan is appropriately designed and implemented. Those procedures represent "control activities," discussed in Chapter 4.

Before installing additional procedures, management should consider carefully whether existing ones may be suitable for addressing identified risks. Because procedures may satisfy multiple objectives, management may discover that additional actions are not warranted; existing procedures may be sufficient or may need to be performed better.

Management also should recognize that it is likely some level of residual risk will always exist not only because resources are always limited, but also because of other limitations inherent in every internal control system. These are discussed in Chapter 7.

Risk analysis is not a theoretical exercise. It is often critical to the entity's success. It is most effective when it includes identification of all key business processes where potential exposures of some consequence exist. It might involve process analysis, such as identification of key dependencies and significant control nodes, and establishing clear responsibility and accountability. Effective process analysis directs special attention to cross-organizational dependencies, identifying, for example: where data originate, where they are stored, how they are converted to useful information and who uses the information. Large organizations usually need to be particularly vigilant in addressing intracompany and intercompany transactions and key dependencies. These processes can be positively affected by quality programs which, with a "buy-in" by employees, can be an important element in risk containment.

Unfortunately, the importance of risk analysis is sometimes recognized too late, as in the case of a major financial services firm where a senior executive offered what amounted to a wistful epitaph: "We just didn't think we faced so much risk."

Managing Change

Economic, industry and regulatory environments change, and entities' activities evolve. Internal control effective under one set of conditions will not necessarily be effective under

another. Fundamental to risk assessment is a process to identify changed conditions and take actions as necessary.

Thus, every entity needs to have a process, formal or informal, to identify conditions that can significantly affect its ability to achieve its objectives. As discussed further in Chapter 5, a key part of that process involves information systems that capture, process and report information about events, activities and conditions that indicate changes to which the entity needs to react. Such information may involve changes in customer preferences or other factors affecting demand for the company's products or services. Or, it may involve new technology affecting production processes or other business activities, or competitive or legislative or regulatory developments. With the requisite information systems in place, the process to identify and respond to changing conditions can be established.

This process will parallel, or be a part of, the entity's regular risk assessment process described above. It involves identifying the changed condition—this requires having mechanisms in place to identify and communicate events or activities that affect the entity's objectives—and analyzing the associated opportunities or risks. Such analysis includes identifying potential causes of achieving or failing to achieve an objective, assessing the likelihood that such causes will occur, evaluating the probable effect on achievement of the objectives and considering the degree to which the risk can be controlled or the opportunity exploited.

Although the process by which an entity manages change is similar to, if not a part of, its regular risk-assessment process, it is discussed separately. This is because of its critical importance to effective internal control and because it can too easily be overlooked or given insufficient attention in the course of dealing with everyday issues.

Circumstances Demanding Special Attention

This focus on managing change is founded on the premise that, because of their potential impact, certain conditions should be the subject of special consideration. The extent to which such conditions require management's attention, of course, depends on the effect they may have in the particular circumstances. Such conditions are:

- *Changed Operating Environment*—A changed regulatory or economic environment can result in increased competitive pressures and significantly different risks. "Divestiture" in the telecommunications industry, and deregulation of commission rates in the brokerage industry, for example, thrust entities into a vastly changed competitive environment.
- *New Personnel*—A senior executive new to an entity may not understand the entity's culture, or may focus solely on performance to the exclusion of control-related activities. High turnover of personnel, in the absence of effective training and supervision, can result in breakdowns.
- *New or Revamped Information Systems*—Normally effective controls can break down when new systems are developed, particularly when done under unusually tight time constraints—for example, to gain competitive advantage or make tactical moves.

- *Rapid Growth*—When operations expand significantly and quickly, existing systems may be strained to the point where controls break down; where processing shifts or clerical personnel are added, existing supervisors may be unable to maintain adequate control.
- *New Technology*—When new technologies are incorporated into production processes or information systems, a high likelihood exists that internal controls will need to be modified. Just-in-time inventory manufacturing technologies, for instance, commonly require changes in cost systems and related controls to ensure reporting of meaningful information.
- *New Lines, Products, Activities*—When an entity enters new business lines or engages in transactions with which it is unfamiliar, existing controls may not be adequate. Savings and loan organizations, for example, ventured into investment and lending arenas in which they had little or no previous experience, without focusing on how to control the risks involved.
- *Corporate Restructurings*—Restructurings—resulting, for example, from a leveraged buyout, or from significant business declines or cost-reduction programs—may be accompanied by staff reductions and inadequate supervision and segregation of duties. Or, a job performing a key control function may be eliminated without a compensating control put in its place. A number of companies learned too late that they made rapid, large-scale cutbacks in personnel without adequate consideration of serious control implications.
- *Foreign Operations*—The expansion or acquisition of foreign operations carries new and often unique risks that management should address. For instance, the control environment is likely to be driven by the culture and customs of local management. Also, business risks may result from factors unique to the local economy and regulatory environment. Or, channels of communication and information systems may not be well established and available to all individuals.

Mechanisms

Mechanisms should exist to identify changes that have taken place or will shortly occur, in any material assumption or condition. These mechanisms need not be elaborate, and usually are rather informal in smaller enterprises. The owner-manager of a small company that manufactures silk-screen machines meets monthly with the heads of sales, finance, purchasing, manufacturing and engineering. During the course of a several-hour meeting, they address technologies, competitor actions and new customer demands. Risks and opportunities are analyzed, leading immediately to action plans for each activity. Implementation begins right away, and the owner-manager follows up with visits over the weeks and months to each activity to see first-hand the way in which implementation is proceeding, and whether the changes in the marketplace are being adequately addressed.

Forward-Looking

To the extent practicable, mechanisms should be forward-looking, so an entity can anticipate and plan for significant changes. Early warning systems should be in place to identify data

signaling new risks. A commercial bank, for instance, uses a multidisciplinary "risk council" to analyze new products being developed in terms of their risks to the bank. Similarly, mechanisms are needed for early identification of opportunities arising from changing conditions. Those banks that identified emerging customer needs for after-hours banking and increasing customer receptivity to interactive computer systems were able to expand significantly their consumer banking market shares through installation and effective marketing of user-friendly automatic teller machine networks.

Naturally, the earlier that changes affecting risks and opportunities are recognized, the better the likelihood that actions can be taken to deal effectively with them. However, as with other control mechanisms, the related costs cannot be ignored. No entity has sufficient resources to obtain and analyze completely the information about all the myriad evolving conditions that can affect it. Further, because no one possesses a crystal ball that accurately predicts the future, even having the most relevant current information is no guarantee that future events or implications can be accurately forecasted. It is often difficult to know whether seemingly significant information is the beginning of an important trend, or merely an aberration.

Accordingly, reasonable mechanisms should be in place to anticipate changes that can affect the entity, helping to avoid impending problems and take advantage of forthcoming opportunities. No one can foresee the future with certainty, but the better an entity can anticipate changes and their effects, the fewer the unpleasant surprises.

Application to Small and Mid-Size Entities

The risk-assessment process is likely to be less formal and less structured in smaller entities than in larger ones, but the basic concepts of this internal control component should be present in every entity, regardless of size. A smaller entity should have established objectives, though they may be implicitly rather than explicitly stated. Since smaller entities usually are more centralized and have fewer levels of authority, the objectives can be easily and effectively communicated to lower level managers more directly and on a continual basis. Similarly, linkages of the entity-wide objectives with activity objectives are usually clear and direct.

The process of identifying and analyzing risks that may prevent achievement of objectives will often consist of top management receiving information directly from employees and outsiders. An owner-manager can learn about risks arising from external factors through direct contact with customers, suppliers, the entity's banker, lawyer, independent auditor and other "outsiders." The CEO can also be attuned to risks arising from internal factors through direct hands-on involvement with all levels of personnel. Risk assessment in a smaller entity can be particularly effective because the in-depth involvement of the CEO and other key managers often means that risks are assessed by people with both access to the appropriate information and a good understanding of its implications.

The mechanisms in a smaller company for managing normal, everyday risks, as well as those resulting from the less common circumstances of substantially changed conditions (such as new regulations, an economic downturn or expansion of product line), can be highly informal

yet effective. The same informal meetings between the CEO and department heads and outside parties that provide information helpful in identifying the risks can also provide the forum for analyzing them and making decisions on how they should be managed. Action plans can be devised quickly with limited numbers of people. Similarly, implementation can be effected immediately as the CEO or key managers visit the departments affected or talk with the customers or suppliers whose needs are being responded to. They can then follow up as needed to ensure that the necessary actions are being taken.

Evaluation

An evaluator will focus on management's process for objective setting, risk analysis and managing change, including its linkages and relevance to business activities. Listed below are issues an evaluator might consider. The list is not all-inclusive, nor will every item apply to every entity; it can, however, serve as a starting point.

Entity-Wide Objectives

- Extent to which the entity-wide objectives provide sufficiently broad statements and guidance on what the entity desires to achieve, yet which are specific enough to relate directly to this entity.
- Effectiveness with which the entity-wide objectives are communicated to employees and board of directors.
- Relation and consistency of strategies with entity-wide objectives.
- Consistency of business plans and budgets with entity-wide objectives, strategic plans and current conditions.

Activity-Level Objectives

- Linkage of activity-level objectives with entity-wide objectives and strategic plans.
- Consistency of activity-level objectives with each other.
- Relevance of activity-level objectives to all significant business processes.
- Specificity of activity-level objectives.
- Adequacy of resources relative to objectives.
- Identification of objectives that are important (critical success factors) to achievement of entity-wide objectives.
- Involvement of all levels of management in objective setting and extent to which they are committed to the objectives.

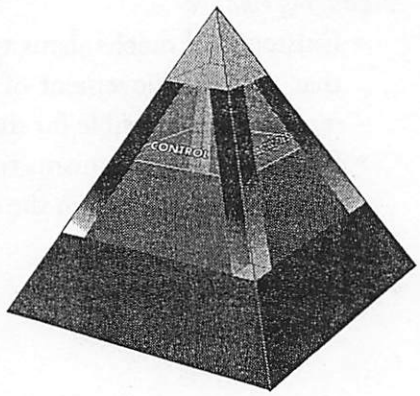
Risks

- Adequacy of mechanisms to identify risks arising from external sources.
- Adequacy of mechanisms to identify risks arising from internal sources.
- Identification of significant risks for each significant activity-level objective.
- Thoroughness and relevance of the risk analysis process, including estimating the significance of risks, assessing the likelihood of their occurring and determining needed actions.

Managing Change

- Existence of mechanisms to anticipate, identify and react to routine events or activities that affect achievement of entity or activity-level objectives (usually implemented by managers responsible for the activities that would be most affected by the changes).
- Existence of mechanisms to identify and react to changes that can have a more dramatic and pervasive effect on the entity, and may demand the attention of top management.

Control Activities



Chapter Summary: Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.

Control activities are policies and procedures, which are the actions of people to implement the policies, to help ensure that management directives identified as necessary to address risks are carried out. Control activities can be divided into three categories, based on the nature of the entity's objectives to which they relate: operations, financial reporting, or compliance.

Although some controls relate solely to one area, there is often overlap. Depending on circumstances, a particular control activity could help satisfy entity objectives in more than one of the three categories. Thus, operations controls also can help ensure reliable financial reporting, financial reporting controls can serve to effect compliance, and so on.

For example, a parts distributorship's sales manager, to keep abreast of sales of certain products and geographical locations, obtains daily "flash" reports from district heads. Because the sales manager relates that information to recorded sales and salespersons' commissions reported by the accounting system, that control activity addresses objectives relating to both operations and financial reporting. In a retail chain, credits issued for merchandise returned by customers are controlled by the numerical sequence of documents and summarized for financial reporting purposes. This summarization also provides an analysis by product for merchandise managers' use in future buying decisions and for inventory control. In this case, control activities established primarily for financial reporting also serve operations.

Although these categories are helpful in discussing internal control, the particular category in which a control happens to be placed is not as important as the role it plays in achieving a particular activity's objectives.

Types of Control Activities

Many different descriptions of types of control activities have been put forth, including preventive controls, detective controls, manual controls, computer controls and management controls. Control activities can be typed by specified control objectives, such as ensuring completeness and accuracy of data processing. Following are certain control activities commonly performed by personnel at various levels in organizations. These are pre-

sented to illustrate the range and variety of control activities, not to suggest any particular categorization.

- *Top Level Reviews*—Reviews are made of actual performance versus budgets, forecasts, prior periods and competitors. Major initiatives are tracked—such as marketing thrusts, improved production processes, and cost containment or reduction programs—to measure the extent to which targets are being reached. Implementation of plans is monitored for new product development, joint ventures or financing. Management actions taken to analyze and follow up on such reporting represent control activities.
- *Direct Functional or Activity Management*—Managers running functions or activities review performance reports. A manager responsible for a bank's consumer loans reviews reports by branch, region and loan (collateral) type, checking summarizations and identifying trends, and relating results to economic statistics and targets. In turn, branch managers receive data on new business by loan-officer and local-customer segment. Branch managers focus also on compliance issues, for example, reviewing reports required by regulators on new deposits over specified amounts. Reconciliations are made of daily cash flows with net positions reported centrally for overnight transfer and investment.
- *Information Processing*—A variety of controls are performed to check accuracy, completeness and authorization of transactions. Data entered are subject to edit checks or matching to approved control files. A customer's order, for example, is accepted only upon reference to an approved customer file and credit limit. Numerical sequences of transactions are accounted for. File totals are compared and reconciled with prior balances and with control accounts. Exceptions in need of follow-up are acted upon by clerical personnel, and reported to supervisors as necessary. Development of new systems and changes to existing ones are controlled, as is access to data, files and programs. Controls over information processing are discussed further below.
- *Physical Controls*—Equipment, inventories, securities, cash and other assets are secured physically, and periodically counted and compared with amounts shown on control records.
- *Performance Indicators*—Relating different sets of data—operating or financial—to one another, together with analyses of the relationships and investigative and corrective actions, serve as control activities. Performance indicators include, for example, purchase price variances, the percentage of orders that are "rush orders" and the percentage of returns to total orders. By investigating unexpected results or unusual trends, management identifies circumstances where the underlying procurement activity objectives are in danger of not being achieved. Whether managers use this information only to make operating decisions, or also follow up on unexpected results reported by financial reporting systems, determines whether analysis of performance indicators serves operational purposes alone or financial reporting control purposes as well.

- *Segregation of Duties*—Duties are divided, or segregated, among different people to reduce the risk of error or inappropriate actions. For instance, responsibilities for authorizing transactions, recording them and handling the related asset are divided. A manager authorizing credit sales would not be responsible for maintaining accounts receivable records or handling cash receipts. Similarly, salespersons would not have the ability to modify product price files or commission rates.

These are just a very few among a myriad of procedures performed every day in enterprises that serve to enforce adherence to established action plans, and to keep entities on track toward achieving their objectives.

Policies and Procedures. Control activities usually involve two elements: a policy establishing what should be done and, serving as a basis for the second element, procedures to effect the policy. A policy, for example, might call for review of customer trading activities by a securities dealer retail branch manager. The procedure is the review itself, performed in a timely manner and with attention given to factors set forth in the policy, such as the nature and volume of securities traded, and their relation to customer net worth and age.

Many times, policies are communicated orally. Unwritten policies can be effective where the policy is a long-standing and well-understood practice, and in smaller organizations where communications channels involve only limited management layers and close interaction and supervision of personnel. But regardless of whether a policy is written, it must be implemented thoughtfully, conscientiously and consistently. A procedure will not be useful if performed mechanically without a sharp continuing focus on conditions to which the policy is directed.

Further, it is essential that conditions identified as a result of the procedures be investigated and appropriate corrective actions taken. Follow-up actions might vary depending on the size and organizational structure of an enterprise. They could range from formal reporting processes in a large company—where business units state why targets weren't met and what actions are being taken to prevent recurrence—to an owner-manager of a small business walking down the hall to speak with the plant manager to discuss what went wrong and what needs to be done.

Integration with Risk Assessment

Along with assessing risks, management should identify and put into effect actions needed to address the risks. The actions identified as addressing a risk also serve to focus attention on control activities to be put in place to help ensure that the actions are carried out properly and in a timely manner.

For example, a company set as an objective "Meeting or exceeding sales targets." Risks identified include having insufficient knowledge of current and potential customers' needs. Management's actions to address the risks included establishing buying histories of existing

customers and undertaking new market research initiatives. These actions also serve as focal points for establishment of control activities.

Control activities are very much a part of the process by which an enterprise strives to achieve its business objectives. Control activities are not simply for their own sake or because it seems to be the "right or proper" thing to do. In this example, management needs to take steps to ensure that sales targets are met. Control activities serve as mechanisms for managing the achievement of that objective. Such activities might include tracking the progress of the development of the customer buying histories against established timetables, and steps to ensure accuracy of the reported data. In this sense, control is built directly into the management process.

Controls over Information Systems

With widespread reliance on information systems, controls are needed over all such systems: financial, compliance and operational, large and small.

Most entities, including small companies or units of larger ones, utilize computers in information processing. Accordingly, the following discussion is geared to information systems that include both manual and computerized elements. For information systems that are strictly manual, different controls would be applied; such controls, though different, would be based on the same underlying concepts of control.

Two broad groupings of information systems control activities can be used. The first is general controls[1]—which apply to many if not all application systems and help ensure their continued, proper operation. The second category is application controls, which include computerized steps within the application software and related manual procedures to control the processing of various types of transactions. Together, these controls serve to ensure completeness, accuracy and validity of the financial and other information in the system.

General Controls

General controls commonly include controls over data center operations, system software acquisition and maintenance, access security, and application system development and maintenance. These controls apply to all systems—mainframe, minicomputer and end-user computing environments.

Data Center Operations Controls. These include job set-up and scheduling, operator actions, backup and recovery procedures, and contingency or disaster recovery planning. In a sophisticated environment, these controls also address capacity planning and resource allocation and use. In a high technology environment, the job scheduler is automatic and job control language is on-line. Storage management tools automatically load data files onto high-speed devices in anticipation of the next job. The shift supervisor no longer needs to initial the

[1] Terminology in existing literature varies. These controls are sometimes called general computer controls, general controls or information technology controls. The term "general controls" is used here for convenience.

console log manually, because it is not printed out; the log is maintained on the system. Hundreds of messages flash by each second on a consolidated console that supports multiple mainframes. Minicomputers run all night, unattended.

System Software Controls. These include controls over the effective acquisition, implementation and maintenance of system software—the operating system, data base management systems, telecommunications software, security software and utilities—which run the system and allow applications to function. The master director of system activities, system software also provides the system logging, tracking and monitoring functions. System software can report on uses of utilities, so that if someone accesses these powerful data-altering functions, at the least their use is recorded and reported for review.

Access Security Controls. These controls have assumed greater importance as telecommunications networks have grown. System users may be halfway around the world or down the hall. Effective access security controls can protect the system, preventing inappropriate access and unauthorized use of the system. If well designed, they can intercept hackers and other trespassers.

Adequate access control activities, such as changing dial-up numbers frequently, or implementing dial-back—where the system calls a potential user back at an authorized number, rather than allowing direct access into the system—can be effective methods to prevent unauthorized access. Access security controls restrict authorized users to only the applications or application functions that they need to do their jobs, supporting an appropriate division of duties. There should be frequent and timely review of the user profiles that permit or restrict access. Former or disgruntled employees can be more of a threat to a system than hackers; terminated employee passwords and user IDs should be revoked immediately. By preventing unauthorized use of and changes to the system, data and program integrity are protected.

Application System Development and Maintenance Controls. Development and maintenance of application systems have traditionally been high-cost areas for most organizations. Total costs for MIS resources, the time needed, the skills of people to perform these tasks, and hardware and software required, are all considerable. To control those costs, many entities have some form of system development methodology. It provides structure for system design and implementation, outlining specific phases, documentation requirements, approvals and checkpoints to control the development or maintenance project. The methodology should provide appropriate control over changes to the system, which may involve required authorization of change requests, review of the changes, approvals, testing results, and implementation protocols, to ensure that changes are made properly.

An alternative to in-house development is the use of packaged software, which has grown in popularity. Vendors provide flexible, integrated systems allowing customization through the use of built-in options. Many system development methodologies address the acquisition of vendor packages as a development alternative and include the necessary steps to provide control over the selection and implementation process.

Application Controls

As the name indicates, application controls are designed to control application processing, helping to ensure the completeness and accuracy of transaction processing, authorization and validity. Particular attention should be paid to an application's interfaces, since they are often linked to other systems that in turn need control, to ensure that all inputs are received for processing and all outputs are distributed appropriately.

One of the most significant contributions computers make to control is their ability to prevent errors from entering the system, as well as detecting and correcting them once they are present. To do this, many application controls depend on computerized edit checks. These consist of format, existence, reasonableness and other checks on the data which are built into each application during its development. When these checks are designed properly, they can help provide control over the data being entered into the system.

Relationship Between General and Application Controls

These two categories of control over computer systems are interrelated. General controls are needed to ensure the function of application controls that depend on computer processes.

For example, application controls such as computer matching and edit checks examine data as they are entered on-line. They provide immediate feedback when something doesn't match, or is in the wrong format, so that corrections can be made. They display error messages that indicate what is wrong with the data, or produce exception reports for subsequent follow-up.

If there are inadequate general controls, it may not be possible to depend on application controls, which assume the system itself will function properly, matching with the right file, or providing an error message that accurately reflects a problem, or including all exceptions in an exception report.

Another example of the required balance between application and general controls is a completeness control, often used over certain types of transactions, involving pre-numbered documents. These are usually documents generated internally, such as purchase orders, where pre-numbered forms are employed. Duplicates are flagged or rejected. To effect this as a control, depending on its design, the system will reject an inappropriate item or hold it in suspense, while users get a report which lists all missing, duplicate and out-of-range items. Or does it? How do those who need to rely on the report content for follow-up know that all items that should be on the report are, in fact, listed?

The answer is the general controls. Controls over system development requiring thorough reviews and testing of applications ensure that the logic of the report program is sound, and that it has been tested to ascertain that all exceptions are reported. To provide control after implementation of the application, controls over access and maintenance ensure that applications are not accessed or changed without authorization and that required, authorized changes are made. The data center operations controls and systems software controls ensure that the right files are used and updated appropriately.

The relationship between the application controls and the general controls is such that general controls are needed to support the functioning of application controls, and both are needed to ensure complete and accurate information processing.

Evolving Issues

Control issues are raised in considering the impact of many emerging technologies. These include CASE (computer assisted software engineering) development tools, prototyping to create new systems, image processing and electronic data interchange. These technologies will affect how controls are implemented, without changing the basic requirements of control.

For one example, in end-user computing (EUC), increasingly powerful microcomputers and ever-cheaper minicomputers allow for distributing data and computing power. Departments and line units do their own processing, often supported by a stand-alone, low-cost local area network. These are user-maintained systems, rather than centrally developed software.

To provide needed control for EUC systems, entity-wide policies for system development, maintenance and operation should be implemented and enforced. Local processing environments should be governed by a level of control activities similar to the more traditional mainframe environment.

An emerging technology is artificial intelligence or expert systems. In the future, as such systems are embedded in many applications—whether developed by a data processing department or end-users, or purchased—issues will include how to decide which applications are best suited, which tool to use and how to control development. Many people feel that such systems will ultimately be controlled in the same way as end-user computing is now. When EUC first started to mushroom, people raised similar concerns before they realized that control would be provided in the same way as before: through appropriate control activities.

Entity Specific

Because each entity has its own set of objectives and implementation strategies, there will be differences in objectives structure and related control activities. Even if two entities had identical objectives and structures, their control activities would be different. Each entity would be managed by different people who use individual judgments in effecting internal control. Moreover, controls reflect the environment and industry in which an entity operates, as well as the complexity of its organization, its history and its culture.

The environment in which an entity operates affects the risks to which it is exposed and may present unique external reporting requirements, or special legal or regulatory requirements. A chemicals manufacturer, for example, must manage greater environmental risks than those facing a typical service company, and must consider waste disposal issues in its financial statement disclosures.

The complexity of an entity, and the nature and scope of its activities, affect its control activities. Complex organizations with diverse activities may face more difficult control issues

than simple organizations with less varied activities. An entity with decentralized operations and an emphasis on local autonomy and innovation presents different control circumstances than a highly centralized one. Other factors that influence an entity's complexity and, therefore, the nature of its controls include: location and geographical dispersion, the extensiveness and sophistication of operations, and information processing methods.

All these factors affect an entity's control activities, which need to be designed accordingly to contribute to the achievement of the entity's objectives.

Application to Small and Mid-Size Entities

The concepts underlying control activities in smaller organizations are not likely to differ significantly from those in larger entities, but the formality with which they operate will vary. Further, smaller entities may find that certain types of control activities are not always relevant because of highly effective controls applied by management of the small or mid-size entity.

For example, direct involvement by the CEO and other key managers in a new marketing plan, and retention of authority for credit sales, significant purchases and draw downs on lines of credit, can provide strong control over those activities, lessening or obviating the need for more detailed control activities. Direct hands-on knowledge of sales to key customers and careful review of key ratios and other performance indicators often can serve the purpose of lower level control activities typically found in large companies.

An appropriate segregation of duties often appears to present difficulties in smaller organizations, at least on the surface. Even companies that have only a few employees, however, can usually parcel out their responsibilities to achieve the necessary checks and balances. But if that is not possible — as may occasionally be the case — direct oversight of the incompatible activities by the owner-manager can provide the necessary control. For example, it is not uncommon, where there is a risk of improper cash payments, for the owner-manager to be named the only authorized check signer, or to require that monthly bank statements be delivered unopened directly to him or her for review of paid checks.

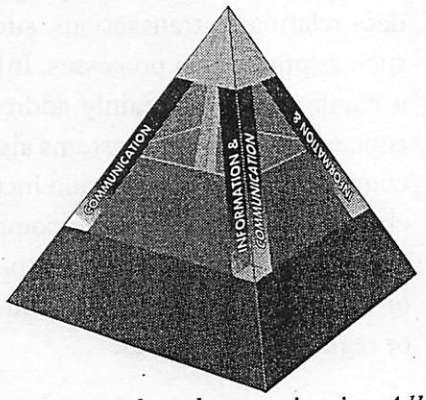
Controls over information systems, particularly general computer controls and more specifically access security controls, may present problems to small and mid-size entities. This is because of the informal way in which control activities are often implemented. Once again, a solution can often be found in the greater amount of direct top management involvement typically found in smaller organizations. Reasonable assurance that any material errors would be detected often comes from management's continual use of information generated by the system, and relating that information to direct knowledge of those activities, together with the existence of certain key controls applied by other personnel.

Evaluation

Control activities must be evaluated in the context of management directives to address risks associated with established objectives for each significant activity. An evaluator therefore will

consider whether control activities relate to the risk-assessment process and whether they are appropriate to ensure that management's directives are carried out. This will be done for each significant business activity, including general controls over computerized information systems. (These will be each of the activities identified in evaluating risk assessment—see Chapter 3.) An evaluator will consider not only whether established control activities are relevant to the risk-assessment process, but also whether they are being applied properly.

Information and Communication



Chapter Summary: Pertinent information must be identified, captured and communicated in a form and timeframe that enables people to carry out their responsibilities. Information systems produce reports, containing operational, financial and compliance-related information, that make it possible to run and control the business. They deal not only with internally generated data, but also information about external events, activities and conditions necessary to informed business decision-making and external reporting. Effective communication also must occur in a broader sense, flowing down, across and up the organization. All personnel must receive a clear message from top management that control responsibilities must be taken seriously. They must understand their own role in the internal control system, as well as how individual activities relate to the work of others. They must have a means of communicating significant information upstream. There also needs to be effective communication with external parties, such as customers, suppliers, regulators and shareholders.

Every enterprise must capture pertinent information—financial and non-financial, relating to external as well as internal events and activities. The information must be identified by management as relevant to managing the business. It must be delivered to people who need it in a form and timeframe that enables them to carry out their control and other responsibilities.

Information

Information is needed at all levels of an organization to run the business, and move toward achievement of the entity's objectives in all categories—operations, financial reporting and compliance. An array of information is used. Financial information, for instance, is used not only in developing financial statements for external dissemination. It is also used for operating decisions, such as monitoring performance and allocating resources. Management reporting of monetary and related measurements enables monitoring, for example, of brand profitability, receivables performance by customer type, market share, customer complaint trends and accident statistics. Reliable internal financial measurements also are essential to planning, budgeting, pricing, evaluating vendor performance, and evaluating joint ventures and other alliances.

Similarly, operating information is essential for developing financial statements. This includes the routine—purchases, sales and other transactions—as well as information on competitors' product releases or economic conditions, which can affect inventory and receivables valuations. Operating information such as airborne particle emissions or personnel data may be needed to achieve both compliance and financial reporting objectives. As such, information developed from internal and external sources, both financial and non-financial, is relevant to all objectives categories.

Information is identified, captured, processed and reported by information systems. The term "information systems" frequently is used in the context of processing internally generated data relating to transactions, such as purchases and sales, and internal operating activities, such as production processes. Information systems — which may be computerized, manual or a combination — certainly address those matters. But, as used here, it is a much broader concept. Information systems also deal with information about external events, activities and conditions. Such information includes: market- or industry-specific economic data that signal changes in demand for the company's products or services; data on goods and services the entity needs for its production process; market intelligence on evolving customer preferences or demands; and information on competitors' product development activities and legislative or regulatory initiatives.

Information systems sometimes operate in a monitoring mode, routinely capturing specific data. In other cases, special actions are taken to obtain needed information. Consider, for example, systems capturing information on customers' satisfaction with the entity's products. Information systems might regularly identify and report sales by product and location, customer gains and losses, returns and requests for allowances, application of product warranty provisions and direct feedback in the form of complaints or other comments. On the other hand, special efforts may be made from time to time to obtain information on evolving market requirements regarding technical product specifications, or customer delivery or service needs. This information may be obtained through questionnaires, interviews, broad-based market demand studies or targeted focus groups.

Information systems can be formal or informal. Conversations with customers, suppliers, regulators and employees often provide some of the most critical information needed to identify risks and opportunities. Similarly, attendance at professional or industry seminars and memberships in trade and other associations can provide valuable information.

Keeping information consistent with needs becomes particularly important when an entity operates in the face of fundamental industry changes, highly innovative and quick-moving competitors or significant customer demand shifts. Information systems must change as needed to support resulting new entity objectives related, for example, to reduced cycle time in bringing products to market, outsourcing certain functions and workforce changes. In such environments there is a special need to differentiate measurements serving as early warning indicators from strictly historical accounting data. Both are important, and the latter, when used effectively, can provide warning signals. But to be effective, information systems must not only identify and capture needed financial and non-financial information, they must also process and report it in a timeframe and way that is useful in controlling the entity's activities.

Strategic and Integrated Systems

Information systems often are an integral part of operational activities. They not only capture information needed in decision-making to effect control, as discussed above, but also are

increasingly designed to carry out strategic initiatives. A recently issued study[1] indicates that the most important management challenge in the 1990s is to integrate the planning, design and implementation of systems with the organization's overall strategy.

Systems Support Strategic Initiatives. The strategic use of information systems has meant success to many organizations. Early examples of such use include an airline's reservation system that gave travel agents easy access to flight information and booking of flights. Another oft-cited example is the hospital supplier that gave on-line access to its system directly to the hospitals, creating a vast competitive advantage as they ordered on-the-spot via terminal. These examples, and others, showed that systems truly could make a difference in achieving competitive advantage.

As the business world learned how to use newer systems that gave better information, more organizations tracked how their products were selling in targeted areas, and whether particular lines were doing better than others. Using technology to help respond to a better-understood marketplace is a growing trend, as systems are used to support proactive rather than reactive business strategies.

Integration with Operations. The strategic use of systems demonstrates the shift that has occurred from purely financial systems to systems integrated into an entity's operations. These systems help control the business process, tracking and recording transactions on a real-time basis, often including many of the organization's operations in an integrated, complex systems environment.

In manufacturing facilities, information systems support all phases of production. They are used for the receipt and acceptance testing of raw materials, selection and combination of components, quality control over finished products, updating inventory and customer records and distribution of finished goods. In many environments, these steps are linked through process control systems and robotics to such an extent that few human hands make contact with the product.

The effect of integrated operations systems is dramatic, as can be seen in a just-in-time (JIT) inventory system. Companies using JIT keep minimal inventory on hand, cutting their costs considerably. The systems themselves order and schedule arrival of raw materials automatically, frequently through the use of EDI (electronic data interchange). Organizations using JIT depend on their systems to meet production goals, since such close monitoring would be impossible without them.

Many of the newer production systems are highly integrated with other organizational systems and may include the organization's financial systems. Financial data and accounting records are updated automatically as the systems perform other applications.

[1] *Systems Auditability and Control*, referred to as the SAC Report (Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation, 1991), has as one of its principal objectives providing guidance on information systems and related control activities.

Here is an example of how such systems can work: In today's insurance companies, claims may be settled on-line. Adjustors query the system about limits on a particular type of claim, check on whether a claimant is insured and print a check for the claim. At the same time, the claim file, claim statistics and other related files are updated. Contrast this with an unintegrated system where each claim is processed separately within each application or sub-system. The integrated system helps control operations, since on-line settlement is faster, more efficient and more effective than the old paper-based method. It produces financial information, and can answer questions such as: How many claims have been paid this period? How much has been paid? It also can facilitate compliance with regulatory requirements through questions such as: Are covered claims processed and paid in a timely fashion? Are loss reserves adequate?

Coexisting Technologies. Despite the challenges of keeping up with the revolution in information systems technology, it is a mistake to assume that newer systems provide better control just because they are new. In fact, the opposite may be true. Older systems may have been tried and tested through their use and provide what is required. The process is such that an organization's systems often evolve to suit requirements, and become an amalgam of many technologies.

Acquisition of technology is an important aspect of corporate strategy, and choices regarding technology can be critical factors in achieving growth objectives. Decisions about its selection and implementation depend on many factors. These include organizational goals, marketplace needs, competitive requirements and, importantly, how the new systems will help effect control, and in turn be subject to the necessary controls, to promote achievement of the entity's objectives.

Information Quality

The quality of system-generated information affects management's ability to make appropriate decisions in managing and controlling the entity's activities. Modern systems often provide on-line query ability, so that the freshest information is available on request.

It is critical that reports contain enough appropriate data to support effective control. The quality of information includes ascertaining whether:

- *Content is appropriate* — Is the needed information there?
- *Information is timely* — Is it there when required?
- *Information is current* — Is it the latest available?
- *Information is accurate* — Are the data correct?
- *Information is accessible* — Can it be obtained easily by appropriate parties?

All of these questions must be addressed by the system design. If not, it is probable that the system will not provide the information that management and other personnel require.

Because having the right information, on time, at the right place is essential to effecting control, information systems, while themselves a component of an internal control system, also must be controlled. The quality of information can depend on the functioning of control activities, discussed in Chapter 4.

Communication

Communication is inherent in information systems. As discussed above, information systems must provide information to appropriate personnel so that they can carry out their operating, financial reporting and compliance responsibilities. But communication also must take place in a broader sense, dealing with expectations, responsibilities of individuals and groups, and other important matters.

Internal

In addition to receiving relevant data for managing their activities, all personnel, particularly those with important operating or financial management responsibilities, need to receive a clear message from top management that internal control responsibilities must be taken seriously. Both the clarity of the message and the effectiveness with which it is communicated are important.

In addition, specific duties must be made clear. Each individual needs to understand the relevant aspects of the internal control system, how they work and his or her role and responsibility in the system. Without this understanding, problems are likely to arise. In one company, for example, unit heads were required to sign a monthly report affirming that specified reconciliations had been performed. Each month, the reports were dutifully signed and submitted. Later, however, after serious problems were uncovered, it was discovered that at least two unit heads did not know what was really expected of them. One believed the reconciliation was complete when the amount of the difference between the two figures was merely identified. Another took the reconciliation process only one step further, believing that its objective was satisfied when each individual reconciling item was identified. In fact, the intended process was not complete until the reasons for the differences were pinpointed and appropriate corrective action was taken.

In performing their duties, personnel should know that whenever the unexpected occurs, attention is to be given not only to the event itself, but also to its cause. In this way, a potential weakness in the system can be identified and action taken to prevent a recurrence. For example, finding out about unsalable inventory should result not only in an appropriate writedown in financial reports, but also in a determination of why the inventory became unsalable in the first place.

People also need to know how their activities relate to the work of others. This knowledge is necessary to recognize a problem or to determine its cause and corrective action. People need to know what behavior is expected, or acceptable, and what is unacceptable. There have been instances of fraudulent financial reporting in which managers, under pressure to meet

budgets, misrepresented operating results. In a number of such instances, no one had told the individuals that such misreporting can be illegal or otherwise improper. This points up the critical nature of how messages are communicated within an organization. A manager who instructs subordinates, "Meet the budget—I don't care how you do it, just do it," can unwittingly send the wrong message.

Personnel also need to have a means of communicating significant information upstream in an organization. Front-line employees who deal with critical operating issues every day are often in the best position to recognize problems as they arise. Sales representatives or account executives may learn of important customer product design needs. Production personnel may become aware of costly process deficiencies. Purchasing personnel may be confronted with improper incentives from suppliers. Accounting department employees may learn of overstatements of sales or inventory, or identify instances where the entity's resources were used for personal benefit.

For such information to be reported upstream, there must be both open channels of communication and a clear-cut willingness to listen. People must believe their superiors truly want to know about problems and will deal with them effectively. Most managers recognize intellectually that they should avoid "shooting the messenger." But when caught up in everyday pressures they can be unreceptive to people bringing them legitimate problems. Employees are quick to pick up on spoken or unspoken signals that a superior doesn't have the time or interest to deal with problems they have uncovered. Compounding such problems, the manager who is unreceptive to troublesome information often is the last to know that the communications channel has been effectively shut down.

In most cases, the normal reporting lines in an organization are the appropriate communications channel. In some circumstances, however, separate lines of communication are needed to serve as a fail-safe mechanism in case normal channels are inoperative. Some companies provide a channel directly to a senior officer, the chief internal auditor or the entity's legal counsel. One company's chief executive makes himself available one evening a week, and makes it well known that visits by employees on any subject are truly welcome. Another chief executive periodically visits with employees in the plant—fostering an atmosphere where people can communicate problems and concerns. Without both open communications channels and a willingness to listen, the upward flow of information in an organization might be blocked.

In all cases, it is important that personnel understand that there will be no reprisals for reporting relevant information. As noted in Chapter 2, a clear message is sent by the existence of mechanisms to encourage employees to report suspected violations of an entity's code of conduct, and the treatment of employees who make such reports. Much has been written about the desirability of "whistle-blower" protection, most frequently in the context of government employees. Some commentators counter with expressions of concern about entities becoming bogged down dealing with unfounded assertions of disgruntled employees.

Certainly, a balance can and should be reached. It is important that management communicate the right messages and provide reasonable vehicles for legitimate upstream reporting.

Communications between management and the board of directors and its committees are critical. Management must keep the board up to date on performance, developments, risks, major initiatives, and any other relevant events or occurrences. The better the communications to the board, the more effective it can be in carrying out its oversight responsibilities, and in acting as a sounding board on critical issues and providing advice and counsel. By the same token, the board should communicate to management what information it needs, and provide direction and feedback.

External

There needs to be appropriate communication not only within the entity, but outside. With open communications channels, customers and suppliers can provide highly significant input on the design or quality of products or services, enabling a company to address evolving customer demands or preferences. Also, anyone dealing with the entity must recognize that improper actions, such as kickbacks and other improper payments, will not be tolerated. Companies may communicate directly with vendors, for example, regarding how the company expects the vendor's employees to act in dealing with it.

Communications from external parties often provide important information on the functioning of the internal control system. External auditors' understanding of an entity's operations and related business issues and control systems provides management and the board important control information.

Regulators such as state banking or insurance authorities report results of compliance reviews or examinations that can highlight control weaknesses. Complaints or inquiries about shipments, receipts, billings or other activities often point to operating problems. They should be reviewed by personnel independent of the original transaction. Personnel should be ready to recognize implications of such circumstances, and investigate and take necessary corrective actions.

Communications to shareholders, regulators, financial analysts and other external parties should provide information relevant to their needs, so they can readily understand the circumstances and risks the entity faces. Such communications should be meaningful, provide pertinent and timely information and, of course, conform to legal and regulatory requirements.

Management's communications with external parties—whether open and forthcoming and serious in follow-up or otherwise—also send messages internally throughout the organization.

Means of Communication

Communication takes such forms as policy manuals, memoranda, bulletin board notices and videotaped messages. Where messages are transmitted orally—in large groups, smaller

meetings or one-on-one sessions — tone of voice and body language serve to emphasize what is being said.

Another powerful communications medium is the action taken by management in dealing with subordinates. Managers should remind themselves, "Actions speak louder than words." Their actions are, in turn, influenced by the history and culture of the entity, drawing on past observations of how their superiors dealt with similar situations.

An entity with a long and rich history of operating with integrity, and whose culture is well understood by people throughout the organization, will likely find little difficulty in communicating its message. An entity without such a tradition will likely need to put more effort into the way messages are communicated.

Application to Small and Mid-Size Entities

Information systems in smaller organizations are likely to be less formal than in large organizations, but their role is just as significant. With today's computer and information technology, internally generated data can be processed effectively and efficiently in most organizations, regardless of size. Information systems in smaller entities will also typically identify and report on relevant external events, activities and conditions, but their effectiveness is usually significantly affected by and dependent on top management's ability to monitor external events. Discussions by an owner-manager or other management personnel with key customers and suppliers, for example, could be a key source of information on evolving customer preferences or supply sources necessary to monitor changing conditions and related risks.

Effective internal communication between top management and employees may well be easier to achieve in a small or mid-size company than in a large enterprise, because of the smaller organization size and its fewer levels, and greater visibility and availability of the CEO. In effect, internal communication takes place through the daily meetings and activities in which the CEO and key managers participate. Without the formal communications channels typically found in large enterprises, many smaller entities find that the more frequent day-to-day contacts coupled with an open-door policy for senior executives provide effective communication. And an "actions-speak-louder-than-words policy" can be an even more important communications device — both internally and externally — in a smaller organization, since the top executives interact directly with a large proportion of the entity's employees, customers and suppliers.

Evaluation

An evaluator will consider the appropriateness of information and communication systems to the entity's needs. Listed below are issues one might consider. The list is not all-inclusive, nor will every item apply to every entity; it can, however, serve as a starting point.

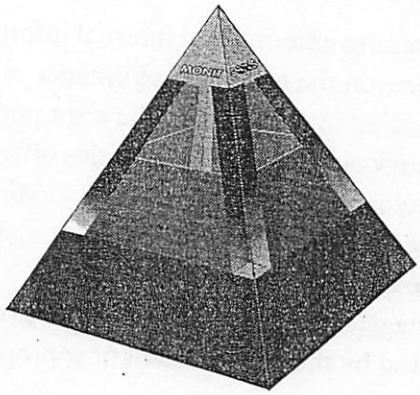
Information

- Obtaining external and internal information, and providing management with necessary reports on the entity's performance relative to established objectives.
- Providing information to the right people in sufficient detail and on time to enable them to carry out their responsibilities efficiently and effectively.
- Development or revision of information systems based on a strategic plan for information systems — linked to the entity's overall strategy — and responsive to achieving the entity-wide and activity-level objectives.
- Management's support for the development of necessary information systems is demonstrated by the commitment of appropriate resources — human and financial.

Communication

- Effectiveness with which employees' duties and control responsibilities are communicated.
- Establishment of channels of communication for people to report suspected improprieties.
- Receptivity of management to employee suggestions of ways to enhance productivity, quality or other similar improvements.
- Adequacy of communication across the organization (for example, between procurement and production activities) and the completeness and timeliness of information and its sufficiency to enable people to discharge their responsibilities effectively.
- Openness and effectiveness of channels with customers, suppliers and other external parties for communicating information on changing customer needs.
- Extent to which outside parties have been made aware of the entity's ethical standards.
- Timely and appropriate follow-up action by management resulting from communications received from customers, vendors, regulators or other external parties.

Monitoring



Chapter Summary: Internal control systems need to be monitored—a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two. Ongoing monitoring occurs in the course of operations. It includes regular management and supervisory activities, and other actions personnel take in performing their duties. The scope and frequency of separate evaluations will depend primarily on an assessment of risks and the effectiveness of ongoing monitoring procedures. Internal control deficiencies should be reported upstream, with serious matters reported to top management and the board.

Internal control systems change over time. The way controls are applied may evolve. Once-effective procedures can become less effective, or perhaps are no longer performed. This can be due to the arrival of new personnel, the varying effectiveness of training and supervision, time and resource constraints or additional pressures. Furthermore, circumstances for which the internal control system originally was designed also may change, causing it to be less able to warn of the risks brought by new conditions. Accordingly, management needs to determine whether the internal control system continues to be relevant and able to address new risks.

Monitoring ensures that internal control continues to operate effectively. This process involves assessment by appropriate personnel of the design and operation of controls on a suitably timely basis, and the taking of necessary actions. It applies to all activities within an organization, and sometimes to outside contractors as well. For example, with outsourcing of health claims processing to a third-party administrator, and such processing directly affecting benefits' costs, the entity will want to monitor the functioning of the administrator's activities and controls.

Monitoring can be done in two ways: through ongoing activities or separate evaluations. Internal control systems usually will be structured to monitor themselves on an ongoing basis to some degree. The greater the degree and effectiveness of ongoing monitoring, the less need for separate evaluations. The frequency of separate evaluations necessary for management to have reasonable assurance about the effectiveness of the internal control system is a matter of management's judgment. In making that determination, consideration should be given to the following: the nature and degree of changes occurring and their associated risks, the competence and experience of the people implementing the controls, as well as the results of the ongoing monitoring. Usually, some combination of ongoing monitoring and separate evaluations will ensure that the internal control system maintains its effectiveness over time.

It should be recognized that ongoing monitoring procedures are built in to the normal, recurring operating activities of an entity. Because they are performed on a real-time basis,

reacting dynamically to changing conditions, and are ingrained in the entity, they are more effective than procedures performed in connection with separate evaluations. Since separate evaluations take place after the fact, problems will often be identified more quickly by the ongoing monitoring routines. Some entities with sound ongoing monitoring activities will nonetheless conduct a separate evaluation of their internal control system, or portions thereof, every few years. An entity that perceives a need for frequent separate evaluations should focus on ways to enhance its ongoing monitoring activities and, thereby, to emphasize "building in" versus "adding on" controls.

Ongoing Monitoring Activities

Activities that serve to monitor the effectiveness of internal control in the ordinary course of operations are manifold. They include regular management and supervisory activities, comparisons, reconciliations and other routine actions.

Examples of ongoing monitoring activities include the following:

- In carrying out its regular management activities, operating management obtains evidence that the system of internal control continues to function. When operating reports are integrated or reconciled with the financial reporting system and used to manage operations on an ongoing basis, significant inaccuracies or exceptions to anticipated results are likely to be spotted quickly. For example, managers of sales, purchasing and production at divisional, subsidiary and corporate levels are in touch with operations and question reports that differ significantly from their knowledge of operations. The effectiveness of the internal control system is enhanced by timely and complete reporting and resolution of these exceptions.
- Communications from external parties corroborate internally generated information or indicate problems. Customers implicitly corroborate billing data by paying their invoices. Conversely, customer complaints about billings could indicate system deficiencies in the processing of sales transactions. Similarly, reports from investment managers on securities gains, losses and income can corroborate or signal problems with the entity's (or the manager's) records. An insurance company's review of safety policies and practices provides information on the functioning of controls, from both operational safety and compliance perspectives, thereby serving as a monitoring technique. Regulators may also communicate with the entity on compliance or other matters that reflect on the functioning of the internal control system.
- Appropriate organizational structure and supervisory activities provide oversight of control functions and identification of deficiencies. For example, clerical activities serving as a control over the accuracy and completeness of transaction processing are routinely supervised. Also, duties of individuals are divided so that different people serve as a check on each other. This is also a deterrent to employee fraud since it inhibits the ability of an individual to conceal his or her suspect activities.

- Data recorded by information systems are compared with physical assets. Finished product inventories, for example, may be examined periodically. The counts are then compared with accounting records, and differences reported.
- Internal and external auditors regularly provide recommendations on the way internal controls can be strengthened. In many entities, auditors focus considerable attention on evaluating the design of internal controls and on testing their effectiveness. Potential weaknesses are identified, and alternative actions recommended to management, often accompanied by information useful in making cost-benefit determinations. Internal auditors or personnel performing similar review functions can be particularly effective in monitoring an entity's activities.
- Training seminars, planning sessions and other meetings provide important feedback to management on whether controls are effective. In addition to particular problems that may indicate control issues, participants' control consciousness often becomes apparent.
- Personnel are asked periodically to state explicitly whether they understand and comply with the entity's code of conduct. Operating and financial personnel may be similarly requested to state whether certain control procedures, such as reconciling specified amounts, are regularly performed. Such statements may be verified by management or internal audit personnel.

It can be seen that these ongoing monitoring activities address important aspects of each of the internal control components.

Separate Evaluations

While ongoing monitoring procedures usually provide important feedback on the effectiveness of other control components, it may be useful to take a fresh look from time to time, focusing directly on the system's effectiveness. This also provides an opportunity to consider the continued effectiveness of the ongoing monitoring procedures.

Scope and Frequency

Evaluations of internal control vary in scope and frequency, depending on the significance of risks being controlled and importance of the controls in reducing the risks. Controls addressing higher-priority risks and those most critical to reducing a given risk will tend to be evaluated more often. Evaluation of an entire internal control system—which will generally be needed less frequently than the assessment of specific controls—may be prompted by a number of reasons: major strategy or management change, major acquisitions or dispositions, or significant changes in operations or methods of processing financial information. When a decision is made to evaluate an entity's entire internal control system, attention should be directed to each of the internal control components with respect to all significant activities. The evaluation scope will also depend on which of the three objectives categories—operations, financial reporting and compliance—are to be addressed.

Who Evaluates

Often, evaluations take the form of self-assessments, where persons responsible for a particular unit or function will determine the effectiveness of controls for their activities. The chief executive of a division, for example, may direct the evaluation of its internal control system. He or she might personally assess the control environment factors, and have individuals in charge of the division's various operating activities assess the effectiveness of other components. Line managers might focus attention primarily on operations and compliance objectives, and the divisional controller may focus on financial reporting objectives. Then, all results would be subject to the chief executive's review. The division's assessments would then be considered by corporate management, along with the internal control evaluations of other divisions.

Internal auditors normally perform internal control evaluations as part of their regular duties, or upon special request of the board of directors, senior management or subsidiary or divisional executives. Similarly, management may use the work of external auditors in considering the effectiveness of internal control. A combination of efforts by both parties may be used in conducting whatever evaluative procedures management deems necessary.

The Evaluation Process

Evaluating a system of internal control is a process in itself. While approaches or techniques vary, there should be a discipline brought to the process, and certain basics inherent in it.

The evaluator must understand each of the entity activities and each of the components of the internal control system being addressed. It may be useful to focus first on how the system purportedly functions, sometimes referred to as the system design. This may involve discussions with entity personnel and review of existing documentation.

The evaluator must determine how the system actually works. Procedures designed to operate in a particular way may over time be modified to operate differently. Or, they may no longer be performed. Sometimes new controls are established but are not known to persons who described the system and are not included in available documentation. A determination as to the actual functioning of the system can be accomplished by holding discussions with personnel who perform or are affected by controls, by examining records on performance of the controls or a combination of procedures.

The evaluator must analyze the internal control system design and the results of tests performed. The analysis should be conducted against the backdrop of the established criteria, with the ultimate goal of determining whether the system provides reasonable assurance with respect to the stated objectives.

Methodology

A wide variety of evaluation methodologies and tools is available, including checklists, questionnaires and flowcharting techniques. Quantitative techniques are presented in the business and academic literature. Also, lists of control objectives have been presented, identifying generic objectives of internal control.

As part of their evaluation methodology, some companies compare their internal control systems to those of other entities, commonly referred to as benchmarking. A company may, for example, measure its system against companies with reputations for having particularly good internal control systems. Comparisons might be done directly with another company, or under the auspices of trade or industry associations. Management consultants may be able to provide comparative information, and peer review functions in some industries can help a company to evaluate its control system against its peers. A word of caution is needed. When comparing internal control systems, consideration must be given to differences that always exist in objectives, facts and circumstances. And, the five individual components and the limitations of internal control (see Chapter 7) need to be kept in mind.

Documentation

The extent of documentation of an entity's internal control system varies with the entity's size, complexity and similar factors. Larger organizations usually have written policy manuals, formal organization charts, written job descriptions, operating instructions, information system flowcharts, and so forth. Smaller companies typically have considerably less documentation.

Many controls are informal and undocumented, yet are regularly performed and highly effective. These controls may be tested in the same ways documented controls are. The fact that controls are not documented does not mean that an internal control system is not effective, or that it cannot be evaluated. An appropriate level of documentation does usually make the evaluation more efficient. It is helpful in other respects: It facilitates employees' understanding of how the system works and their particular roles, and makes it easier to modify when necessary.

The evaluator may decide to document the evaluation process itself. He or she will usually draw on existing documentation of the entity's internal control system. That will typically be supplemented with additional system documentation, along with descriptions of the tests and analyses performed in the evaluation process.

The nature and extent of documentation normally will become more substantive when statements about the system or evaluation are made to additional parties. Where management intends to make a statement to external parties regarding internal control system effectiveness, it should consider developing and retaining documentation to support the statement. Such documentation may be useful if the statement is subsequently challenged.

Action Plan

Executives directing evaluations of internal control systems for the first time might consider the following suggested outline of where to start and what to do:

- Decide on the evaluation's scope, in terms of the categories of objectives, internal control components and activities to be addressed.
- Identify ongoing monitoring activities that routinely provide comfort that internal control is effective.

- Analyze control evaluation work by internal auditors, and consider control-related findings of external auditors.
- Prioritize by unit, component or otherwise the higher risk areas that warrant immediate attention.
- Based on the above, develop an evaluation program with short- and long-range segments.
- Bring together the parties who will carry out the evaluation. Together, consider not only scope and timeframes, but also methodology, tools to be used, input from internal and external auditors and regulators, means of reporting findings and expected documentation.
- Monitor progress and review findings.
- See that necessary follow-up actions are taken, and modify subsequent evaluation segments as necessary.

Much of the work will be delegated. It's important, however, that the person responsible for conducting the evaluation manage the process through to completion.

Reporting Deficiencies

Deficiencies in an entity's internal control system surface from many sources, including the entity's ongoing monitoring procedures, separate evaluations of the internal control system and external parties.

The term "deficiency" as used here is defined broadly as a condition within an internal control system worthy of attention. A deficiency, therefore, may represent a perceived, potential or real shortcoming, or an opportunity to strengthen the internal control system to provide a greater likelihood that the entity's objectives will be achieved.

Sources of Information

One of the best sources of information on control deficiencies is the internal control system itself. Ongoing monitoring activities of an enterprise, including managerial activities and everyday supervision of employees, generate insights from personnel directly involved in the entity's activities. These insights are gained in real time and can provide quick identification of deficiencies. Other sources of control deficiencies are the separate evaluations of an internal control system. Evaluations performed by management, internal auditors or other personnel can highlight areas in need of improvement.

A number of external parties frequently provide important information on the functioning of an entity's internal control system. These include customers, vendors and others doing business with the entity, independent public accountants and regulators. Reports from external sources must be carefully considered for their internal control implications, and appropriate corrective actions taken.

What Should Be Reported

What should be reported? A universal answer is not possible, as this is highly subjective. Certain parameters, however, can be drawn.

Certainly, all internal control deficiencies that can affect the entity's attaining its objectives should be reported to those who can take necessary action, as discussed in the next section. The nature of matters to be communicated will vary depending on individuals' authority to deal with circumstances that arise, and the oversight activities of superiors.

In considering what needs to be communicated, it is necessary to look at the implications of findings. For example, a salesperson points out that earned sales commissions were computed incorrectly. Payroll department personnel investigate and find that an outdated price on a particular product was used, resulting in undercomputation of commissions, as well as underbillings to customers. Action taken may include recalculation of all salespersons' commissions and billings since the price change went into effect. However, this action still may not address a number of important related questions. Why wasn't the new price used in the first place? What controls exist to ensure price increases are entered to the information system correctly and on time? Is there a problem with the computer programs that compute sales commissions and customer billings? If so, are controls over software development or changes to software in need of attention? Would another component of internal control have identified the problem on a timely basis had the salesperson not pointed out the error?

Thus, a seemingly simple problem with an apparent solution might have more far-reaching control implications. This underscores the need for reporting errors or other problems upstream. It is essential not only that the particular transaction or event be reported, but that potentially faulty controls be reevaluated.

It can be argued that no problem is so insignificant as to make investigation of its control implications unwarranted. An employee's taking of a few dollars from a petty cash fund for personal use, for example, would not be significant in terms of that particular event, and probably not in terms of the amount of the entire petty cash fund. Thus, investigating it might not be worthwhile. However, such apparent condoning personal use of the entity's money might send an unintended message to employees.

To Whom to Report

Information generated by employees in conducting regular operating activities usually is reported through normal channels to their immediate superior. He or she may in turn communicate upstream or laterally in the organization so that the information ends up with people who can and should act on it. As discussed in Chapter 5, there should be alternative communications channels for reporting sensitive information such as illegal or improper acts.

Findings of internal control deficiencies usually should be reported not only to the individual responsible for the function or activity involved, who is in the position to take corrective action, but also to at least one level of management above the directly responsible person. This process enables that individual to provide needed support or oversight for taking corrective action, and to communicate with others in the organization whose activities may be affected. Where findings cut across organizational boundaries, the reporting should cross over as well and be directed to a sufficiently high level to ensure appropriate action.

Reporting Directives

Providing needed information on internal control deficiencies to the right party is critical to the continued effectiveness of an internal control system. Protocols can be established to identify what information is needed at a particular level for decision-making.

Such protocols are based on the general rule that a manager should receive control information needed to affect action or behavior of people under his or her responsibility, or to achieve the activity's objectives. A chief executive normally would want to be apprised, for example, of very serious infractions of policies and procedures. He or she would also want supporting information on the nature of matters that could have significant financial consequences or strategic implications, or that could affect the entity's reputation. Senior managers should be apprised of control deficiencies affecting their units. Examples include where assets with a specified monetary value are at risk, where the competence of personnel is lacking or where important financial reconciliations are not performed correctly. Managers should be informed of control deficiencies in their units in increasing levels of detail as one moves down the organizational structure.

Protocols are established by supervisors, who define for subordinates what matters should be reported. The degree of specificity will vary, usually increasing at lower levels in the organization. While reporting protocols can inhibit effective reporting if too narrowly defined, they can enhance the reporting process if sufficient flexibility is provided.

Parties to whom deficiencies are to be communicated sometimes provide specific directives regarding information to be reported. A board of directors or audit committee, for example, may ask management or internal or external auditors to communicate only those findings of deficiencies meeting a specified threshold of seriousness or importance. One such threshold used by the public accounting profession is "reportable conditions." They are defined as:

> ... significant deficiencies in the design or operation of the internal control structure, which could adversely affect the organization's ability to record, process, summarize and report financial data consistent with the assertions of management in the financial statements.[1]

This definition relates to financial reporting objectives, though the concept probably could be adapted to cover operations and compliance objectives as well.

Application to Small and Mid-Size Entities

Ongoing monitoring activities of small and mid-size entities are more likely to be informal and involve the CEO and other key managers. Their monitoring of controls is typically a by-product of monitoring the business. It is accomplished through hands-on involvement in most if not all facets of operations. Their close involvement in operations often will bring to light

[1] Reportable conditions include what are referred to as "material weaknesses," discussed in the *Reporting to External Parties* volume.

significant variances from expectations and inaccuracies in operating or financial data. An owner-manager of a small business may frequently visit the factory floor, assembly facility or warehouse, and compare physical inventory with amounts reported by the data processing system. Direct knowledge of significant customer and vendor complaints, as well as any communications from regulators, also may alert the management of a smaller enterprise about operating or compliance problems that could signal a breakdown in controls.

Small and mid-size entities are less likely to undergo separate evaluations of their internal controls systems, and the need for separate evaluations may be offset by highly effective ongoing monitoring activities. Mid-size companies may have an internal auditor who performs separate evaluations. Even smaller entities might assign accounting personnel certain job functions that serve to evaluate controls. Some entities request that their external auditor perform evaluations of certain aspects of the control system, on perhaps a rotating basis, to provide the CEO with information about effectiveness.

Because of the more limited organization structures, deficiencies surfacing from monitoring procedures can easily be communicated to the right person. Personnel in a smaller entity usually have a clear understanding of the types of problems that need to be reported upstream. What may not always be apparent is who is responsible for determining the cause of a problem and taking corrective action. This is as important to a small or mid-size organization as it is for a large one.

Evaluation

In considering the extent to which the continued effectiveness of internal control is monitored, both ongoing monitoring activities and separate evaluations of the internal control system, or portions thereof, should be considered. Listed below are issues one might consider. The list is not all-inclusive, nor will every item apply to every entity; it may, however, serve as a starting point.

Ongoing Monitoring

- Extent to which personnel, in carrying out their regular activities, obtain evidence as to whether the system of internal control continues to function.
- Extent to which communications from external parties corroborate internally generated information, or indicate problems.
- Periodic comparison of amounts recorded by the accounting system with physical assets.
- Responsiveness to internal and external auditor recommendations on means to strengthen internal controls.
- Extent to which training seminars, planning sessions and other meetings provide feedback to management on whether controls operate effectively.
- Whether personnel are asked periodically to state whether they understand and comply with the entity's code of conduct and regularly perform critical control activities.
- Effectiveness of internal audit activities.

Separate Evaluations

- Scope and frequency of separate evaluations of the internal control system.
- Appropriateness of the evaluation process.
- Whether the methodology for evaluating a system is logical and appropriate.
- Appropriateness of the level of documentation.

Reporting Deficiencies

- Existence of mechanism for capturing and reporting identified internal control deficiencies.
- Appropriateness of reporting protocols.
- Appropriateness of follow-up actions.

CHAPTER 7

Limitations of Internal Control

Chapter Summary: Internal control, no matter how well designed and operated, can provide only reasonable assurance to management and the board of directors regarding achievement of an entity's objectives. The likelihood of achievement is affected by limitations inherent in all internal control systems. These include the realities that human judgment in decision-making can be faulty, and that breakdowns can occur because of such human failures as simple error or mistake. Additionally, controls can be circumvented by the collusion of two or more people, and management has the ability to override the internal control system. Another limiting factor is the need to consider controls' relative costs and benefits.

Internal control has been viewed by some observers as ensuring an entity will not fail—that is, the entity will always achieve its operations, financial reporting and compliance objectives. In this sense, internal control sometimes is looked upon as a cure-all for all real and potential business ills. This view is misguided. Internal control is not a panacea.

In considering limitations of internal control, two distinct concepts must be recognized:

- First, internal control—even effective internal control—operates at different levels with respect to different objectives. For objectives related to the effectiveness and efficiency of an entity's operations—achievement of its basic mission, profitability goals and the like—internal control can help to ensure that management is aware of the entity's progress, or lack of it. But it cannot provide even reasonable assurance that the objectives themselves will be achieved.
- Second, internal control cannot provide absolute assurance with respect to any of the three objectives categories.

The first set of limitations acknowledges that certain events or conditions are simply outside management's control. This is discussed in Chapter 3 under "Achievement of Objectives." The second has to do with the reality that no system will always do what it's intended to do. The best that can be expected in any internal control system is that reasonable assurance is obtained. This is discussed in this chapter.

Reasonable assurance certainly does not imply that internal control systems will frequently fail. Many factors, individually and collectively, serve to provide strength to the concept of reasonable assurance. The cumulative effect of controls that satisfy multiple objectives and the multipurpose nature of controls reduce the risk that an entity may not achieve its objectives. Furthermore, the normal, everyday operating activities and responsibilities of people functioning at various levels of an organization are directed at achieving the entity's objectives. Indeed, among a cross-section of well-controlled entities, it is very likely that most will be regularly apprised of movement toward their operations objectives, will regularly achieve compliance objectives, and will consistently produce—period after period, year after

year—reliable financial statements. However, because of the inherent limitations discussed above, there is no guarantee that, for example, an uncontrollable event, a mistake or improper reporting incident could never occur. In other words, even an effective internal control system can experience a failure. Reasonable assurance is not absolute assurance.

Judgment

The effectiveness of controls will be limited by the realities of human frailty in the making of business decisions. Such decisions must be made with human judgment in the time available, based on information at hand, and under the pressures of the conduct of business. Some decisions based on human judgment may later, with the clairvoyance of hindsight, be found to produce less than desirable results, and may need to be changed.

The nature of internal control-related decisions that must be made based on human judgment is described further below in the discussion of breakdowns, management override and costs versus benefits.

Breakdowns

Even if internal controls are well designed, they can break down. Personnel may misunderstand instructions. They may make judgment mistakes. Or, they may commit errors due to carelessness, distraction or fatigue. An accounting department supervisor responsible for investigating exceptions might simply forget or fail to pursue the investigation far enough to be able to make appropriate corrections. Temporary personnel executing control duties for vacationing or sick employees might not perform correctly. System changes may be implemented before personnel have been trained to react appropriately to signs of incorrect functioning.

Management Override

An internal control system can only be as effective as the people who are responsible for its functioning. Even in effectively controlled entities—those with generally high levels of integrity and control consciousness—a manager might be able to override internal control.

The term "management override" is used here to mean overruling prescribed policies or procedures for illegitimate purposes with the intent of personal gain or an enhanced presentation of an entity's financial condition or compliance status. A manager of a division or unit, or a member of top management, might override the control system for many reasons: to increase reported revenue to cover an unanticipated decrease in market share, to enhance reported earnings to meet unrealistic budgets, to boost the market value of the entity prior to a public offering or sale, to meet sales or earnings projections to bolster bonus pay-outs tied to performance, to appear to cover violations of debt covenant agreements, or to hide lack of compliance with legal requirements. Override practices include deliberate misrepresentations to bankers, lawyers, accountants and vendors, and intentionally issuing false documents such as purchase orders and sales invoices.

Management override should not be confused with management intervention, which represents management's actions to depart from prescribed policies or procedures for legitimate purposes. Management intervention is necessary to deal with non-recurring and non-standard transactions or events that otherwise might be handled inappropriately by the control system. Provision for management intervention is necessary in all internal control systems because no system can be designed to anticipate every condition. Management's actions to intervene are generally overt and commonly documented or otherwise disclosed to appropriate personnel, whereas actions to override usually are not documented or disclosed, with an intent to cover up the actions.

Collusion

The collusive activities of two or more individuals can result in control failures. Individuals acting collectively to perpetrate and conceal an action from detection often can alter financial data or other management information in a manner that cannot be identified by the control system. For example, there may be collusion between an employee performing an important control function and a customer, supplier or another employee. On a different level, several layers of sales or divisional management might collude in circumventing controls so that reported results meet budgets or incentive targets.

Costs Versus Benefits

Resources always have constraints, and entities must consider the relative costs and benefits of establishing controls.

In determining whether a particular control should be established, the risk of failure and the potential effect on the entity are considered along with the related costs of establishing a new control. For example, it may not pay for a company to install sophisticated inventory controls to monitor levels of raw material if the cost of raw material used in a production process is low, the material is not perishable, ready supply sources exist and storage space is readily available.

Cost and benefit measurements for implementing controls are done with different levels of precision. Generally, it is easier to deal with the cost side of the equation which, in many cases, can be quantified in a fairly precise manner. All direct costs associated with instituting a control, and indirect costs where practically measurable, are usually considered. Some companies also include opportunity costs associated with use of the resources.

In other cases, however, it may be more difficult to quantify costs. It may be difficult to quantify time and effort related, for example, to certain control environment factors, such as management's commitment to ethical values or the competence of personnel; risk assessments; and capturing certain external information such as market intelligence on evolving customer preferences. The benefit side often requires an even more subjective valuation. For example, the benefits of effective training programs are usually readily apparent, but difficult to quantify. Nevertheless, certain factors can be considered in assessing potential benefits:

the likelihood of the undesired condition occurring, the nature of the activities, and the potential financial or operating effect the event might have on the entity.

The complexity of cost-benefit determinations is compounded by the interrelationship of controls with business operations. Where controls are integrated with, or "built in" to, management and business processes, it is difficult to isolate either their costs or benefits.

Similarly, many times a variety of controls may serve, individually or together, to mitigate a particular risk. Consider the case of returned shipments. When they are recorded, is it enough to reconcile updates of inventory and accounts receivable master files to total returns? Do individual customer account codes also need to be verified and, if so, to what extent? Is the monthly reconciliation of subsidiary files to master files sufficient? Or, are more extensive procedures needed to ensure that the subsidiary records are properly updated for the returns? And what mechanisms are in place to focus attention on whether returns are symptomatic of a systemic problem in product design, manufacturing, shipping, billing or customer service? The answers to these questions depend on the risks involved in the particular circumstances and the related costs and benefits of establishing each control procedure.

Cost-benefit determinations also vary considerably depending on the nature of the business. For example, a computer system providing information on the frequency with which customers place orders, the dollar value of orders, and the number of items purchased per order, is very important to a mail order catalog company. For a manufacturer of top-of-the-line, custom-made sailing vessels, such detailed customer profile information would be much less important. For the boat maker, such an information system would probably not be deemed cost-beneficial. Because of the relative insignificance of a particular activity or related risk, it may not be necessary even to make a cost-benefit analysis at all. The effort to conduct the analysis may not be justified.

The challenge is to find the right balance. Excessive control is costly and counterproductive. Customers making telephone orders will not tolerate order acceptance procedures that are too cumbersome or time-consuming. A bank that makes creditworthy potential borrowers "jump through hoops" will not book many new loans. Too little control, on the other hand, presents undue risk of bad debts. An appropriate balance is needed in a highly competitive environment. And, despite the difficulties, cost-benefit decisions will continue to be made.

Roles and Responsibilities

Chapter Summary: Everyone in an organization has some responsibility for internal control. Management, however, is responsible for an entity's internal control system. The chief executive officer is ultimately responsible and should assume "ownership" of the control system. Financial and accounting officers are central to the way management exercises control, though all management personnel play important roles and are accountable for controlling their units' activities. Similarly, internal auditors contribute to the ongoing effectiveness of the internal control system, but they do not have primary responsibility for establishing or maintaining it. The board of directors and its audit committee provide important oversight to the internal control system. A number of external parties, such as external auditors, often contribute to the achievement of the entity's objectives and provide information useful in effecting internal control. However, they are not responsible for the effectiveness of, nor are they a part of, the entity's internal control system.

Internal control is effected by a number of parties, each with important responsibilities. The board of directors (directly or through its committees), management, internal auditors and other personnel all make important contributions to an effective internal control system. Other parties, such as external auditors and regulatory bodies, are sometimes associated with internal control. There is a distinction between those who are part of an entity's internal control system and those who are not, but whose actions nonetheless can affect the system or help achieve the entity's objectives.

Parties internal to an organization are a part of the internal control system. They contribute, each in his or her own way, to effective internal control—that is, to providing reasonable assurance that specified entity objectives are achieved.

Parties external to the entity may also help the entity achieve its objectives through actions that provide information useful to the entity in effecting control, or through actions that independently contribute to the entity's objectives. However, merely because a party contributes, directly or indirectly, to achieving an entity's objectives, does not thereby make that party a part of the entity's internal control system.

Responsible Parties

Every individual within an entity has some role in effecting internal control. Roles vary in responsibility and involvement. The roles and responsibilities of management, the board of directors, internal auditors and other personnel are discussed below.

Management

Management is directly responsible for all activities of an entity, including its internal control system. Naturally, management at different levels in an entity will have different internal control responsibilities. These will differ, often considerably, depending on the entity's characteristics.

In any organization, "the buck stops" with the chief executive. He or she has ultimate ownership responsibility for the internal control system. One of the most important aspects of carrying out this responsibility is to ensure the existence of a positive control environment. More than any other individual or function, the chief executive sets the "tone at the top" that affects control environment factors and other components of internal control. The influence of the CEO on an entire organization cannot be overstated. What's not always obvious is the influence a CEO has over the selection of the board of directors. A CEO with high ethical standards can go a long way in ensuring that the board reflects those values. On the other hand, a CEO who lacks integrity may not be able, or want, to obtain board members who possess it. One individual who serves on a number of boards of directors and audit committees said unequivocally that if he has any reservations about the integrity of a CEO, he will flatly turn down an invitation to serve. Effective boards and audit committees also will look closely at top management's integrity and ethical values to determine whether the internal control system has the necessary critical underpinnings.

The chief executive's responsibilities include seeing that all the components of internal control are in place. The CEO generally fulfills this duty by:

- Providing leadership and direction to senior managers. Together with them, the CEO shapes the values, principles and major operating policies that form the foundation of the entity's internal control system. For example, the CEO and key senior managers will set entity-wide objectives and broad-based policies. They take actions concerning the entity's organizational structure, content and communication of key policies, and the type of planning and reporting systems the entity will use.
- Meeting periodically with senior managers responsible for the major functional areas—sales, marketing, production, procurement, finance, human resources, etc.—to review their responsibilities, including how they are controlling the business. The CEO will gain knowledge of controls inherent in their operations, improvements required and status of efforts under way. To discharge this responsibility, it is critical that the CEO clearly define what information he or she needs.

Senior managers in charge of organizational units have responsibility for internal control related to their units' objectives. They guide the development and implementation of internal control policies and procedures that address their units' objectives and ensure that they are consistent with the entity-wide objectives. They provide direction, for example, on the unit's organizational structure and personnel hiring and training practices, as well as budgeting and other information systems that promote control over the unit's activities. In this sense, in a cascading responsibility, each executive is effectively a CEO for his or her sphere of responsibility.

Senior managers usually assign responsibility for the establishment of more specific internal control procedures to personnel responsible for the unit's particular functions or departments. Accordingly, these subunit managers usually play a more hands-on role in devising and

executing particular internal control procedures. Often, these managers are directly responsible for determining internal control procedures that address unit objectives, such as developing authorization procedures for purchasing raw materials or accepting new customers, or reviewing production reports to monitor product output. They will also make recommendations on the controls, monitor their application and meet with upper level managers to report on the controls' functioning.

Depending on the levels of management in an entity, these subunit managers, or lower level management or supervisory personnel, are directly involved in executing control policies and procedures at a detailed level. It is their responsibility to take action on exceptions and other problems as they arise. This may involve investigating data entry errors or transactions appearing on exception reports, looking into reasons for departmental expense budget variances or following up on customer back-orders or product inventory positions. Significant matters, whether pertaining to a particular transaction or an indication of larger concerns, are communicated upward in the organization.

With each manager's respective responsibilities should come not only the requisite authority, but also accountability. Each manager is accountable to the next higher level for his or her portion of the internal control system, with the CEO ultimately accountable to the board.

Although different management levels have distinct internal control responsibilities and functions, their actions should coalesce in the entity's internal control system.

Financial Officers. Of particular significance to monitoring are finance and controllership officers and their staffs, whose activities cut across, up and down the operating and other units of an enterprise. These financial executives often are involved in developing entity-wide budgets and plans. They track and analyze performance, often from operations and compliance perspectives, as well as a financial one. These activities are usually part of an entity's central or "corporate" organization, but they commonly also have "dotted line" responsibility for monitoring division, subsidiary or other unit activities. As such, the chief financial officer, chief accounting officer, controller and others in an entity's financial function are central to the way management exercises control.

The importance of the role of the chief accounting officer in preventing and detecting fraudulent financial reporting was emphasized in the Treadway Commission report: "As a member of top management, the chief accounting officer helps set the tone of the organization's ethical conduct; is responsible for the financial statements; generally has primary responsibility for designing, implementing and monitoring the company's financial reporting system; and is in a unique position regarding identification of unusual situations caused by fraudulent financial reporting." The report noted that the chief financial officer or controller may perform functions of a chief accounting officer.

When looking at the components of internal control, it is clear that the chief financial (accounting) officer and his or her staff play critical roles. That person should be a key player

when the entity's objectives are established and strategies decided, risks are analyzed and decisions are made on how changes affecting the entity will be managed. He or she provides valuable input and direction, and is positioned to focus on monitoring and following up on the actions decided.

As such, the chief financial (accounting) officer should come to the table an equal partner with the other functional heads in an entity. Any attempt by management to have him or her more narrowly focused—limited to principally areas of financial reporting and treasury, for example—could severely limit the entity's ability to succeed.

Board of Directors

Management is accountable to the board of directors or trustees, which provides governance, guidance and oversight. By selecting management, the board has a major role in defining what it expects in integrity and ethical values, and can confirm its expectations through its oversight activities. Similarly, by reserving authority in certain key decisions, the board can play a role in high-level objective setting and strategic planning, and with the oversight that the board provides, the board is involved pervasively in internal control.

Effective board members are objective, capable and inquisitive. They have a working knowledge of the entity's activities and environment, and commit the time necessary to fulfill their board responsibilities. They should utilize resources as needed to investigate any issues they deem important, and have an open and unrestricted communications channel with all entity personnel, including the internal auditors, and with the external auditors and legal counsel.

Many boards of directors carry out their duties largely through committees. Their use and focus vary from one entity to another, but often include audit, compensation, finance, nominating and employee benefits. Each committee can bring specific emphasis to certain components of internal control. For example, the audit committee has a direct role relating to financial reporting, and the nominating committee plays an important role in internal control by its consideration of qualifications of prospective board members. In fact, all board committees, through their oversight roles, are an important part of the internal control system. Where a particular committee has not been established, the related functions are carried out by the board itself.

Audit Committee. Over the years, attention has been given by a number of regulatory and professional bodies to establishing audit committees. Although audit committees have received increased emphasis over the years, they are not universally required, nor are their specific duties and activities prescribed. Audit committees of different entities have different responsibilities, and their levels of involvement vary.

Although some variations in responsibilities and duties are necessary and appropriate, certain characteristics and functions generally are common to all effective audit committees. Management is responsible for the reliability of the financial statements, but an effective audit committee plays an important role. The audit committee (or the board itself, where no audit committee exists) is in a unique position: It has the authority to question top management

regarding how it is carrying out its financial reporting responsibilities, and it also has authority to ensure that corrective action is taken. The audit committee, in conjunction with or in addition to a strong internal audit function, is often in the best position within an entity to identify and act in instances where top management overrides internal controls or otherwise seeks to misrepresent reported financial results. Thus, there are instances where an audit committee, or board, must carry its oversight role to the point of directly addressing serious events or conditions.

The Treadway Commission provided "general guidelines," which deal with committee size and terms of appointment, meeting schedules and participants, full board reporting, members' knowledge of company operations, review of plans of internal and external auditors, adoption of new accounting principles, significant estimates, reserves, contingencies and variances between years.

The Treadway Commission emphasized the value of audit committees and recommended that all public companies be required to establish audit committees composed solely of independent directors. The New York Stock Exchange requires such audit committees, and the National Association of Securities Dealers, for companies with securities included in its NASDAQ National Market System, requires audit committees having a majority of independent directors. The Treadway Commission recognized the practical difficulties, particularly for smaller, newly public companies, in recruiting a sufficient number of qualified independent directors. It also recognized that procedures and controls can exist that are the functional equivalent of an audit committee. Although there are no universal requirements for audit committees, it is clear that internal control is strengthened by their presence. It makes eminent sense for even small companies, to the extent practicable, to have audit committees composed of independent directors.

Compensation Committee. This committee can see that emphasis is placed on compensation arrangements that help achieve the entity's objectives and that do not unduly emphasize short-term results at the expense of long-term performance.

The Finance Committee. This committee is useful in controlling major commitments of funds and ensuring that capital expenditure budgets are consistent with operating plans.

The Nominating Committee. This committee provides control over the selection of candidates for directors and perhaps for top management.

The Employee Benefits Committee. This committee oversees employee benefit programs and sees that they are consistent with the entity's objectives and that fiduciary responsibilities are being appropriately discharged.

Other Committees. There may be other committees of the board which oversee specific areas, such as ethics, public policy or technology. Generally, these committees are established only in certain large organizations, or sometimes in other enterprises due to particular circumstances of the entity.

Internal Auditors

Internal auditors directly examine internal controls and recommend improvements. Standards established by the Institute of Internal Auditors specify that the scope of internal auditing should encompass the examination and evaluation of the adequacy and effectiveness of the organization's system of internal control and the quality of performance in carrying out assigned responsibilities.[1] The standards state that the internal auditors should:

- "Review the reliability and integrity of financial and operating information and the means used to identify, measure, classify, and report such information.
- "Review the systems established to ensure compliance with those policies, plans, procedures, laws, and regulations which could have a significant impact on operations and reports and should determine whether the organization is in compliance.
- "Review the means of safeguarding assets and, as appropriate, verify the existence of such assets.
- "Appraise the economy and efficiency with which resources are employed.
- "Review operations or programs to ascertain whether results are consistent with established objectives and goals and whether the operations or programs are being carried out as planned."

All activities within an organization are potentially within the scope of the internal auditors' responsibility. In some entities, the internal audit function is heavily involved with controls over operations. For example, internal auditors may periodically monitor production quality, test the timeliness of shipments to customers or evaluate the efficiency of the plant layout. In other entities, the internal audit function may focus primarily on compliance or financial reporting-related activities.

The Institute of Internal Auditors standards also set forth the internal auditors' responsibility for the roles they may be assigned. Those standards, among other things, state that internal auditors should be independent of the activities they audit. They possess, or should possess, such independence through their position and authority within the entity and through recognition of their objectivity.

Organizational position and authority involve such matters as a reporting line to an individual who has sufficient authority to ensure appropriate audit coverage, consideration and response; selection and dismissal of the director of internal auditing only with board of directors' or audit committee's concurrence; internal auditor access to the board or audit committee; and internal auditor authority to follow up on findings and recommendations.

Internal auditors are objective when not placed in a position of subordinating their judgment on audit matters to that of others. The primary protection for this objectivity is appropriate internal auditor staff assignments. These assignments should be made to avoid potential and actual conflicts of interest and bias. Staff assignments should be rotated periodically and

[1] The Institute of Internal Auditors, Inc., *Codification of Standards for the Professional Practice of Internal Auditing* (Altamonte Springs, FL: IIA, 1989).

internal auditors should not assume operating responsibilities. Similarly, they should not be assigned to audit activities with which they were involved recently in connection with prior operating assignments.

It should be recognized that the internal audit function does not—as some people believe—have primary responsibility for establishing or maintaining the internal control system. That, as noted, is the responsibility of the CEO, along with key managers with designated responsibilities (which may include the chief internal auditor). The internal auditors play an important role in evaluating the effectiveness of control systems and thus contribute to ongoing effectiveness. Because of organizational position and authority in an entity, and the objectivity with which it carries out its activities, an internal audit function often plays a very significant role in effective internal control.

Other Entity Personnel

Internal control is, to some degree, the responsibility of everyone in an entity and therefore should be an explicit or implicit part of everyone's job description. This is true from two perspectives.

- First, virtually all employees play some role in effecting control. They may produce information used in the internal control system—for example, inventory records, work-in-process data, sales or expense reports—or take other actions needed to effect control. These actions may include performing reconciliations, following up on exception reports, performing physical inspections or investigating reasons for cost variances or other performance indicators. The care with which those activities are performed directly affects the effectiveness of the internal control system.
- Second, all personnel should be responsible for communicating to a higher organizational level problems in operations, noncompliance with the code of conduct, or other violations of policy or illegal actions. Internal control relies on checks and balances, including segregation of duties, and on employees' not "looking the other way." Personnel should understand the need to resist pressure from superiors to participate in improper activities, and channels outside of normal reporting lines should be available to permit reporting of such circumstances.

Internal control is everyone's business, and roles and responsibilities of all personnel should be well defined and effectively communicated.

External Parties

A number of external parties can contribute to achievement of the entity's objectives—sometimes by actions that parallel those taken within an entity. In other cases, external parties may provide information useful to the entity in its internal control activities.

External Auditors

Perhaps no other external party plays as important a role in contributing to achievement of the entity's financial reporting objectives as the independent certified public accountants. They

bring to management and the board of directors a unique independent and objective view, and contribute to an entity's achievement of its financial reporting objectives, as well as other objectives.

In connection with a financial statement audit, the auditor expresses an opinion on the fairness of the financial statements in conformity with generally accepted accounting principles, and thus contributes to the entity's financial reporting objectives. While an entity's internal control system can provide a degree of assurance regarding the fair presentation of the financial statements, the auditor brings the assurance to a higher level. The auditor, in addition, often provides information to management useful to them in conducting their control responsibilities.

People have different perceptions regarding the attention given during a financial statement audit to an entity's internal control system. Some believe that an auditor expressing a standard, unqualified, "clean" opinion on the financial statements has concluded that the entity's internal control system is effective. Others believe that, at the very least, the auditor necessarily has conducted a sufficiently thorough review of the internal control system to identify all or most significant weaknesses. Neither of these views is accurate.

To put a financial statement audit in perspective, it may help first to recognize that an entity can have an ineffective internal control system, and an auditor may still be able to issue an opinion that the financial statements are "fairly presented." This is because an auditor focuses attention directly on the financial statements. If corrections to the financial statements are needed, they can be made, in which case a "clean" opinion can be rendered. The auditor gives an opinion on the financial statements, not on the internal control system. Inadequate controls may affect the audit, and make it more costly, due to the need for the auditor to perform more extensive tests of financial statement balances before forming an opinion.

An auditor must gain sufficient knowledge of an entity's internal control system in order to plan the audit. The extent of attention given to internal control varies from audit to audit. In some cases, considerable attention is given, and in others, relatively little attention is given. But even in the former case, an auditor usually would not be in a position to identify all internal control weaknesses that might exist.

In most cases, auditors conducting a financial statement audit do, in fact, provide information useful to management in carrying out their internal control-related responsibilities:

- By communicating audit findings, analytical information and recommendations for use in taking actions necessary to achieve established objectives.
- By communicating findings regarding deficiencies in internal control that come to their attention, and recommendations for improvement.

This information frequently will relate not only to financial reporting but to operations and compliance activities as well, and can make important contributions to an entity's achieve-

ment of its objectives in each of these areas. The information is reported to management and, depending on its significance, to the board of directors or audit committee.

Legislators and Regulators

Legislators and regulators affect the internal control systems of many entities, either through requirements to establish internal controls or through examinations of particular entities. Many of the relevant laws and regulations deal only with internal controls over financial reporting, although some, particularly those that apply to government organizations, can deal with operations and compliance objectives, as well.

The Foreign Corrupt Practices Act of 1977 requires that public companies establish and maintain internal accounting control systems that satisfy specified objectives. Other federal laws and regulations apply to federal financial assistance programs, which address a variety of activities ranging from civil rights matters to cash management, and specify required internal control procedures or practices. The Single Audit Act of 1984 requires independent auditors to report on entities' compliance with the requirements—as do a number of regulations in certain industries such as financial services. The Federal Deposit Insurance Corporation Improvement Act of 1991 requires that certain banks report on the effectiveness of their internal controls over financial reporting, along with an independent auditor's attestation report.

Several regulatory agencies directly examine entities for which they have oversight responsibility. For example, federal and state bank examiners conduct examinations of banks, and often focus on certain aspects of the banks' internal control systems. These agencies make recommendations, and frequently are empowered to take enforcement action.

Thus, legislators and regulators affect entities' internal control systems in two ways. They establish rules that provide the impetus for management to ensure that internal control systems meet the minimum statutory and regulatory requirements. And, pursuant to examination of a particular entity, they provide information used by the entity's internal control system, and provide recommendations and sometimes directives to management regarding needed internal control system improvements.

Parties Interacting with the Entity

Customers, vendors and others transacting business with an entity are an important source of information used in conducting control activities:

- A customer, for example, informs a company about shipping delays, inferior product quality or failure to otherwise meet the customer's needs for product or service. Or, a customer may be more proactive and work with an entity in developing needed product enhancements.
- A vendor provides statements or information regarding completed or open shipments and billings, which is used in identifying and correcting discrepancies and reconciling balances.
- A potential supplier notifies top management of an employee's request for a kickback.

These parties provide information that, in some cases, can be extremely important to an entity in achieving its operations, financial reporting and compliance objectives. The entity must have mechanisms in place with which to receive such information and to take appropriate action. Appropriate action would include not only addressing the particular situation reported, but also investigating the underlying source of the problem and fixing it.

In addition to customers and vendors, other parties, such as creditors, can provide oversight regarding achievement of an entity's objectives. A bank, for example, may request reports on an entity's compliance with certain debt covenants, and recommend performance indicators or other desired targets or controls.

Financial Analysts, Bond Rating Agencies and the News Media

Financial analysts and bond rating agencies consider many factors relevant to an entity's worthiness as an investment. They analyze management's objectives and strategies, historical financial statements and prospective financial information, actions taken in response to conditions in the economy and marketplace, potential for success in the short and long term, and industry performance and peer group comparisons. The print and broadcast media, particularly financial journalists, may also at times undertake similar analyses.

The investigative and monitoring activities of these parties can provide insights to management on how others perceive the entity's performance, industry and economic risks the entity faces, innovative operating or financing strategies that may improve performance, and industry trends. This information is sometimes provided directly in face-to-face meetings between the parties and management, or indirectly in analyses for investors, potential investors and the public. In either case, management should consider the observations and insights of financial analysts, bond rating agencies and the news media that may enhance internal control.