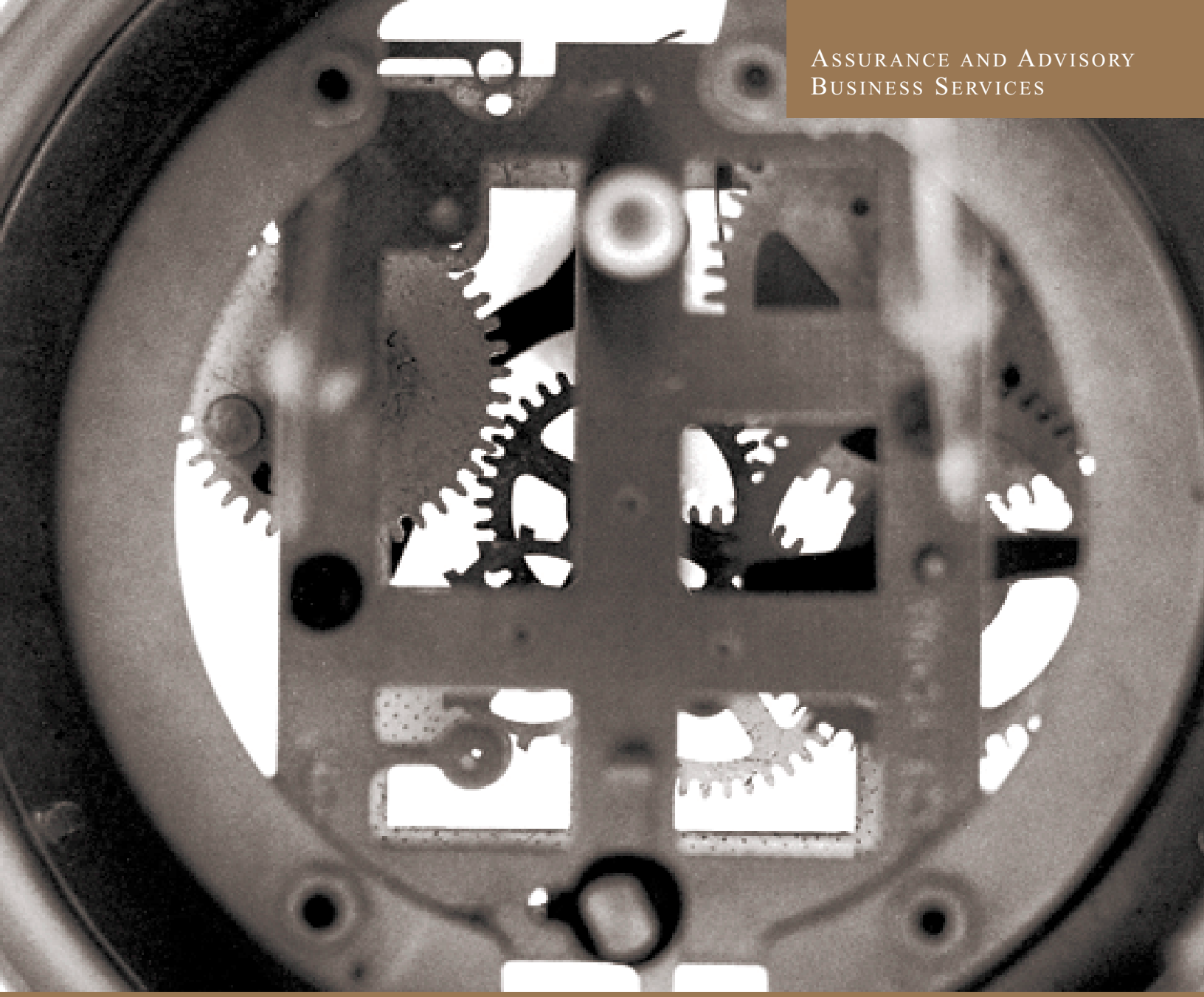


Assurance and Advisory
Business Services

Ernst & Young

Quality In Everything We Do

Preparing for Internal Control Reporting

A Guide for Management's Assessment under Section 404 of the Sarbanes-Oxley Act

To Our Clients and Other Friends

The recently enacted Sarbanes-Oxley Act of 2002 (the Act) finally makes reporting on internal control a reality for SEC registrants and their independent auditors. While this has been the subject of much discussion and debate for nearly 30 years, until now, only the Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA) has required many insured depository institutions to provide reports from management on the effectiveness of internal controls over financial reporting, as well as reports from independent auditors on their examination of management's assertions.

This Guide addresses the pending requirements of Section 404 of the Act. Section 404(a) of the Act directs the SEC to adopt rules requiring annual reports (i.e., Forms 10-K, 10-KSB, 20-F, and 40-F) to contain an assessment, as of the end of the issuer's fiscal year, of the effectiveness of internal control over financial reporting. Section 404(b) of the Act requires the new Public Company Accounting Oversight Board (the Board) to adopt standards for independent auditors to attest to management's report on internal control. The SEC and the new Board still must complete the required standard setting, so the new Section 404 internal control reports will not become effective in 2002. According to the recent SEC rule proposal, the rules under Section 404, if adopted, would apply to companies whose fiscal years end on or after September 15, 2003. However, management should not wait for the final rules to begin the process of developing appropriate documentation and establishing procedures for evaluating internal controls.

Separately, as required by Section 302(a) of the Act, the SEC recently adopted final rules requiring a company's CEO and CFO to certify each quarterly and annual report. For such reports for periods ending after August 29, 2002, the CEO and CFO must assess the effectiveness of the issuer's disclosure controls and procedures, of which internal controls over financial reporting are a part. However, these rules do not require attestation and reporting by the independent auditor with respect to that assessment or the related disclosures about controls and procedures in annual and quarterly reports. Because the new SEC rules do not establish standards for making such assessments, we expect that most companies will need to

develop much more extensive documentation and evaluation procedures in connection with their future Section 404 reports than would appear to be necessary for the current Section 302 certifications. Our separate publications, *Summary of SEC Final Rule: Certification of Disclosure in Companies' Quarterly and Annual Reports,* and *Implementation Considerations for the Evaluation and Certification of Disclosure Controls and Procedures*, provide information on the Section 302 certification under the new SEC rules.

Companies have long recognized the importance of strong internal controls. Effective internal control can help companies achieve established financial goals, prevent loss of resources, and prepare reliable financial statements. And, as amended in 1977, the Securities Exchange Act requires that companies maintain adequate internal control. As a result, many companies already have some level of documentation of their internal controls. However, most companies have not completed the comprehensive documentation and evaluation procedures that mandatory public reporting on internal control by management and independent auditors will require. Starting now, rather than later, not only will help you prepare for the future reporting requirements, but also will help identify areas where controls should be strengthened, or redesigned to be more effective and efficient.

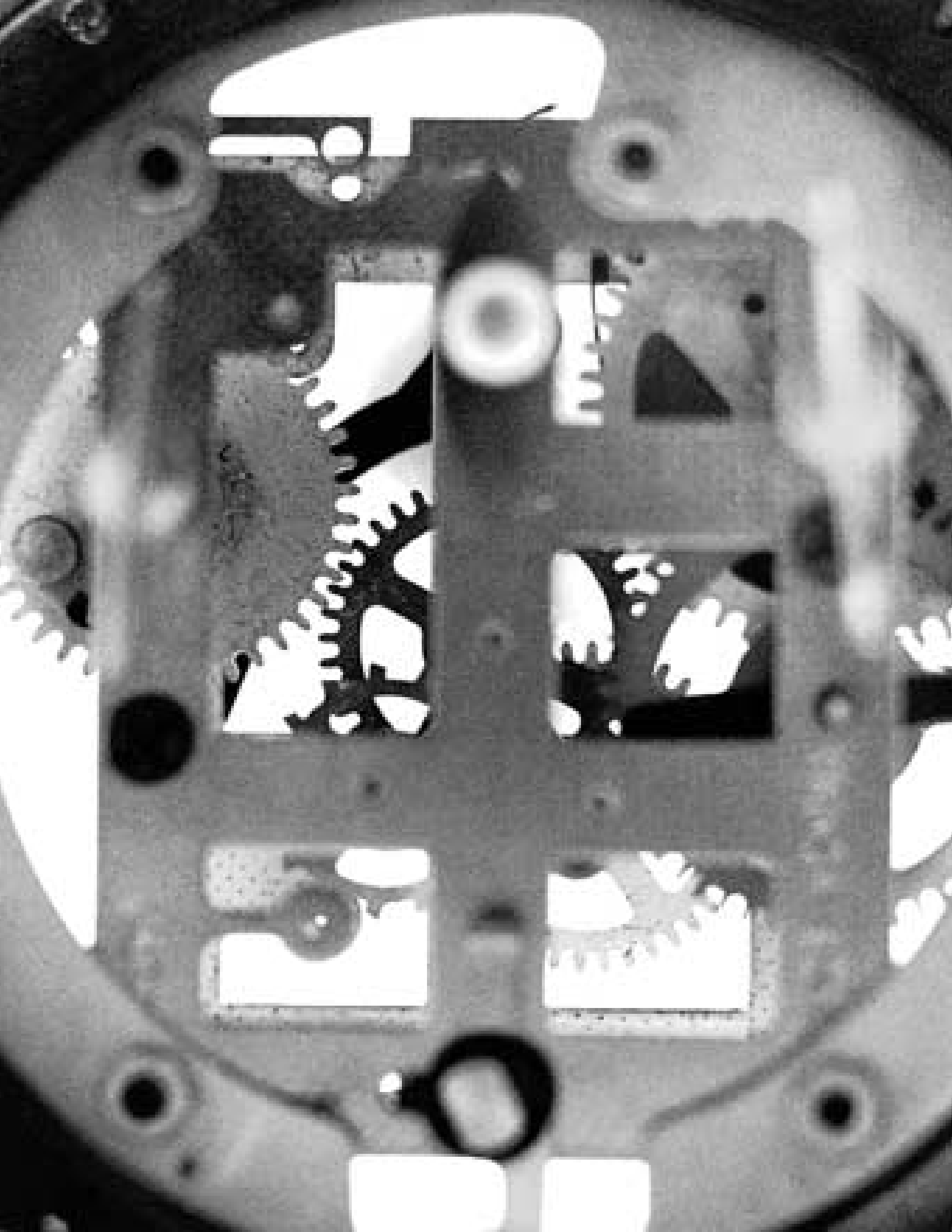
The most commonly used and understood framework for evaluating internal controls over financial reporting is that contained in the report of The Committee of Sponsoring Organizations of the Treadway Commission (COSO). The COSO report, *Internal Control—Integrated Framework*, established a broad definition of internal control extending to all objectives of an organization. The COSO report established three categories of controls: effectiveness and efficiency of operations, reliability of financial reporting, and compliance with laws and regulations. It also identified five interrelated components that must be present and functioning to have an effective internal control system, and it described the criteria for effective internal control. Although the rules for reporting under Section 404 of the Act have not yet been finalized, the recent SEC rule proposal indicates that management's assessment of internal controls and procedures for financial reporting would be based on current auditing standards relating to internal control, which are consistent with the definition contained in the COSO report.

This Guide is designed to assist management by providing a methodology for transforming COSO's conceptual framework into a detailed, meaningful evaluation of internal controls over financial reporting. In addition to this Guide, we offer to our clients our years of extensive experience in the evaluation of internal controls and additional guidance and tools that we will develop as the SEC and the new Board propose and adopt specific requirements.

We would be pleased to discuss these materials with you. Our knowledge and experience can assist you in documenting and developing a process for evaluating internal controls in your organization.

Methodology for Evaluating Internal Controls

Phase	Comments
Understand the Definition of Internal Control	The starting point for an evaluation of internal control is defining the criteria against which the assessment will be made. Section 1 discusses the definition of internal control as established by the COSO report.
Organize a Project Team to Conduct the Evaluation	Selecting an appropriate team and establishing ground rules such as responsibilities, documentation approach, and timing are important to a successful project. Section 2 discusses these matters.
Evaluate Internal Control at the Entity Level	Begin the evaluation by considering internal control at the entity level. Strong internal control at the entity level is an important part of an effective system of internal control. Section 3 explains the elements of the five components of internal control that may have a pervasive effect on the organization.
Understand and Evaluate Internal Control at the Process, Transaction, or Application Level	Controls at the process, transaction, or application level also are important to an effective system of control. This phase likely will require the most time to complete. As discussed in Section 4, completing this phase involves: ▸ Determining significant accounts ▸ Identifying significant processes that affect those accounts ▸ Identifying the major classes of transactions that are embedded in those significant processes ▸ Determining where errors could occur in the processes ▸ Identifying controls designed to prevent or detect those errors
Evaluate Overall Effectiveness, Identify Matters for Improvement, and Establish Monitoring System	The evaluation of the overall effectiveness of internal control is both the end and the beginning of the process. In a dynamic business environment, controls will require modification from time to time. Certain systems may require control enhancements to respond to new products or emerging risks. In other areas, the evaluation may point out redundant controls or other procedures that are no longer necessary. In either event, the discussion of the evaluation process, ongoing monitoring, and cost-benefit considerations included in Section 5 will be useful in making such determinations.



Contents

Methodology for Evaluating Internal Controls

Understand the Definition of Internal Control

- COSO Definition

Organize a Project Team to Conduct the Evaluation

Evaluate Internal Control at the Entity Level

Understand and Evaluate Internal Control at the Process, Transaction, or Application Level

Evaluate Overall Effectiveness, Identify Matters for Improvement, and Establish Monitoring System

1 Understanding Internal Control

The environment in which companies conduct their business continues to change dramatically. Economic factors, advances in technology, and increasing global competition are just a few examples of these changes. With each new development, management is faced with greater challenges to control costs, manage liquidity, and achieve a competitive advantage.

These challenges have intensified the concern of both management and directors over their ability to evaluate operating performance. Also, the recent increase in high profile business failures, allegations of corporate fraud, and financial statement restatements has directed public and congressional attention to, among other things, the adequacy of internal control over financial reporting. To protect investors by improving the accuracy and reliability of corporate disclosures, the Sarbanes-Oxley Act of 2002 (the Act) was passed by Congress and signed into law by the President. Certain provisions of the Act require certifications of each quarterly and annual report filed with the Securities and Exchange Commission (SEC) by an issuer's CEO and CFO, including representations on certain control-related matters. Other provisions that are not yet effective will require an annual internal control report by management stating the responsibility of management for establishing and maintaining adequate internal controls for financial reporting, and providing an assessment, as of the end of the most recent fiscal year, of the effectiveness of the issuer's internal control structure and procedures for financial reporting. The issuer's independent auditor also will be required to attest to and report on management's assessment pursuant to standards to be developed by the new Public Company Accounting Oversight Board (the Board).

The SEC created a new term—"disclosure controls and procedures"—in its final rule for implementing the CEO and CFO requirements of Section 302 of the Act. Some elements of the final rule are effective for reports filed after August 29, 2002, while others are effective for reports filed for periods ending after August 29, 2002. We believe the

SEC's intent was to develop a broader concept that includes not only the traditional internal controls over financial reporting but also the controls over the disclosure of all material financial and non-financial information in Exchange Act reports. This Guide is not intended to provide guidance on the periodic Section 302 certifications. We have summarized the SEC final rule and related implementation considerations in other Ernst & Young publications.

Instead, this Guide is designed to provide management with an approach for developing, over a period of time, a comprehensive assessment and documentation of the effectiveness of internal controls over financial reporting. Such an assessment and related supporting documentation eventually will be required for management assessments and independent auditor attestations on management assessments pursuant to Section 404 of the Act. Internal control reporting will not become effective until final rules are adopted by the SEC and the Board. However, according to the recent SEC rule proposal, the rules under Section 404, if adopted, would apply to companies whose fiscal years end on or after September 15, 2003. Accordingly, starting now rather than later will help you not only prepare for the future Section 404 reporting requirements, but also identify areas where controls should be strengthened or redesigned to be more effective and efficient.

The Importance of Internal Controls

Internal controls are fundamental to the accurate recording of transactions and the preparation of reliable financial reports. Many business activities involve a high volume of transactions and numerous judgments each day. Without adequate controls to ensure the proper recording of transactions, the resulting financial data may become unreliable and undermine management's ability to make decisions, as well as its credibility with shareholders, regulators, and the public.

An effective internal control structure (also referred to as the system of internal control or, more simply, internal control) is comprehensive and involves people throughout the organization, including many who do not think of themselves as having any accounting or control responsibilities (e.g., workers reporting time spent on specific projects or tasks). Of course, it also involves those who keep accounting records, prepare and disseminate policies, and monitor systems. Finally, it involves members of the board of directors and audit committees, who have ultimate responsibility for oversight of the financial reporting process.

The enactment of the Foreign Corrupt Practices Act (FCPA) in 1977 emphasized the importance of internal controls. The FCPA, which amended the Securities Exchange Act, requires all publicly held companies (whether or not they are involved in foreign operations) to (1) devise and maintain a system of internal control sufficient to provide reasonable assurance that assets are safeguarded and transactions are properly authorized and recorded, and (2) keep reasonably detailed records that accurately and fairly reflect financial activities.

Subsequently, the importance of internal controls has been emphasized in many ways. Auditing standards related to internal control have been updated and enhanced. The Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA) introduced requirements for management of certain federally insured financial institutions to report on internal control over financial reporting and compliance with certain laws and regulations, accompanied by independent auditor attestation reports on the examination of management assessments of internal control over financial reporting and agreed-upon procedures related to compliance with certain laws and regulations. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued its final report on internal control in 1992 based on a three-year study. And, most recently, the Act has added requirements for management certification on control-related matters and for reporting on internal control over financial reporting.

As a result of the passage of the Act, senior executives of all public companies are focusing renewed attention on the design, operation, and effectiveness of the system of internal control in their organizations. They also are

developing processes and documentation to support the new Section 302 certification requirements of the Act, as well as the future Section 404 reporting requirements that will be adopted by the SEC. Such actions will help identify those areas where corrective action, if any, is necessary and allow time to design and implement such corrective action before the initial Section 404 report.

This Guide is designed to provide management with an approach to assess and document the effectiveness of internal controls over financial reporting. We anticipate developing additional guidance when the SEC and the new Board propose and adopt the rules and standards for implementing the internal control reporting and auditor attestation reporting requirements of Section 404 of the Act.

Defining Internal Control

In order to assess an organization's internal control, one must first identify the criteria against which the assessment will be made. Therefore, it is important to appropriately define internal control early in the evaluation process. In September 1992, COSO issued a report that provides a definition of internal control and establishes criteria that can be used to evaluate an organization's internal controls. The COSO report, *Internal Control—Integrated Framework*, contains the most widely accepted definition of internal control.

The COSO report defines internal control 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 three categories: effectiveness and efficiency of operations, reliability of financial reporting, and compliance with laws and regulations. It also identifies five interrelated components of effective internal control:

- Control environment
- Risk assessment
- Control activities
- Information and communications
- Monitoring

This definition also is the basis for the guidance for independent auditors included in Statement on Auditing Standards (SAS) No. 55, *Consideration of Internal Control in a Financial Statement Audit*, as amended by SAS 78 and SAS 94. Although the rules for reporting under Section 404 of the Act have not yet been finalized, the recent SEC rule proposal indicates that management's assessment of internal controls and procedures for financial reporting would be based on current auditing standards relating to internal control, which are consistent with the definition contained in the COSO report. In addition, there is uncertainty as to whether the new Board will expand on the current AICPA attestation standards for internal control reporting. We suggest getting started based on an assumption that the current standards, or substantially similar ones, will be in effect.

Evaluating the Effectiveness of Internal Controls

This Guide will assist management in developing a process for evaluating and documenting the effectiveness of internal controls over financial reporting based on the definitions included in SAS 55, as amended, and the COSO report. Although there are some terminology differences, this Guide addresses all the concepts or components embodied in SAS 55, as amended, and in the COSO report related to internal controls over financial reporting. This Guide may be used independently, or it may be used to complement COSO materials.

The fourth volume of the COSO report, *Evaluation Tools*, provides illustrative guidance and assistance in evaluating internal control systems in relation to the criteria for effective internal controls set forth in COSO's first volume, *Framework. Evaluation Tools* includes a set of blank evaluation forms, a reference manual, and an illustrative set of the forms completed for a hypothetical company. Although the COSO materials may be useful in evaluating a system of internal control, they do not provide a vehicle to evaluate controls at a detailed level. As the COSO report indicates, the guidance in the *Evaluation Tools* volume is "for purely illustrative purposes" and is not intended to present "…a preferred method to conduct and document an evaluation."

Controls Over Compliance with Laws and Regulations and Operations

While COSO's definition of internal control encompasses controls over financial reporting, compliance with laws and regulations, and effectiveness and efficiency of operations, the COSO report recommends that external reporting by management should be focused on those internal controls that relate to financial reporting objectives. Pending issuance of the related rules and standards by the SEC and new Board, we believe the COSO recommendation is reasonable in preparing for Section 404 reporting.

Presently there are no established criteria to measure the effectiveness of internal controls over compliance with laws and regulations or the effectiveness and efficiency of operations. This Guide focuses on controls over financial reporting. However, there are many similarities and common considerations among controls related to all three internal control objectives, and much of this Guide would be useful in an evaluation of controls over compliance with laws and regulations or operations.

A Detailed Study of Control

Some companies already have extensive documentation of their procedures and control mechanisms, including accounting policy and procedure manuals, information systems manuals, and job descriptions. Also, internal audit departments often have documentation of internal controls and procedures and have tested whether selected controls are functioning as designed. Finally, the independent auditors likely will have evaluated controls in some areas. However, the focus of a financial statement audit is to give an opinion on the annual financial statements—not to report on the system of internal control. Financial statement audit procedures are designed to be performed most effectively and efficiently in order to conclude as to the fairness of amounts and disclosures presented in the financial statements. Such audit procedures may include extensive substantive procedures and may not necessarily include tests of controls affecting all significant accounts. Therefore, it is unlikely that the independent auditors' working papers will contain documentation of controls adequate to meet the needs of management for purposes of Section 404 of the Act.

Thus, while a great deal of documentation relating to systems and controls may be available, companies may not have completed a comprehensive documentation and evaluation of the effectiveness of their internal controls as contemplated by COSO and sufficient to support separate internal control reporting and attestation.

The Treadway Commission envisioned a comprehensive study and evaluation of controls when it recommended that public companies perform the following steps in their efforts to prevent and detect fraudulent financial reporting:

- Identify and understand the factors that can lead to fraudulent financial reporting, including factors unique to the company
- Assess the risk of fraudulent financial reporting that these factors create within the company
- Design and implement internal controls that will provide reasonable assurance that fraudulent financial reporting will be prevented or detected

This Guide suggests a practical approach to performing and documenting this comprehensive evaluation of a company's internal control. It can be used to review existing controls and documentation for completeness and to determine whether controls should be improved in any area.

Other Benefits of This Process

In addition to providing a basis for management's future reporting under Section 404 of the Act, a comprehensive evaluation of internal control also might result in:

- Reducing the cost of accounting processes
- Identifying existing control procedures that are redundant, inefficient, or cost ineffective
- Simplifying systems

- Increasing productivity
- Improving the effectiveness of the design or operation of controls

For example, some companies may find that automating certain manual controls improves both efficiency and compliance with management's policies. Others may find that certain procedures are duplicative or no longer effective or necessary (e.g., because of changes in the environment).

Methodology for Evaluating Internal Controls

Understand the Definition of Internal Control

Organize a Project Team to Conduct the Evaluation

Consider Including Personnel From:
- Operations
- Finance and Accounting
- Information Technology
- Internal Audit

Evaluate Internal Control at the Entity Level

Understand and Evaluate Internal Control at the Process, Transaction, or Application Level

Evaluate Overall Effectiveness, Identify Matters for Improvement, and Establish Monitoring System

2 Organizing the Evaluation

Business enterprises differ greatly, and a company's distinguishing characteristics—such as its size, complexity, and where it does business—will influence how it organizes any evaluation of its internal control. The larger the enterprise, the more likely that senior management is farther away from day-to-day operations, and the more formal the approach to the evaluation probably should be. In addition, the level of existing documentation of the various internal control components also will affect how the evaluation will be organized and performed.

Each company must decide for itself how best to organize for the evaluation. Many companies might have followed the SEC's suggestion to establish a "disclosure committee" in connection with preparing for the certifications required under Section 302 of the Act. The SEC indicated that such a disclosure committee would function under the oversight of the CEO and CFO and generally would be expected to include the controller or principal accounting officer, general counsel, principal risk management officer, chief (or principal) investor relations officer, and the appropriate business segment managers.

Because internal control over financial reporting is a subset of the broader "disclosure controls and procedures" term that the SEC created in its recent rulemaking on Section 302 certifications, there likely would be some overlap of members of a disclosure committee and members of a team that is responsible for assessing and documenting internal control over financial reporting for the annual Section 404 requirements. Companies might want to supplement a disclosure committee with others. The important considerations are that the responsibility for the evaluation be assigned to qualified individuals and that those individuals have the necessary authority to conduct the evaluation in a manner deemed appropriate for the size, complexity, and structure of the organization. The approach outlined below suggests the formation of a committee or project team to perform the evaluation.

Project Sponsor

The project sponsor should be one of the company's principal executives (such as the CEO or CFO, both of whom now must make periodic certifications) to (1) emphasize the importance attached to the successful completion of the evaluation, and (2) increase the likelihood that communications from the project team will be given a high priority throughout the company.

The Project Team

The function of the project team is to plan and supervise the development, staffing, and execution of the company's internal control evaluation. Thus, the project team will design the evaluation and recommend who is to be involved, what allocation of company resources will be necessary, and how the evaluation is to be completed.

The project team leader should be a senior officer who has significant authority to garner immediate attention to questions and concerns raised by the project team. The project team members should be seasoned managers who, as a group, are familiar with the operations of the company, the business risks of its various activities, its controls, and the legal and regulatory requirements that apply to it.

The project team might include the following personnel:

Operations —

- Management representative(s) of the company's major business segments
- Management representative(s) of the company's foreign operations

Finance and Accounting —

- Corporate controller and/or chief financial officer
- Major business segment and/or foreign operation controllers

Information Technology —

- Chief information officer
- Security officer

Internal Audit —

- General auditor or vice president — internal audit
- Directors from internal audit function

Companies in certain specialized industries should also consider involving personnel from quality control groups or quasi-audit functions. For example, financial institutions should consider involving a representative from credit review, and insurance companies should consider involving actuaries or representatives from the loss reserve committee.

A project team should have the capability and the authority to make the necessary judgments and recommend changes concerning such subjective and sensitive matters as "control consciousness," cost-benefit analyses, and the effectiveness of the company's internal control. Since the evaluation of "control consciousness" involves the attitudes of senior management, the project team also should include an individual who can deal with the subject objectively — such as an audit committee member, legal counsel, or an outside specialist.

The project team is responsible for ensuring satisfactory completion of the evaluation. However, the degree of involvement by the project team in executing the evaluation likely will differ from company to company and from activity to activity. For example, the project team as a whole should be concerned with policy and decision-making, including identifying the individual accounting systems that require review at the company's various locations. However, the team may well delegate the gathering of information and the supervising of the day-to-day activities of those performing the study and evaluation. For example, it may be appropriate for the internal auditor or the controller and his or her staff to analyze the identified accounting systems and present recommendations to the project team, as a group, for its approval. Or, in evaluating controls over inventories, it may be appropriate for operations personnel to be directly involved in the process. However, training regarding the evaluation process and the documentation tools will be especially important to ensure consistency and quality in situations where multiple teams conduct evaluations and complete documentation.

As indicated earlier, the board and senior management should oversee the company's evaluation efforts. Such oversight might include review of periodic reports and the final report from the project team.

A Plan of Action

The project team should develop a plan of action outlining its intended objectives and activities. The plan should include the following:

Organization —

- To whom the project team will report
- Project team leader and other project team members and their principal responsibilities
- Experts in specialized areas, such as information systems, who will work with the project team
- External advisors and how they will be involved

Scope and timing of the review —

- The factors in the control environment to be reviewed
- The significant accounts and related processes to be considered (This step ensures that all important financial statement accounts and footnote disclosures are included in the review of internal controls over significant processes.)

- The internal controls over financial reporting to be evaluated at each location
- To the extent that companies will want to evaluate controls in areas beyond financial reporting (e.g., compliance with specific laws and regulations, risk management/insurance, merger and acquisition processes, system conversions), the project team will need to identify these additional areas of focus in the planning stages of the effort
- The planned scope of the evaluations, which may vary from system to system depending on the information already available
- The planned timetable for completing the project team's various activities

Problem areas for early attention —

- Processes that are suspected of containing significant deficiencies or material weaknesses
- Locations or processes about which little information is available, such as systems in a new subsidiary

Documentation and reports —

- The planned timing and content of reports and to whom they will be addressed
- The other types of documentation to be developed by the project team, such as memoranda of decisions, flowcharts, and minutes of meetings

Background information —

- Summary information about the company's organization (subsidiaries and divisions) and its principal business activities
- Information about the company's accounting and record-keeping systems, such as where accounting data are processed, the significant processes at each location, the extent to which the various processes are integrated, the budgetary system, and financial reporting requirements (internal and external)
- An inventory of the company's documentation of its internal controls (e.g., policy and procedure manuals, internal audit working papers and reports)
- Information about existing self-assessment and reporting mechanisms in place for various locations, organizational units, etc.
- The project team's principal contacts at each location

Getting Started

The first step in evaluating internal controls is assessing internal control at the entity level. Once that assessment is completed, the project team gains an understanding of the processes by which financial statement information is generated, considers the types of errors that could occur (i.e., what could go wrong), and considers the relevant internal control policies and procedures designed to prevent or detect the types of errors that could occur. The completion of these phases will provide the project team with the information necessary to conclude as to the effectiveness of the design of the company's internal control. The final step is to perform testing to determine that the controls are in fact functioning as designed. For many companies, the internal audit department will have already performed the testing of some controls. The other sections of this Guide provide additional guidance on these phases of the process of understanding and evaluating internal control.

Documentation

The project team should issue ongoing internal reports on the various procedures that were performed, as well as its conclusions and recommendations. In addition to the documentation prepared during the evaluation process, other documentation may be necessary to show the company's commitment to organizing, performing, and completing the review of its internal controls, and to demonstrate that a system is in place to continually monitor effectiveness. This documentation might include:

- Project timetable and responsibilities
- Board of director and/or audit committee minutes
- Correspondence with corporate counsel and the independent auditor
- A summary of weaknesses identified while completing the evaluation and the related follow-up to be performed

The project team should also consider how the results of the evaluation will be communicated within the organization. Detailed findings should be presented to the individuals directly responsible for controls evaluated. Those findings should be summarized and presented with an overall evaluation to senior management and to the audit committee.

Methodology for Evaluating Internal Controls

Understand the Definition of Internal Control

Organize a Project Team to Conduct the Evaluation

Evaluate Internal Control at the Entity Level

- Control Environment
- Risk Assessment
- Information and Communication
- Control Activities
- Monitoring

Understand and Evaluate Internal Control at the Process, Transaction, or Application Level

Evaluate Overall Effectiveness, Identify Matters for Improvement, and Establish Monitoring System

3 Evaluating Internal Control at the Entity Level

A logical place to begin any comprehensive evaluation of internal controls is at the top—internal control at the entity level. This step includes a review of those elements of the five components of internal control that have a pervasive effect on the organization.

The following are the five components of internal control:

- *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.
- *Risk Assessment* is the entity's identification and analysis of relevant risks to the achievement of its objectives, forming a basis for determining how the risks should be managed.
- *Information and Communication* systems support the identification, capture, and exchange of information in a form and time frame that enable people to carry out their responsibilities.
- *Control Activities* are the policies and procedures that help ensure that management's directives are carried out.
- *Monitoring* is a process that assesses the quality of internal control performance over time.

Control Environment

The Treadway Commission stated that the tone set by top management—the corporate environment or culture within which financial reporting occurs—is the most important factor contributing to the integrity of the financial reporting process. In other words, if the tone set by management is lax, an impressive set of written rules and procedures will accomplish little.

The control environment reflects the overall attitude, awareness, and actions of the board of directors, management, owners, and others concerning the importance of control and the emphasis placed on control in the company's policies, procedures, methods, and organizational structure. The control environment encompasses management's attitude toward the development of accounting estimates and its financial reporting philosophy, and is the context in which the accounting system and internal controls operate.

In its report, *Internal Control—Integrated Framework*, COSO stated, "The control environment has a pervasive influence on the way business activities are structured, objectives [are] established and risks [are] assessed. It also influences control activities, information and communications 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 the atmosphere within which a company's accounting controls exist and the financial statements are prepared. Therefore, obtaining an understanding of the control environment is essential in the process of identifying factors that may have a pervasive effect on the risk of errors in the processing of transactions, and on the judgments management makes when it prepares financial statements. A satisfactory control environment does not guarantee the effectiveness of any specific control, but it can be a positive factor in assessing the risk of errors. An effective control environment also provides a basis for expecting that accounting systems that are functioning properly at one point in the year will continue to function properly throughout the year. Therefore, the control environment is a key ingredient of effective internal controls.

The project team considers the following factors as they review the control environment:

- Integrity, ethical values, and behavior of key executives
- Management's control consciousness and operating style
- Commitment to competence
- Board of directors and/or audit committee participation in governance and oversight
- Organizational structure and assignment of authority and responsibility
- Human resource policies and practices

Integrity, Ethical Values, and Behavior of Key Executives

Integrity and ethical values are essential elements of the control environment, affecting the design, administration, and monitoring of key processes. Integrity and ethical behavior are the product of the company's ethical and behavioral standards, how they are communicated, and how they are monitored and enforced in its business activities. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of the entity's values and behavioral standards to personnel through policy statements and codes of conduct, and by the examples the executives set.

Management's Control Consciousness and Operating Style

Management is responsible for directing and controlling operations and for establishing, communicating, and monitoring policies and procedures. Every aspect of the control environment is profoundly influenced by the actions and decisions (or, in certain cases, inaction or indecision) of management. In an effective control environment, management's control consciousness and operating style create a positive atmosphere that is conducive to the effective operation of the processes and controls, and an environment in which the likelihood of error is reduced.

Control consciousness refers to the importance management attaches to internal controls and thus to the environment in which specific controls function. For the most part, it is an intangible concept; a management attitude that, when communicated, helps ensure that adequate controls are in place and reduce the likelihood that specific controls will be circumvented.

Commitment to Competence

Commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge. Among the many factors that should be considered by management are the nature and degree of judgment to be applied to a specific job and the extent of supervision that will be provided. The project team considers whether key personnel appear to be competent to carry out their assigned responsibilities (e.g., whether personnel have the knowledge and expertise to understand and execute the requirements of the generally accepted accounting principles under which the company is required to report).

Board of Directors and/or Audit Committee Participation in Governance and Oversight

The board of directors, through its own activities and supported by an audit committee, is responsible for overseeing the accounting and financial reporting policies and procedures.

While the specific activities and responsibilities of audit committees vary and need to be modified or tailored to the individual circumstances, the board of directors has a fiduciary responsibility to shareholders and others for reliable financial reports. As a result, the board of directors and the audit committee should be concerned with the company's financial reporting to shareholders and the investing public, and they should monitor the company's accounting policies and the internal and independent audit processes.

In assessing the effects of the board of directors and/or audit committee on the control environment, the project team should consider such aspects as the board's and/or audit committee's independence from management, the experience and stature of its members, the extent of its involvement and its scrutiny of the company's activities, the appropriateness of its actions, the degree to which difficult questions are raised and pursued with management, and its interactions with the internal and independent auditors.

Organizational Structure and Assignment of Authority and Responsibility

The organizational structure of an entity provides the overall framework for planning, directing, and controlling operations. An effective organizational structure provides for the assignment of responsibility, such that all personnel within the company have a clear understanding of their reporting relationships and responsibilities.

In its review of the organizational structure, the project team should consider methods of (1) assigning authority, (2) monitoring decentralized operations, (3) assigning and monitoring responsibilities for information systems (including the use of service organizations), and (4) establishing and monitoring policies and procedures (e.g., conflict of interest, corporate security, and codes of conduct) throughout the organization.

The project team should focus on the substance of the organizational structure and methods of assigning authority and responsibility rather than merely their form. Accordingly, the overall level of awareness of and compliance with policies and procedures by company personnel is as important as the extent of management's monitoring of them. The review of the organizational structure can also assist the project team in determining the degree to which proper segregation of duties is achieved and to assess the effects of significant weaknesses in this regard.

Human Resource Policies and Practices

Human resource policies and practices relate to hiring, orienting, training, evaluating, counseling, promoting, and compensating personnel. The effectiveness of policies and procedures, including controls, usually depends on the individuals who execute them. Therefore, the competence and integrity of a company's personnel are important elements of its control environment. A company's ability to recruit and retain sufficient competent and responsible personnel is, in turn, dependent to a great extent on its human resource policies and practices. In addition, the level of competence and integrity of the personnel involved in a specific process is one of the factors to consider in evaluating the effectiveness of controls over the process.

Risk Assessment

All entities, regardless of size, structure, nature, or industry, encounter risks at all levels within their organization. Risks affect a company'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. In fact, 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 those levels.

The process of identifying, analyzing, and managing risks is a critical component of an effective internal control system. And, acknowledging that change is always present, identifying changed conditions, and taking actions as necessary to respond to those changes are fundamental to an effective risk assessment process.

In understanding the risk assessment process at the entity level, the project team considers such factors as:

- Whether entity-level objectives, including how they are supported by strategic plans and complemented on a process/application level, have been established and communicated
- Whether a risk assessment process, including estimating the significance of risks, assessing the likelihood of their occurrence, and determining needed actions, has been established
- Whether mechanisms are in place to anticipate, identify, and react to changes that may have a dramatic and pervasive effect on the entity (e.g., asset/liability management committee in a financial institution, commodities trading risk management group in a manufacturing entity)
- Whether mechanisms are in place to anticipate, identify, and react to routine events or activities that affect achievement of entity or process/application-level objectives
- Whether the accounting department has processes in place to identify significant changes in generally accepted accounting principles promulgated by relevant authoritative bodies
- Whether communication channels are in place to notify the accounting department of changes in the entity's business practices that may affect the method or the process of recording transactions
- Whether the accounting department has processes to identify significant changes in the operating environment, including regulatory changes

Information and Communication

Information and communication is the process of capturing and exchanging the information needed to conduct, manage, and control the company's operations. The quality of the company's information and communication system affects management's ability to make appropriate decisions in controlling the company's activities and to prepare reliable financial reports. Information and communication involves capturing and providing information to appropriate personnel so that they can carry out their responsibilities, including providing an understanding of individual roles and responsibilities pertaining to internal control over financial reporting.

In understanding the information and communication at the entity level, the project team considers such factors as:

Information

- Whether the information system provides management with necessary reports on the entity's performance relative to established objectives, including relevant external and internal information
- Whether information is provided to the right people in sufficient detail and on time to enable them to carry out their responsibilities efficiently and effectively
- To what extent information systems are developed or revised based on a strategic plan that is interrelated with the entity's overall information systems, and is responsive to achieving the entity-level and process/application level objectives
- Whether management commits the appropriate human and financial resources to develop the necessary information systems
- How management ensures and monitors user involvement in the development (including revisions) and testing of programs
- Whether a disaster recovery plan has been established for all primary data centers

Communication

- Whether management communicates employees' duties and control responsibilities in an effective manner
- Whether communication channels have been established for people to report suspected improprieties
- The adequacy of communication across the organization to enable people to discharge their responsibilities effectively
- Whether management takes timely and appropriate follow-up action on communications received from customers, vendors, regulators, or other external parties
- Whether the entity is subject to monitoring and compliance requirements imposed by legislative and regulatory bodies
- The extent to which other parties outside the entity (e.g., customers, suppliers) have been made aware of the entity's ethical standards and policies

Control Activities

Control activities are policies and procedures that help ensure that management's directives are carried out. They help ensure that the necessary actions are taken to address risks to achievement of the company's objectives. Control activities, whether automated or manual, have various objectives and are applied at various organizational and functional levels.

In understanding the control activities at the entity level, the project team considers such factors as:

- Whether the necessary policies and procedures exist with respect to each of the company's activities
- The extent to which controls called for by policy are being applied
- Whether management has clear objectives in terms of budget, profit, and other financial and operating goals, and whether these objectives are clearly written, communicated throughout the entity, and are actively monitored
- Whether planning and reporting systems are in place to identify variances from planned performance and communicate such variances to the appropriate level of management
- Whether the appropriate level of management investigates variances and takes appropriate and timely corrective actions
- To what extent duties are divided or segregated among different people to reduce the risk of fraud or inappropriate actions
- To what extent duties are divided logically through appropriate set up of information technology (IT) applications
- Whether periodic comparisons are made of amounts recorded in the accounting system with physical assets
- Whether adequate safeguards are in place to prevent unauthorized access to or destruction of documents, records, and assets
- Whether policies for controlling access to programs and data files have been established
- Whether access security software, operating system software, and/or application software is used to control access to data and programs
- Whether an information security function is in place and responsible for monitoring compliance with information security policies and procedures

Monitoring

An important management responsibility is to establish and maintain internal control. Management monitors controls to consider whether they are operating as intended and whether they are modified as appropriate for changes in conditions. Monitoring is a process of assessing the quality of internal control performance over time, considering whether controls are operating as intended, and assuring that they are modified as appropriate for

changes in conditions. It involves assessing the design and operation of controls on a regular basis and taking necessary corrective actions. This process is accomplished through ongoing activities and separate evaluations, or by various combinations of the two.

In understanding the monitoring processes at the entity level, the project team considers such factors as:

- Whether periodic evaluations of internal control are made
- The extent to which personnel, in carrying out their regular duties, obtain evidence as to whether the system of internal control continues to function
- The extent to which communications from external parties either corroborate internally generated information or indicate problems
- Whether management implements internal control recommendations made by internal and independent auditors
- Management's approach to correcting known reportable conditions on a timely basis
- Management's approach to dealing with reports and recommendations from regulators
- The existence of an internal audit function that management uses to assist in their monitoring activities, including factors such as:
  - —Independence (authority and reporting relationships)
  - —Reporting lines (reports directly to the board of directors and/or audit committee or has unrestricted access to the board of directors and/or audit committee)
  - —Adequacy of staffing, training, and existence of specialized skills given the environment (e.g., use of experienced, trained information systems auditors in complex and highly automated environments)
  - —Adherence to applicable professional standards
  - —Scope of activities (e.g., balance between financial and operational audits, coverage and rotation of decentralized operations)
  - —Adequacy of planning, risk assessment, and documentation of work performed and conclusions reached
  - —Freedom from operating responsibilities

The project team should evaluate whether the system of internal controls is self-monitoring and whether it includes appropriate mechanisms to ensure correction of any deficiencies noted. In the event the methods of self-monitoring and correction are evaluated as being inadequate, specific recommendations to improve the system should be proposed.

Smaller Business Considerations

In a smaller business, the manager (who frequently also is the owner) is, in effect, the substitute for many of the formal control mechanisms discussed in the preceding sections. A manager of a smaller business who assumes an active role in a company's day-to-day operations generally has a first-hand knowledge of all aspects of the business. Such a manager is in a position to monitor and control the business effectively and can be an important element in mitigating the absence of specific controls and a lack of segregation of duties. Moreover, when a manager is diligent and pays attention to detail, employees will probably do likewise.

Overall Assessment

Reaching conclusions about a company's internal control at the entity level involves a high degree of subjectivity because of the intangible nature of the factors to consider and because there are no objective, well-defined standards for assessing internal control at the entity level. The project team needs to identify mechanisms and procedures that are ineffective and those that are missing but needed. All this, however, should not be permitted to obscure the central fact that the best policies and practices in the world are worthless if the will to make them work is lacking.

The overall assessment of internal control at the entity level ultimately comes down to two important questions:

- Has management created a control environment in which people are motivated to comply with controls rather than to ignore or circumvent them?
- Has the company installed the necessary control mechanisms to monitor and correct noncompliance, and are the mechanisms functioning effectively?

Methodology for Evaluating Internal Controls

Understand the Definition of Internal Control

Organize a Project Team to Conduct the Evaluation

Evaluate Internal Control at the Entity Level

Understand and Evaluate Internal Control at the Process, Transaction, or Application Level

- Determine Significant Accounts
- Identify and Evaluate the Major Classes of Transactions
- Other Control Considerations
- Effects of Information Technology

Evaluate Overall Effectiveness, Identify Matters for Improvement, and Establish Monitoring System

4 Understanding and Evaluating Internal Control at the Process, Transaction, or Application Level

After completing an evaluation of internal control at the entity level, the organization's accounting system becomes the primary focus for the evaluation of internal control over financial reporting. For this purpose, the accounting system is represented by the individual processes (i.e., business processes and/or accounting activities) that are significant to the company's financial reporting.

Determine Significant Accounts

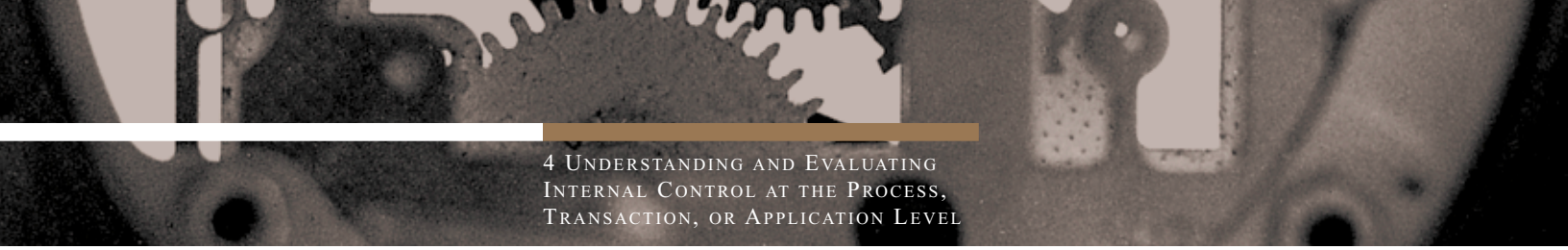
The starting point in identifying the significant processes is to identify the significant accounts or groups of accounts, beginning at the financial statement caption or footnote disclosure level. An account or group of accounts is significant if it could contain errors of importance (i.e., errors that individually or collectively could have a material effect on the financial statements, or other matters such as illegal acts, conflicts of interest, and unauthorized management perquisites that, even though they are not material, could adversely affect the company's reputation or its relationship with customers, shareholders, or the public if these matters were to remain undetected).

Other factors that should be considered in assessing the significance of an account include the size and composition of an account and its susceptibility to manipulation or loss; the nature of the account; the volume of activity; the size, complexity, and homogeneity of the individual transactions processed through the account; and the subjectivity in determining the account balance (i.e., the extent to which the account is affected by judgments).

The overall degree of change occurring in the company's business and its effect on the account or group of accounts also should be considered. Generally, a company undergoing significant changes (e.g., in rate of growth, markets, products, people, and technology) will have more uncertainties and greater risk than one with stability.

Identify and Evaluate the Major Classes of Transactions

The next area of focus is to identify and evaluate the major classes of transactions. The identification of major classes of transactions forms the link between the identification of significant accounts or groups of accounts and the understanding and evaluation of processes and related controls. Major classes of transactions include all classes of transactions that materially affect significant accounts or groups of accounts, either directly through entries in the general ledger or indirectly through the creation of rights or obligations that may not be recorded in the general ledger. Processes, whether business-oriented or accounting-oriented, generate or encompass classes of transactions that can be categorized as routine, non-routine, or estimation transactions. It is important to distinguish between the



various major classes of transactions because there are differences in the components and risks related to each class and, as a result, the likelihood of errors of importance arising from the related processes differs as well.

Routine Transactions

Routine transactions represent frequently recurring financial data recorded in the books and records or non-financial data used to manage the business.

For example, a manufacturing company may have the following processes resulting in routine transactions:

- Sales and accounts receivable
- Cash receipts
- Purchasing and accounts payable
- Cash disbursements
- Payroll
- Inventories and cost of sales

Some companies will have more than one process for similar transactions. For example, there may be separate processes for domestic and export sales, and payroll may be broken down between salaried employees and hourly paid employees.

Non-Routine Transactions

These are transactions applied only periodically, generally in conjunction with the preparation of financial statements. Any major class of transaction that does not easily fit the definition of a routine transaction or an estimation transaction may be viewed as a non-routine transaction. Typical non-routine transactions include:

- Calculating income tax expense
- Determining accruals for goods and services received but not yet invoiced
- Counting and pricing inventory
- Determining prepaid expenses

Estimation Transactions

These are transactions that reflect the numerous judgments, decisions, and choices made in preparing financial statements (e.g., estimating the allowance for excess or obsolete inventory, determining the allowance for loan losses, or estimating warranty reserves).

Estimation transactions are required either because the measurement of some amounts or the valuation of some accounts is uncertain, pending the outcome of future events, or because relevant data concerning events that have already occurred cannot be accumulated on a timely, cost-effective basis.

In distinguishing between the major classes of transactions, it is important to note that routine transactions generally are subject to a more formalized system of controls because of the objectivity of data and volume of information processed. Conversely, because estimation transactions and non-routine transactions often are more subjective (i.e., involving estimates) or are performed less often, controls over these transactions typically are less formal. Consequently, the risk of errors occurring may be greater.

Understand the Flow of Transactions

Once the project team has identified the major classes of transactions, a more detailed understanding of the significant processes is necessary to understand the flow of each major class of transactions. The objective of this step is to identify and develop an understanding of the records, documents, and basic processing procedures in use to identify where errors may occur. Most processes involve a series of tasks such as validating or editing input data, sorting and merging data, making calculations, updating transactions and master files, generating transactions, and summarizing and displaying or reporting data. The processing procedures of relevance for purposes of identifying where errors could occur are those activities required to initiate, record, process, and report the major classes of transactions. These include procedures for correcting and reprocessing previously rejected transactions and for correcting erroneous transactions through adjusting journal entries.

No matter what category of major class of transaction affects an account, one must understand the flow and the nature of information; consider the types of errors that could occur in the initiation, recording, processing, and reporting of the transactions; and consider the relevant internal control policies or procedures.

While the documentation of the understanding and evaluation will vary depending on the category of transaction (e.g., making use of flow charts to document processes resulting in routine transactions and memoranda to document processes resulting in estimation and non-routine transactions), the objectives of recording accounting data are consistent.

Financial Reporting Process

Finally, the project team needs to include in its understanding and evaluation the company's process for producing financial reports. The understanding of the company's significant processes and how they interrelate with the company's financial reporting process will provide the project team with a basis for what additional information is required to understand the financial reporting process. The financial reporting process typically includes:

- The procedures used to enter transaction totals into the general ledger.
- The procedures used to initiate, record, and process journal entries in the general ledger.
- Other procedures used to record recurring and nonrecurring adjustments to the financial statements, such as consolidating adjustments, report combinations, and reclassifications.
- The procedures for drafting financial statements and related footnote disclosures.
- The preparation of management's analysis of financial and operational performance of the business.

Other Control Considerations

Policies and procedures regarding authorization, safeguarding of assets, asset accountability, and segregation of duties are established by management to provide reasonable assurance that:

- Assets are acquired, safeguarded, and used, and that liabilities are incurred and discharged, in accordance with management's decisions.
- Financial information is accurately maintained in the books and records with respect to assets and liabilities resulting from such decisions.

These policies and procedures are integral to a system of internal control and relate primarily to management's control over the disposition of the company's assets and liabilities and only indirectly to controls over the processing of data, which are concerned with the accurate, timely, and complete recording of transactions. However, the absence of such controls may increase the risk of errors of importance in the financial information maintained in the company's books and records.

As these policies and procedures frequently take the form of controls, the absence of adequate policies and procedures over any of these areas may affect the project team's determination of the effectiveness of specific controls over processes.

- *Authorization*
  General and specific authorization and approval levels and procedures designed to ensure that transactions and activities are executed in accordance with management's intentions.
- *Safeguarding of assets*
  Restrictions, designed to prevent the loss of assets, on access to and use of assets and records, including physical access and indirect access through the preparation and processing of data that authorize, or otherwise facilitate, the use or disposition of assets.

- *Asset accountability*
  Procedures to compare recorded assets with actual assets and to effect appropriate actions when differences are identified. Such procedures help provide assurance that procedures relating to authorization and access to assets are being followed.
- *Segregation of duties*
  Prevention of any single individual from performing incompatible activities, or of an IT application set-up from granting users inappropriate or excessive access to functionality (e.g., if an individual is in a position to both perpetrate and conceal errors in the normal course of performing his or her duties).

Effects of Information Technology

In more complex automated applications, controls identified by management may often involve information technology (IT). IT controls include application controls and IT general controls. These controls help ensure that transactions are valid, properly authorized, and completely and accurately processed.

Application Controls

Application controls apply to the processing of individual transactions and may consist of programmed procedures (e.g., the specific programs to process or edit a transaction) or non-programmed controls (e.g., manual balancing of IT-produced information). Programmed controls, which are either programmed control procedures (e.g., edit, matching, or reconciliation routines) or IT processes (e.g., calculations, on-line entries, or automatic interfaces between systems), often exist and are relied on by management to ensure the accuracy and completeness of data generated by automated applications. For example, to ensure all invoices to customers are correctly priced, management may rely on an automated edit routine to identify pricing transactions that do not meet established criteria combined with access control software to restrict access to the price master file. Similarly, management may rely on an IT process such as the automated extension of sales invoices to ensure that all sales are properly valued.

Programmed controls may be found at various stages of the data processing:

- *Input*
  Controls will exist to ensure the validity and completeness of the data input (e.g., summarization of transactions generated in branch offices). There may be numerous validations performed to prevent the input of erroneous data.
- *Processing*
  Controls also will exist to provide correct valuation and posting. Processes may perform either simple or complex calculations (e.g., product pricing, option valuations). The administration of processing instructions and parameters is also a key control issue.
- *Output*
  Special controls may be in place when output generates payments (e.g., validation of supplier identification number prior to processing of payment).

A programmed control by itself may not be sufficient to ensure the application is preventing errors from occurring during processing or to detect and correct errors that may have occurred during processing. However, a programmed control, in combination with effective IT general controls may provide the desired level of control.

IT General Controls

IT general controls relate to underlying controls over application and system software acquisition and maintenance, access security, and segregation of duties that are in place to make sure programmed controls continue to be effective. Typically, IT general controls are designed to:

- Ensure that all changes to applications are properly authorized, tested, and approved before they are implemented
- Ensure that only authorized persons and applications have access to data, and then only to perform specifically designed functions (e.g., inquire, execute, or update)

If, in consideration of "what could go wrong" questions, the project team determines that management is relying on programmed controls or that the control identified is dependent on IT-generated data, then a second question must be asked: "How does management know that programmed controls are operating effectively?" The response may be that (1) user procedures verify the accuracy of the processing (e.g., manually recomputing complex calculations, or reconciling IT reports to manual batch totals) and/or (2) management depends on the IT system to effectively execute the control or produce the data. When (2) is the response, the effect of IT general controls (i.e., program changes and/or access to data files, including the general controls within integrated application environments such as key settings and segregation of duties among users that affect the whole application) should be considered in making the preliminary evaluation of the effectiveness of all controls that depend on the IT system or IT-generated data.

Many companies use outside service organizations to process transactions. In such situations, in addition to evaluating controls within the company, management must develop an understanding of the significance of the service organization's processing to the company's accounting system and controls. Based on the degree of significance, management may need to make an assessment of the controls in place at the service organization. Often, the service organization's auditor will have prepared a report on these controls that will be useful to management in assessing these controls.

The underlying concerns with respect to controls are the same whether transactions are processed internally or by an outside service organization.

Methodology for Evaluating Internal Controls

Understand the Definition of Internal Control

Organize a Project Team to Conduct the Evaluation

Evaluate Internal Control at the Entity Level

Understand and Evaluate Internal Control at the Process, Transaction, or Application Level

Evaluate Overall Effectiveness, Identify Matters for Improvement, and Establish Monitoring System

- Determine Whether Controls as Designed are Effective
- Assess Whether Controls are Functioning as Designed
- Identify Matters for Improvement
- Establish Monitoring System

5 Evaluating Overall Effectiveness of Controls, Identifying Matters for Improvement, and Ongoing Monitoring

Establishing and maintaining effective internal controls is an important management responsibility. To provide reasonable assurance that an entity's objectives will be achieved, the system of internal control should be under ongoing supervision by management to determine that it is operating as intended and that it is modified as appropriate for changes in conditions.

The COSO report indicates that an internal control system, no matter how well conceived and operated, can provide only reasonable—not absolute—assurance to management and the board of directors and audit committee regarding achievement of an entity's objectives. The report further indicates that the likelihood of achievement of these objectives is affected by limitations inherent in all internal control systems. It then states that one of these limiting factors is that the design of an internal control system must reflect the fact that there are resource constraints, and that the benefits of controls must be considered relative to their costs.

Evaluating Overall Effectiveness

The final step in evaluating internal controls over financial reporting is to make an overall assessment of the design and operation of controls based on the results of the detailed evaluations performed at the process level.

Determining Whether Controls as Designed Are Effective

The determination of whether controls as designed are effective should be completed by a reviewer in a supervisory capacity (e.g., the division controller or the subsidiary's treasurer) or a member of the project team. In making this assessment, the reviewer should consider:

- Account characteristics of related accounts (such as size, susceptibility to error or manipulation)
- The effectiveness of internal control at the entity level
- Conclusions related to the Information Technology processes
- The design of the control itself
- The sensitivity of the control
- Policies and procedures regarding authorization, the safeguarding of assets, asset accountability, and segregation of duties

Determining whether the controls achieve a given objective (e.g., with respect to financial reporting objectives, that errors of importance do not occur) often requires considerable judgment. The key question is whether the essential controls would be likely to prevent and/or detect a material error relating to each of the relevant financial statement assertions.

If the controls in place are not effective in preventing and/or detecting material errors relating to each of the relevant financial statement assertions (or controls are absent), additional or different manual or programmed controls may be necessary. Before installing new procedures, the company should make a cost-benefit decision (see following section) to determine whether the cost would exceed the benefits.

Assessing Whether Controls Are Functioning as Designed

Management should have reasonable assurance that the procedures are functioning as designed. An initial step in this process will often involve the reviewer performing a walk-through of a transaction to determine that the reviewer's understanding as to the intended functioning of the process and related controls is correct. Once this walk-through has been completed, testing the effectiveness of the controls can begin.

Testing to determine whether controls are functioning as designed may be accomplished by the reviewer making inquiries of the individuals responsible for the control and examining evidence (e.g., reviewing bank reconciliations) that the control was performed and was effective, or by the reviewer retracing a transaction and/or reperforming controls (e.g., recalculating extensions on a sample of invoices). In other instances, assurance that controls are functioning as intended may be gained by observing employees as they perform their work and through interviews to determine how employees understand what is required in the event an error is identified in the performance of their duties.

In cases where transactions are processed by the IT system, in addition to following the physical flow of documents and forms, the reviewer also follows the flow of data and file information through the automated process in the application (at a system level, not a detailed logic level). This may involve procedures such as inquiry of independent and knowledgeable personnel, review of user manuals, observation of a user processing transactions at a terminal in the case of an on-line application, and review of documentation such as output reports.

At the conclusion of this task, the reviewer should document whether the manual and programmed controls are functioning as designed and include any other pertinent comments that might assist the project team.

Identifying Matters for Improvement

In a dynamic business environment, controls will require modification from time to time. Certain systems may require control enhancements to respond to new products or emerging risks. Automating certain manual controls may improve both efficiency and compliance with management's policies. In other areas, the evaluation may point out redundant controls or other procedures that are no longer necessary. In such situations the company may be able to maintain an acceptable level of controls and improve its results by making the appropriate changes.

In the event that areas are identified where controls are not sufficient to provide reasonable assurance that the risk of errors occurring is reduced to a sufficiently low level, the project team should suggest improvements. All suggestions for enhancements should consider the concept of reasonable assurance.

Both auditing literature and the COSO report strongly imply that internal control need not be free of risk where the cost of eliminating a risk would exceed the benefits expected to be gained. Accordingly, when a reviewer or the project team identifies a risk, a cost-benefit decision should be made as to whether the costs to install and maintain a control that will reduce or eliminate the risk would exceed the expected benefits. Usually, controls can only reduce, not entirely eliminate, a risk. Further, cost-benefit analyses can be used to determine whether existing controls should be retained.

There frequently is more than one course of action that will reduce a given risk; further, a company's controls in a particular area may be layered or overlapping. Accordingly, the best course of action in the circumstances should be determined; this may require considering the costs and benefits of more than one control.

Applying the Cost-Benefit Concept

The principle that failing to reduce a risk is justified when the costs would exceed the benefits is easier to state than to apply. In many instances, significant difficulties will be encountered in applying the cost-benefit rationale because identification and precise measurement of the costs and benefits will be impossible. The risk to be eliminated also can be difficult to quantify, the benefit to be gained could be the elimination of an unquantifiable risk, and the cost may include intangibles such as impaired employee morale or customer goodwill.

Therefore, virtually any cost-benefit decision made to determine whether to implement a control would be highly dependent on judgments. Accordingly, if a cost-benefit analysis leaves doubt as to whether the cost of the control is greater than the benefit, it will usually be prudent to implement or retain the control.

Moreover, there are situations that are so clearly unacceptable that they must be modified at almost any cost, and hence the cost-benefit question is virtually academic. For example, if a material weakness exists, the controls necessary to correct the condition should be implemented regardless of cost. Auditing literature defines a material weakness as a condition in which:

> "… the design or operation of one or more of the internal control components does not reduce to a relatively low level the risk that misstatements caused by error or fraud in amounts that would be material in relation to the financial statements being audited may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions."

Conditions indicating the existence of a material weakness include:

- The company does not have reasonable assurance that its internal control will permit the preparation of annual financial statements in conformity with generally accepted accounting principles (GAAP)
- The company's independent auditors cannot, as a practical matter, complete an audit
- The company issues interim financial statements to third parties but does not have reasonable assurance (recognizing the relatively greater imprecision in interim statements) that its internal controls will permit the preparation of interim financial statements in conformity with GAAP
- The company does not have reasonable assurance that all material amounts of assets will be adequately safeguarded (i.e., access to assets is appropriate)

All aspects of internal control are subject to cost-benefit judgments, including:

- Routine procedures (e.g., matching invoices and receiving reports)
- Periodic monitoring (e.g., tests of controls, studies of portions of the system, and reexaminations of prior cost-benefit studies). This includes decisions as to the types of monitoring (e.g., by internal auditors) and the frequency of monitoring (e.g., quarterly, annually)
- Documentation of:
  - —Transactions
  - —The control system
  - —Monitoring activities
  - —Cost-benefit decisions
- Policies and practices for internal reporting of:
  - —Malfunctioning or circumvented controls
  - —Changes in circumstances that either create new or additional risks or reduce or eliminate existing risks
- Policies and practices for taking timely, corrective actions.

In many (perhaps most) cases, a formal cost-benefit analysis will be impracticable or unnecessary. For example, those performing the analysis may recognize after the first or second step that the costs will far exceed any benefits. On the other hand, those performing the

analysis might conclude that the costs of reducing the risk will be minimal, so, as a practical matter, the control might as well be installed.

However, for those situations where a formal cost-benefit analysis makes sense, considering factors in the following sequence may be useful:

1. List all reasonable alternatives (including controls) that might be adopted to reduce or eliminate the risks and—if they have not already been identified—all the risks that would be reduced or eliminated by each alternative.
2. Identify (list) all the relevant items of cost that would be incurred for each alternative control.
3. Determine the costs and risks that are quantifiable.
4. Quantify those costs and risks.
5. Estimate the probability that a loss could occur if the weakness is not corrected, and how frequently it could occur (if applicable).
6. Estimate, for each alternative, the probability (if any) that a loss could occur if the control is installed, and how frequently it could occur (if applicable).
7. Develop a "best estimate" of the benefits of eliminating or reducing the risk (e.g., by multiplying for each alternative the quantifiable risks by the reduction in the probability a loss could occur and then by the reduction in the frequency of occurrence).
8. Decide whether the costs of correcting the weakness would likely exceed the benefits, or vice versa, based on a comparison of the costs (quantifiable and unquantifiable) and the benefits (quantifiable and unquantifiable).

Monitoring

Finally, as mentioned earlier, internal control should be self-monitoring and self-correcting. This means a company should establish mechanisms to continually monitor and maintain the system of internal control and take corrective action in a timely manner, when necessary.

Generally, one group should not be assigned exclusive responsibility for making the system of internal control self-monitoring and self-correcting. The system of internal control is, in its broadest sense, comprehensive. It involves people throughout the organization, including many who may not think of themselves as having any accounting or control responsibilities.

Many people must share the responsibility for ensuring that the system of internal control is self-monitoring and self-correcting. These people should include those who establish, issue, and monitor accounting policies and procedures: divisional controllers, internal auditors, the corporate controller, the chief financial officer, other members of senior management, audit committee members, and members of the board of directors. They all need to be concerned, with varying degrees of detail, that the system of internal control is kept "under control." To help ensure this, appropriate lines of communication and adequate feedback are needed, both when the system of internal control is under control and when problems arise.

The project team should not consider its task completed until either:

- It is satisfied that appropriate self-monitoring and self-correcting mechanisms are in place, or
- It has made reasonably specific recommendations for establishing such mechanisms.

If such recommendations are necessary, they might encompass such matters as:

- Establishing the responsibility for issuing policies and procedures to one or more existing or new groups
- Establishing an internal audit activity
- Reporting monitoring activities to appropriate levels of management
- Actions to be taken when employees do not follow established controls
- The ongoing involvement of the board or audit committee

Once all the key recommendations have been implemented, a baseline will have been established for annual updates of management assessments to enable management to report on the effectiveness of controls. This does not mean that evaluations will cease. On the contrary, it means that evaluations will have become a part of the company's ongoing, repetitive processes and thus an important part of the company's internal control. After implementation, the company can expect that any weaknesses—and some will inevitably arise—will be corrected within a reasonable period of time.

ERNST & YOUNG LLP www.ey.com

© 2002 Ernst & Young LLP.
All Rights Reserved.
Ernst & Young is
a registered trademark.

SCORE Retrieval File
No. EE0677