2004

Internal control reporting : implementing Sarbanes-Oxley Act section 404; Financial reporting alerts

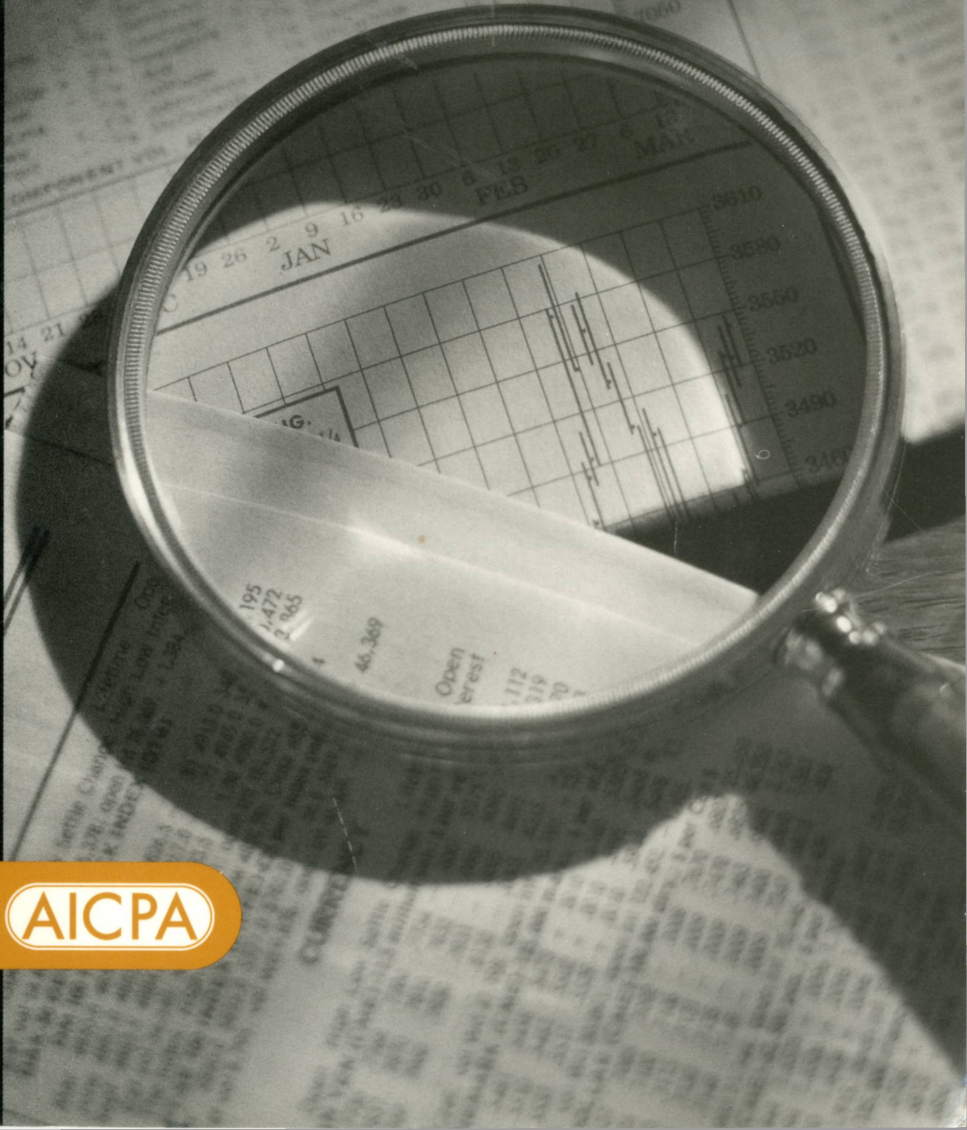
Michael J. Ramos

Robert Durak

FINANCIAL REPORTING ALERTS

Internal Control Reporting

Implementing Sarbanes-Oxley Act Section 404



AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS

AICPA

FINANCIAL REPORTING ALERTS

Internal Control Reporting

Implementing Sarbanes-Oxley Act Section 404

AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS

AICPA

Notice to Readers

This Financial Reporting Alert was developed by an independent consultant and the staff of the American Institute of Certified Public Accountants (AICPA). Its content represents the opinions of the author. This Financial Reporting Alert has not been approved, disapproved, or otherwise acted upon by any senior technical committee of the AICPA and has no official or authoritative status.

Written by
Michael J. Ramos, CPA

Edited by
Robert Durak, CPA
Senior Manager
Accounting and Auditing Publications

1 2 3 4 5 6 7 8 9 0 AAG 0 9 8 7 6 5 4

Table of Contents

Internal Control Reporting—Implementing Sarbanes-Oxley Act Section 404

Introduction

In July 2002, the Sarbanes-Oxley Act of 2002 (the "Act") was signed into law, bringing with it sweeping changes to many aspects of the financial reporting, corporate governance, and regulatory landscape for public companies. Section 404 of the Act requires public companies to include with their annual report to the Securities and Exchange Commission (SEC) a separate report on the assessment of the effectiveness of the entity's internal control. Additionally, the entity's external auditors must attest to and report on the assessment made by management. These reporting requirements generally become effective for the end of the entity's first fiscal year ending on or after June 15, 2004.

Since the passage of the Act, many issues have arisen regarding the implementation of the internal control assessment and reporting process. The purpose of this Alert is to articulate significant technical issues that have surfaced and to provide direction for those responsible for managing or participating in the implementation of section 404, including:

- The entity's CEO and CFO, who have the overall responsibility for assessing and reporting on internal control
- Internal auditors
- Third parties who might be engaged by the entity to assist with the assessment process

Summary of Relevant Rules and Other Authoritative Literature

Management's assessment and reporting on internal control will be shaped by several key rules and standards, including:

- *SEC rules*. The Sarbanes-Oxley Act directed the SEC to adopt detailed rules to implement the requirements of the Act relating to internal control. These rules define for issuers the requirements for assessing and reporting on internal control. To read the SEC rules, go to the SEC Web site at www.sec.gov/rules/final/33-8238.htm.
- *External auditor standards*. These standards describe the approach, required tests, and other guidance that the entity's external auditors are expected to follow when reporting on management's assertion about the effectiveness of internal control. These standards do not affect the issuer directly, but they do have a significant *indirect* effect on the procedures performed by management.
- *The COSO Internal Control Integrated Framework.* Management's report on internal control effectiveness is required to disclose the criteria against which management assesses effectiveness. The COSO framework is one example set of criteria and it is anticipated that most U.S. entities will use COSO in their evaluation. To obtain the COSO framework, call the AICPA at (888) 777-7077 or visit www.cpa2biz.com and order *Internal Control—Integrated Framework* (product no. 990012kk).

The SEC Rules

The SEC issued its final rule on management's report on internal control in May 2003, and the rule became effective on August 14, 2003. It is the entity's annual report to the SEC (Form 10-K) which contains management's report on internal control, and therefore, it is the SEC rules regarding those reports that management must follow in planning and performing its assessment of control effectiveness.

Definition of Internal Control

The SEC rules clarify that management's assessment and report is limited to *internal control over financial reporting*. Management is not required to consider other aspects of control, such as controls pertaining to operating efficiency. The SEC's definition of internal control encompasses the COSO definition (described later in this Alert in the section entitled "The COSO Internal Control Integrated Framework") but the SEC does not mandate that the entity use COSO as its criteria for judging effectiveness.

Annual Reporting Requirements

Under the SEC rules, the company's annual 10-K must include:

1. *Management's Annual Report on Internal Control Over Financial Reporting.* This report on the company's internal control over financial reporting should contain:
   a. A statement of management's responsibilities for establishing and maintaining adequate internal control over financial reporting.
   b. A statement identifying the framework used by management to evaluate the effectiveness of the company's internal control over financial reporting.
   c. Management's assessment of the effectiveness of the company's internal control over financial reporting as of the end of the most recent fiscal year, including a statement as to whether or not internal control over financial reporting is effective. This discussion must include disclosure of any material weakness in the company's internal control over financial reporting identified by management. Management is not permitted to conclude that the registrant's internal control over financial reporting is effective if there are one or more material weaknesses in the company's internal control over financial reporting.
   d. A statement that the registered public accounting firm that audited the financial statements included in the annual report has issued an attestation report on management's assessment of the registrant's internal control over financial reporting.

2. *Attestation Report of the Registered Public Accounting Firm.* This is the registered public accounting firm's attestation report on management's assessment of the company's internal control over financial reporting.

3. *Changes in Internal Control Over Financial Reporting.* This report must disclose any change in the company's internal control over financial reporting that has materially affected or is reasonably likely to materially affect the company's internal control over financial reporting.

Key provisions of these reporting requirements that merit management's consideration include the following.

- *"As of" reporting.* Management assesses the effectiveness of internal control *as of* the end of the fiscal year, rather than throughout the reporting period. This reporting requirement has significant implications for the reporting of material weaknesses that were identified and corrected during the period. It also will affect the timing of management's tests of the design and operating effectiveness of controls.
- *Material weakness in internal control.* Management is required to disclose any material weakness[1] in the company's internal control. Further, the existence of one or more material weaknesses precludes management from concluding that its internal control is effective.

Both of these considerations are discussed in more detail in the section titled "Reporting" in this Alert.

Quarterly Reporting Requirements

The SEC rules also require management to evaluate any change in the entity's internal control that occurred during a fiscal quarter and that has materially affected, or is reasonably likely to materially affect, the entity's internal control over financial reporting.

Additionally, management is required to evaluate the effectiveness of the entity's "disclosure controls and procedures" and issue a report as to their effectiveness on a quarterly basis. With these rules, the SEC introduced a new term, "disclosure controls and procedures," which is different from "internal controls over financial reporting" and much broader.

1. For a definition of material weakness, see the "Reporting" section of this Alert.

As defined, "disclosure controls and procedures" encompass the controls over all material financial *and nonfinancial information* in Exchange Act reports. Information that would fall under this definition that would *not* be part of an entity's internal control over financial reporting might include the signing of a significant contract, changes in a strategic relationship, management compensation, or legal proceedings.

This Alert will not discuss the evaluation of disclosure controls and procedures but will be limited to a discussion of the annual and quarterly evaluation and reporting of internal control over financial reporting.

The External Auditor's Standards

The entity's external auditors are required to audit management's internal control report in accordance with certain professional standards. These standards *directly* affect *only* the work of the external auditor. The work performed by the entity to assess the effectiveness of its internal controls need only comply with the requirements of the SEC rules. However, the auditing standards related to internal control reporting will have a *significant indirect* effect on the way in which management plans and performs its internal control testwork. For example, the standards may require the external auditors to include certain divisions, categories of controls, or control procedures within the scope of their work. If that is the case, then management would need to ensure that the scope of their assessment process is congruent with the requirements of external auditors.

The Current State of the Audit Standards Relating to Internal Control

At the time this Alert was prepared, the Public Company Accounting Oversight Board (PCAOB) had released a draft of a proposed auditing standard relating to the independent auditor's audit of management's report on internal controls. This proposed standard would provide the definitive guidance to auditors on the requirements for auditing management's report on internal control. The following overview is based on this *proposed* standard.

Expectations are that this standard will become final early in 2004. To more fully understand the independent auditor's requirements and how they affect management's assessment process, you should obtain and read the final standard once it becomes available. The current proposed standard is posted on the PCAOB Web site at www.pcaobus.org/rules/Release2003-017.pdf. Remember that the final standard issued by the PCAOB may differ significantly from the proposed standard.

Highlights of the Proposed Auditing Standard

The PCAOB's proposed auditing standard addresses several important areas that will affect financial statement issuers. A brief discussion of these follows.

The Audit Process. The overall objective of the external auditor's engagement is to form an opinion about management's assessment of the effectiveness of internal control. To form his or her opinion, the auditor will:

- Evaluate the reliability of the process used by management to assess the entity's internal control.
- Review and rely on the results of *some* of the tests performed by management, internal auditors, and others during their assessment process.
- Perform his or her own tests.

This framework of the auditor's process poses several important questions for management, including:

- What are the qualities of management's process for assessing internal control that the external auditors deem necessary to make the process "reliable"?
- Which of management's tests will the external auditor be able to rely on and which will be subject to retesting by the auditor?

Required Elements of Management's Process. The proposed standard provides guidance on the *required* elements of management's process for assessing the effectiveness of internal control. The absence of one or more of those required elements may result in a modification to the standard audit report. For this reason, it is critical that management's process comply with all requirements established by the new standard.

The proposed audit standard states that the auditor should determine whether management's assessment process has addressed the following elements.

- Determining which controls should be tested, including controls over relevant assertions related to all significant accounts and disclosures in the financial statements. Generally, such controls include:
  - Controls over initiating, recording, processing, and reporting significant accounts and disclosures and related assertions embodied in the financial statements.
  - Controls over the selection and application of accounting policies that are in conformity with generally accepted accounting principles.
  - Antifraud programs and controls.
  - Controls, including information technology general controls, on which other controls are dependent.
  - Controls over significant nonroutine and nonsystematic transactions, such as accounts involving judgments and estimates.
  - Controls over the period-end financial reporting process, including controls over procedures used to enter transaction totals into the general ledger; to initiate, record, and process journal entries in the general ledger; and to record recurring and nonrecurring adjustments to the financial statements (for example, consolidating adjustments, report combinations, and reclassifications).
- Evaluating the likelihood that failure of the control could result in a misstatement and the degree to which other controls, if effective, achieve the same control objectives.
- Determining the locations or business units to include in the evaluation for a company with multiple locations or business units.

- Evaluating the design effectiveness of controls.
- Evaluating the operating effectiveness of controls based on procedures sufficient to assess their operating effectiveness. To evaluate the effectiveness of the company's internal control over financial reporting, management must have evaluated controls over all relevant assertions related to all significant accounts and disclosures.
- Determining the deficiencies in internal control over financial reporting that are of such a magnitude and likelihood of occurrence that they constitute significant deficiencies or material weaknesses.
- Communicating findings to the auditor and to others, if applicable.
- Evaluating whether findings are reasonable and support management's assessment.

Documentation of Testwork to Support Management's Assertion. The proposed standard provides additional guidance on the nature and extent of the documentation required by the entity to support management's assessment of internal control. The proposed standard also states that inadequate documentation is a control deficiency that may rise to the level of a material weakness.

The proposed standard also addresses other situations that are likely to occur in practice, including:

- Extent of testing of multiple locations, business segments, or subsidiaries
- Required tests when the entity uses a service organization to process transactions
- Updated testwork required when the original testing was performed at an interim date in advance of the year-end reporting date

Using the Work of Internal Auditors and Others. Many entities are using the work of their own internal audit staff and others within the organization to perform tests of the effectiveness of internal control. At issue is the extent to which the external auditors can rely on those tests to reach their own conclusion.

The proposed auditing standard provides extensive guidance on the extent to which the independent auditors may rely on the work performed by management (including work performed by internal auditors and others) in their internal control audit. The standard defines three categories of controls and the extent to which the independent auditor may rely on the work of others to reach a conclusion.

- *No reliance.* For some areas the auditor is prohibited from using the results of management's tests. These areas include:
  - Controls that are part of the control environment
  - Controls over the period-end financial reporting process
  - Controls that have a pervasive effect on the financial statements

  That the independent auditors can not rely on the results of management's tests in these areas does not relieve management of its responsibilities to perform these tests. That is, tests directed toward these control areas will be performed twice, once by management and again by the independent auditors.

- *Limited reliance.* The auditor's use of the results of procedures performed by management should be limited to the following areas:
  - Controls over significant nonroutine and nonsystematic transactions
  - Controls over significant accounts, processes, or disclosures where the auditor has assessed the risk of failure of the controls to operate effectively as high

- *Full reliance.* Auditors are allowed to use the results of management's tests in all other areas, such as controls over routine processing of significant accounts and disclosures.

The COSO Internal Control Integrated Framework

In 1985, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) was formed to sponsor the National Commission on Fraudulent Financial Reporting, whose charge was to study and report on the factors that can lead to fraudulent financial reporting. Since this initial undertaking, COSO has expanded its mission to improving the quality of financial reporting. A significant part of this mission is aimed at developing guidance on internal control. In 1992, COSO published *Internal Control—Integrated Framework*, which established a framework for internal control and provided evaluation tools that business and other entities could use to evaluate their control systems.[2] This COSO report can be obtained through the AICPA by calling (888) 777-7077 or by going online at www.cpa2biz.com. The product number is 990012kk.

The COSO Internal Control Components

The COSO framework describes five interrelated components of internal control.

- *Control environment.* Senior management must set an appropriate "tone at the top" that positively influences the control consciousness of entity personnel. The control environment is the foundation for all other components of internal controls and provides discipline and structure.
- *Risk assessment.* The entity must be aware of and deal with the risks it faces. It must set objectives, integrated through-

2. In 2003, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) published a draft of a document entitled *Enterprise Risk Management Framework*, whose purpose was to provide guidance on the process used by management to identify and manage risk across the enterprise. This new framework does not supersede or otherwise amend its earlier internal control framework. Internal control is encompassed within and an integral part of enterprise risk management. Enterprise risk management is broader than internal control, expanding and elaborating on internal control to form a more robust conceptualization focusing more fully on risk. *Internal Control—Integrated Framework* remains in place for entities and others looking at internal control by itself.

out all value chain activities, so that the organization is operating in concert. Once these objectives are set, the entity must then identify the risks to achieving those objectives, analyze them, and develop ways to manage them.

- *Control activities.* Control policies and procedures must be established and executed to help ensure the actions identified by management as necessary to address risks are effectively carried out.

- *Information and communications.* Surrounding the control activities are information and communication systems, including the accounting system. These systems enable the entity's people to capture and exchange the information needed to conduct, manage, and control its operations.

- *Monitoring*. The entire control process must be monitored, and modifications made as necessary. In this way, the system can react dynamically, changing as conditions warrant.

The COSO report describes these individual components as being tightly integrated with each other. Each component has a relationship with and can influence the functioning of every other component. When evaluating the effectiveness of internal control, management should consider it as an integrated whole. Weak controls in one area can be offset by stronger controls in another area.

Key Characteristics of the COSO Framework

Flexible, Adaptable, No "One Size Fits All" Approach

The COSO framework is not a rigid, prescriptive approach to internal controls. It recognizes that different entities will make different choices about how to control their businesses. Internal control is not a "one size fits all" proposition. Consequently, internal control can not be evaluated against a detailed set of fixed, required procedures. Management will have to exercise a great deal of judgment, driven by the particular needs of the entity, to determine the nature of the controls in place and whether they are functioning effectively.

Effectiveness Determined by Achievement of Objectives

Management should judge the effectiveness of internal control by how well the controls enable the entity to achieve stated objectives. Controls have value only to the degree to which they allow the entity to achieve its objectives. Thus, the COSO framework adopts a business objectives-driven approach to defining internal control. Under that approach, the entity:

1. Establishes business objectives. The SEC rules describe those objectives as relating to the preparation of reliable financial statements.
2. Identifies the risks to achieving those objectives.
3. Determines how to manage the identified risks. The establishment of internal controls is just one of several options.
4. Where appropriate, establishes control objectives as a way to manage certain risks. Individual controls are then designed and implemented to meet the stated control objectives.

Significant Control Objectives

The COSO framework focuses on the achievement of control *objectives* (rather than the existence of predetermined control procedures), and it is expected that management will rely on some control procedures more than others to achieve these objectives. For example, management may decide to rely more on detective controls rather than preventive controls to identify and correct unauthorized transactions. At the entity level, some control objectives or activity-level processing streams may be more significant to the entity's financial statements or financial reporting process than others.

When assessing the effectiveness of internal control *as a whole*, management should be sure to identify the controls it relies on most to produce reliable financial statements, and to include the testing of these controls in the scope of its work.

The Importance of the Control Environment

Managers typically think of internal control only in terms of the policies and procedures related to the processing of transactions.

For example, the matching of a vendor invoice to a master file of approved vendors, the recalculation of that invoice, or the reconciliation of the accounts payable subsidiary ledger to the general ledger account are all examples of controls over the processing of purchases.

The COSO framework does not limit itself to these types of business activity-level procedures. The framework acknowledges that the *environment* in which those procedures operate has a direct effect on their effectiveness. In fact, this environment is described as the foundation of all other control components. The control environment encompasses the following:

- Integrity and ethical values
- Commitment to competence
- Board of directors or audit committee
- Management's philosophy and operating style
- Organizational structure
- Assignment of authority and responsibility
- Human resource policies and practices

When evaluating the effectiveness of internal control, management must be sure to perform tests that allow it to assess the effectiveness of the control environment. The section of this Alert titled "Testing of Internal Control" discusses this matter in more detail.

Antifraud Programs and Controls. Management is responsible for designing and implementing systems and procedures for the prevention and detection of fraud and, along with the board of directors, for ensuring a culture and environment that promotes honesty and ethical behavior. Broadly stated, three fundamental elements are essential when implementing a system to prevent, deter, and detect fraud. They are: (1) create and maintain a culture of honesty and high ethics; (2) evaluate the risks of fraud and implement the processes, procedures, and controls needed to mitigate the risks and reduce the opportunities for fraud; and (3) develop an appropriate oversight process. The AICPA

Antifraud & Corporate Responsibility Resource Center provides extensive guidance for developing antifraud programs and controls.

Reasonable Assurance

No matter how well designed or operated, internal control can provide only reasonable assurance that objectives will be met. Reasonable assurance is a high threshold, but it stops short of absolute assurance. The presence of an internal control failure does not, in and of itself, mean that a system is ineffective. The COSO report states that "even an effective internal control system can experience failure."

Information Technology Considerations

The COSO framework groups information technology (IT)-related controls into two types: general computer controls and application-specific controls.

- *General controls* include controls over:
  - Data center operations (for example, job scheduling, backup, and recovery procedures)
  - Systems software controls (for example, the acquisition and implementation of operating systems)
  - Access security
  - Application system development and maintenance controls (for example, the acquisition and implementation of individual computer software applications)
- *Application controls* are designed to control information processing and help ensure the completeness and accuracy of transaction processing, authorization, and validity. Application controls also encompass the way in which different applications interface with each other and exchange data.

The COSO report does not mandate this approach to assessing the effectiveness of internal controls but states that this is one set of groupings of IT-related control activities that can be used.

Many entities will find the COSO guidance on IT-related controls to be insubstantial and may look for additional guidance.

The Control Objectives for Information and Related Technology (COBIT) framework is a good source for such guidance.

The COBIT Framework

Since the release of COSO, the Information Systems Audit and Control Association and Foundation (ISACA) has developed its COBIT framework, which provides a generally applicable and accepted standard for IT security and control practices. Among IT audit professionals, COBIT is widely accepted.

The COBIT framework is similar to COSO in that it puts controls within the context of an entity's need to achieve certain business objectives and the risks it faces toward achievement. In defining the goals of IT governance and control, COBIT takes a rather broad brush and does not limit itself to the financial reporting process. For the purpose of complying with the SEC internal control reporting requirements, management should limit its consideration of IT controls to those that affect the reliability of financial reporting, either directly (for example, application controls) or indirectly (for example, general controls).

COBIT groups the IT processes into four categories, each of which is critical in delivering information that meets certain stated criteria.

- *Planning and organization.* These processes cover strategy and tactics and concern the identification of the way IT can best contribute to the achievement of stated business objectives, both now and in the future.
- *Acquisition and implementation*. To realize the IT strategy, IT solutions need to be identified, developed, or acquired, as well as implemented and integrated into business processes.
- *Delivery and support*. These processes include the actual processing of data by application systems.
- *Monitoring*. All IT processes need to be regularly assessed over time for their quality and compliance with control requirements.

The delivery and support category of processes is analogous to the COSO category of application controls. The other categories identified by COBIT approximate the general controls described by COSO but are somewhat broader in scope.

AICPA Trust Services, Including SysTrust℠ and WebTrust℠

SysTrust and WebTrust are professional services that address areas such as security, privacy, processing integrity, availability, and confidentiality through the use of the AICPA/CICA Trust Services Principles and Criteria. Management can benefit from using these suitable criteria in several ways when implementing Sarbanes-Oxley section 404 requirements. They can use the AICPA/CICA Trust Services Principles and Criteria as:

1. A guideline to setting up appropriate controls and systems that will instill confidence and trust.
2. A method of evaluating a system to determine whether it meets specific criteria and employs best practices.
3. An internal method of assurance and self-assessment that management, the board, and others can rely upon.

For more information about Trust Services, visit AICPA Online at www.aicpa.org/trustservices.

Project Planning Considerations

In order to reach a reliable conclusion about the effectiveness of the entity's internal control, management will need to plan a logical, structured approach to its testing and evaluation, for example:

1. Ensure adequate documentation of existing controls. If controls are found to be missing or to contain design deficiencies, then new or redesigned controls need to be documented and implemented.
2. Perform tests of the design and operating effectiveness of all significant controls.
3. Evaluate the test results and form a conclusion about the effectiveness of internal control. If the tests reveal signifi-

cant deficiencies or material weaknesses in internal control, then corrective action should be taken immediately.

4. Prepare management's report on internal control.

General Planning Considerations

During the course of the project to assess internal control effectiveness, management will be required to make important judgments regarding:

- The focus of testing and areas of risk requiring increased scrutiny
- The nature of the testwork and other procedures necessary to achieve the project's objectives
- The scope of the work to be performed, for example, the locations or business units to be included in testing

Planning involves gathering information to help make broad, preliminary judgments on these matters. The knowledge gained from gathering this information also provides the requisite knowledge to make informed decisions as the engagement proceeds. In that sense, planning is an ongoing process. Preliminary judgments made at the onset of the project are revisited continuously as the project progresses and more information becomes available.

Information Sources

Sources of information that are useful for planning an assessment of internal control include the following:

- Published sources such as:
  - Form 10K and other SEC filings
  - Annual report
  - Information available in the Investor Relations section of the entity's Web site
  - Analyst reports
- Inquiries of key individuals with knowledge of the entity's most significant business process and financial reporting processes and how these processes are monitored and controlled.

Areas of Focus

The tests of control effectiveness should be focused on the entity's most significant control objectives. Determining these control objectives is largely a matter of judgment that requires management to consider the most significant risks of producing reliable financial statements and the controls that mitigate these risks. Factors that management should consider include the following:

- The entity's most significant business process activities
- Significant risks facing the entity and the industry
- Significant accounts, classes of transactions, and disclosures in the entity's financial statements
- Areas that pose a high risk of material misstatement to the financial statements, including those that:
  - Have a known or suspected control weakness
  - Possess a high risk for material misstatement irrespective of any controls

Management Override of Controls

Assessing internal control effectiveness may necessitate addressing the key area of management override of controls, a characteristic of many fraudulent financial reporting schemes. The audit committee plays an important role in helping the board of directors fulfill its oversight responsibilities with respect to the entity's financial reporting process and the system of internal control. In exercising this oversight responsibility, the audit committee should consider the potential for management override of controls or other inappropriate influence over the financial reporting process.

Structuring the Project Team

Performing an assessment of internal control is a complex process. Management should assemble a project team that includes individuals with a wide variety of technical expertise, including the following:

- Financial reporting requirements and processes

- Operations management
- Auditing concepts, techniques, and tools
- Information technology
- Securities law and SEC reporting requirements

Members of the project team should have sufficient authority and stature within the organization to allow them access to information and resources. The team should report directly to the CEO and CFO, who ultimately bear the responsibility for establishing and maintaining internal control and reporting on its effectiveness.

Engaging Third Parties for Assistance

Entities that lack sufficient resources or expertise may look to third parties for assistance. Completely outsourcing the entire project to a third party normally would be inappropriate for management to do—ultimately, management should remain responsible for evaluating and reporting on the effectiveness of the entity's internal control. However, third parties may be engaged to participate as part of the project team or to provide other services such as training.

When engaging third parties for help on the project, management should clarify with the third party:

- *Qualifications*. This includes the nature of their expertise and their experience in performing the work you will ask of them.
- *Scope of work.* Management should be sure to define, as unambiguously as possible, the scope of the third party's work. For example, if the entity engages a third party to assist "in the documentation of internal control," what does that entail? Is that limited to the preparation of documentation for controls already in existence? What if, during this process, management discovers that some necessary controls do not exist or the ones that do are inadequately designed? Is the design or re-design of controls within the original scope of work?

- *Work product*. The work performed by a third party may result in evidence used by management to support its assessment of internal control effectiveness. As such, the external auditors also may rely on some or all of the work to reach their conclusion about management's assertion. When engaging third parties, management should obtain a clear understanding about the form and content of the work product to ensure that it is suitable for their purposes and, if necessary, acceptable for use by the external auditors.

Working With the External Auditors

Management's relationship with its external auditor will play a role in determining effectiveness, efficiency, and cost of the project. Particularly in the first year of implementation, the entity's efforts to assess internal control effectiveness should be closely coordinated with the needs of the external auditor. A lack of coordination with the auditors could result in a variety of negative, unforeseen consequences, including:

- Duplication of effort
- Reperformance of certain tests
- Performance of additional tests or unanticipated expansion of the scope of the engagement
- Misunderstandings relating to the definition or reporting of material weaknesses

Issues to Consider With the External Auditors

The communication between management and the external auditors should take place early and continue throughout the project. Many issues will arise during the course of the project. For some of these issues, the input of the external auditors will be important if management is to reach a suitable resolution. Issues that management should consider discussing with its external auditors include the following.

Project Planning

- The overall process and approach management will take to evaluate internal control effectiveness
- The scope of the project
- The degree to which the external auditors will rely on the results of management's test work to reach their conclusion
- The list of controls determined to be significant and, therefore, the primary focus of the project
- The use of service centers and reliance on service center reports

Documentation

- Documentation of internal control policies and procedures, including the form of the documentation and what the documentation will contain
- The nature and extent of the documentation of tests of controls
- How to determine whether documentation of controls and tests of controls is sufficient

Tests of Internal Control

- The nature and extent of the planned tests of controls and whether the evidence expected to be obtained in those tests is sufficient to allow management to draw a reliable conclusion about the design and operating effectiveness of internal control
- The general type of deviations or conditions that might be considered significant deficiencies[3] or material weaknesses[4] and therefore should be considered when designing tests of controls

3. See definitions of "significant deficiencies" and "material weaknesses" in the "Reporting" section of this Alert.

4. See footnote 3.

- The planned timing of management's tests of controls and whether this timing will allow management to draw conclusions about the design and operating effectiveness of internal control "as of" year end
- The nature and extent of procedures that may be required to update management's conclusions about effectiveness from the time the procedures were performed until year-end
- The results of management's tests of controls and the conclusions reached regarding the effectiveness of internal control

Reporting

- Contents of management's report on internal control, including:
  - Completeness of the report and whether the contents satisfy the SEC reporting requirements
  - Possible deletion of material that is not required
- Disclosure of material weaknesses that exist at the reporting date
- The nonreporting of material weaknesses that existed and were reported at an interim period but subsequently have been remediated

Auditor Independence

To perform an audit of an entity's financial statements, the external auditor must be independent of the entity. The SEC has developed a detailed body of rules that define auditor independence. Underlying these detailed rules are fundamental concepts of independence including:

- Auditors should not act in the capacity of management
- Auditors should not audit their own work

At the time this Alert was prepared, there was considerable debate regarding the extent to which an entity's external auditors could become involved in management's assessment of the effectiveness of internal control without violating the SEC's independence rules or their underlying concepts.

Until these issues of auditor independence become more settled, the audit committee should proceed carefully when engaging the entity's external auditors to assist in management's internal control assessment process. The nature of the relationship and scope of work should be defined in a way that the auditor's independence both in appearance and in fact remains uncompromised. The audit committee or board of directors should be involved in all discussions and have the final authority for determining whether and how the external auditors will be engaged to assist in any internal control related matters. The consequences of violating the SEC's auditor independence rules may be severe, and in some cases, the SEC may even require the entity to have its financial statements re-audited.

Documentation of Internal Control and Tests of Controls

Within the context of assessing internal control to comply with the SEC reporting requirements, there are two separate sets of documentation:

- Documentation of the entity's internal control policies and procedures
- Documentation of management's tests to support its conclusion about the design and operating effectiveness of those controls

Documentation of Internal Control Policies and Procedures

The adequate documentation of internal control is important for the following reasons.

- *To improve reliability of internal control.* The documentation of an entity's internal control policies and procedures improves the effectiveness and reliability of the system. Without adequate documentation, the performance of the system depends exclusively on the skills and competence of the individual responsible for performing the procedure. As such, performance can vary greatly between individuals or over time. Adequate documentation reduces this variability by facilitating the consistent dissemination of critical information. Additionally, by clearly stating the parameters within which control procedures should be performed, it becomes easier to identify deviations from the policy or procedure—that is, material weaknesses can be identified.

- *To enable effective monitoring*. Management is required to report material changes in internal control on a quarterly basis. As a result, one of the most important features of the monitoring component of the entity's internal control system is its ability to identify changes. Documentation facilitates this monitoring element.

In addition to enhancing the overall effectiveness of internal control, documentation of control policies and procedures also will facilitate management's assessment of effectiveness by providing a basis for:

- Evaluating design effectiveness
- Planning tests of operating effectiveness

Management should be careful to distinguish between the documentation of internal control and internal control itself. Creating a document that describes the control policies and procedures that should be followed is *not* internal control. Internal control is the *process* used by the *people* to carry out those documented policies and procedures.

The mere documentation of a control policy or procedure provides *no evidence* to support the operating effectiveness of the control. To support a conclusion about effectiveness, management will need to gather evidence by performing tests of controls.

Assessing the Adequacy of Existing Documentation

Many entities currently are involved in projects to assess the adequacy of their existing documentation of internal control. In assessing the adequacy of documentation, management should determine whether:

- *All significant controls objectives have been considered*. As described above, some control objectives, policies, and procedures will be more significant to the entity's overall internal control structure than others. When considering the adequacy of an entity's documentation of internal control, individual policies and procedures should be documented for all significant control objectives. If control policies have not been documented for certain significant control objectives, management must determine whether:
  - Controls do not exist to achieve the stated control objective, in which case the entity must design, implement, and document new control procedures, or
  - Controls exist to achieve the control objective; however they are informal, communicated verbally, or otherwise not documented. In this case, suitable documentation must be developed to facilitate an evaluation of the effectiveness of the design of the control.
- *Documentation is sufficient*. To be sufficient, the documentation should allow management and the external auditor to:
  - Determine whether the policy or procedure is adequately designed
  - Design and perform procedures to test the operating effectiveness of the controls

Documenting the Control Environment

The documentation of the entity's control environment should encompass all of the control environment elements described in COSO and summarized in "The Importance of the Control Environment" in the "Key Characteristics of the COSO Framework" section of this Alert. Those elements usually are described in documents such as:

- Board of directors' charter
- Audit committee documents and charter
- Company code of conduct

- Disclosure committee[5] charter
- Human resource policies and personnel handbook

Documentation can also encompass the elements essential in management's antifraud programs and controls.

Documenting Activity Level Control Policies and Procedures

The documentation of controls related to transaction processing streams should contain the following elements.

- A link between the control objective and the control policy or procedure
- A description of the control policy or procedure that achieves the control objective
- A description of:
  - How the control procedure is to be applied
  - Who is responsible for performing the procedure
  - How frequently the procedure is performed

There are no requirements for the form of the documentation. There are many different acceptable ways to document control policies and procedures, including narratives, "walk through" descriptions of key documents, and flowcharts. Computerized documentation tools may be used to facilitate this process.

Documentation of Tests of Controls

The entity should document the tests performed and evidence obtained to evaluate both the design and operating effectiveness of internal control. This documentation serves two purposes.

- It provides the CEO and CFO with the information needed to make and support their assessment of the effectiveness of internal control

5. As described in the section of this Alert titled "The SEC Rules" management is required to report on the effectiveness of the entity's disclosure controls and procedures on a quarterly basis. The SEC has recommended that entities form a disclosure committee to comply with this requirement.

- It may be used, at least in part, by the external auditors to reach their conclusion about management's assertion[6]

No definitive guidance on the form or content of the entity's documentation of its tests of controls currently exists. However, one might expect such guidance to address matters such as the following:

- The objective of the test performed
- A description of the test performance, including:
  - The scope of the procedures, for example, the number of transactions tested or business segments reviewed
  - When the test was performed or the period covered by the test
  - Who performed the test
- The results of the tests
- The conclusion reached as a result of the tests performed

Automated Documentation Tools

Since the passage of the Sarbanes-Oxley Act, many companies have developed computer software products that aid in complying with the internal control provisions of the Act. These software tools typically center on helping companies automate the documentation of internal control policies and procedures, although some products perform additional functions such as automating the testing and reporting on internal controls, business process activities (for example, the approval and payment of vendor invoices), or both.

The first function of an automated tool typically is to serve as a repository for all of the documentation relating to the design of internal control. In those instances where the documentation of the control or the control itself either does not exist or otherwise is deficient, the software may allow the company to efficiently (1) document existing policies or (2) design and document new ones.

6. The degree to which the external auditors may rely on tests performed by the entity to evaluate the effectiveness of internal control is a matter that is expected to be addressed in the Public Company Accounting Oversight Board's (PCAOB's) final standard, as discussed in the section of this Alert titled "The External Auditor's Standards."

Documentation Process

Automated internal control documentation tools typically use a combination of the following methods for creating and accumulating internal control documentation.

- *Reference existing documentation.* In many instances, the documentation of a policy or procedure already exists, for example, human resource policies or personnel manuals. When that is the case, the automated tool will allow this existing documentation to be accessed and reviewed by the user. To allow for this sharing of existing information, the automated tool may have to:
  - Interface with existing systems
  - Import existing data
- *Menu-driven responses.* To create documentation for a new or existing control procedure, the automated tool may provide users with choices from a pull down menu. For example, in order to describe a control objective, the user may be presented with a choice of: "ensure proper authorization of transactions," "verify accuracy," "ensure the capture of all valid transactions," and so on.
- *Free responses*. Instead of choosing from a predetermined list of possibilities, users may enter their own response into a text box.

Regardless of the method used to document new or existing controls, the goal remains the same—to accurately describe the entity's control policies and procedures as they currently exist. Whether that goal is achieved depends primarily on the qualifications, knowledge, and training of the user. To effectively document the entity's control policies and procedures, the user should have an in-depth understanding of all of the following:

- The entity's operations and existing control policies and procedures
- Internal control concepts, as described in the COSO framework (or other framework, if the entity does not use COSO)

- The financial reporting process
- The assertions that are represented in the financial statements[7]

Maintaining Information Integrity

In order to be effective, management must be able to rely on the accuracy of the documentation maintained. In order to achieve this integrity, the automated tool should have the following features.

- *Logical access controls.* The ability to modify documentation should be tightly controlled in the same way that access to all of an entity's sensitive information and computer applications is controlled. Individual users should be granted access privileges only to those areas of documentation that pertain to their assigned responsibilities. These access privileges should be administered carefully.
- *Standardized updating procedures*. As with any database, changes to data—in this case, the documentation of internal control—should be monitored and controlled. Modifications to the documentation should be done in an orderly fashion that ensures that all required changes are made. Once the changes have been made, they should be reviewed.

Monitoring Documentation Changes

Once the documentation warehouse becomes established as an accurate reflection of internal control, and standardized updating procedures are in place, any changes to the documentation should represent actual changes to internal control. Management is required to report material changes in internal control. Identifying and capturing changes to the internal control documentation will enable this requirement to be met.

7. Financial statement assertions are described in the auditing literature as the assertions that are embodied in an entity's financial statements. For example, implicit in the financial statements is the assertion that the statements present *all* transactions and that only bona fide, authorized transactions are included. The five financial statement assertions are: completeness, existence or occurrence, valuation, rights or ownership, and presentation and disclosure. A working knowledge of these assertions will help users understand risks and related controls. For example, there is a risk that the entity will fail to capture and process all valid transactions (completeness assertion). Therefore, a control objective of the entity's system should be to ensure completeness.

The automated documentation tool should have a means for identifying changes since the last reporting date. In order to help reviewers evaluate their significance, these changes should be able to be grouped in a variety of ways, including business process, control objective, and financial statement account grouping.

Testing of Internal Control

Management's tests of internal control should be:

- *Complete*. If the COSO criteria are used to measure internal control effectiveness, then all five components of internal control, including the control environment, should be tested.
- *Sufficient*. The scope and extent of the tests should be sufficient for management to draw a reliable conclusion about the overall effectiveness of internal control taken as a whole.
- *Timely*. The timing of the tests, or the time period covered by the tests, should allow management to draw a reliable conclusion as to the effectiveness of controls as of the reporting date, that is, fiscal year end.

Additionally, the entity should address both the design and the operating effectiveness of the control.

- *Design effectiveness.* A control policy or procedure should be designed in a way that material misstatements to the financial statements will be prevented or detected in a timely manner.
- *Operating effectiveness*. Tests to evaluate operating effectiveness should allow management to evaluate how the control procedure was applied, the consistency with which it was applied, and by whom it was applied.

To be effective, the tests should have:

- Clearly stated objectives
- A design that is appropriate to achieve those objectives

- A scope and extent that is comprehensive enough to draw a reliable conclusion

Testing the Control Environment

The control environment has a significant influence on the operating effectiveness of the other components of the COSO integrated framework. The control environment is different from the other components in that it:

- Has an *indirect* effect on the amounts and disclosures reported in the financial statement, and
- Is *not* transaction-oriented. As such, it does not lend itself to transaction-oriented testing.

Testing the operating effectiveness of the control environment may pose a challenge for management. Documenting the control policies that make up the control environment is not sufficient to draw a conclusion as to operating effectiveness. For example, the mere existence of a company code of conduct and its dissemination is not sufficient to allow management to conclude on the effectiveness of the related elements of the entity's control environment. Following the guidance provided above, tests must be performed to allow management to determine:

- How management, the board of directors, the audit committee, and the employees of the company applied the policies described in the code of conduct to their work
- The consistency with which individuals followed the guidelines contained in the code
- Who followed the code and who did not

In general, two different approaches have begun to emerge for testing the control environment.

- *Indirect*. Under this approach, management focuses its primary testing on activity-level controls. The results of those tests are evaluated carefully, and any deficiencies are investigated thoroughly to understand their root causes. Based on the information gained from these tests of activity-level controls, management is able to infer the relative effectiveness of the control environment.

- *Direct.* Under this approach, management plans and performs tests to gather evidence directly about the operating effectiveness of the control environment. Such tests might include employee surveys, interviews with selected individuals, and the performance of a computer general controls review. Management uses the results of these tests of the control environment to design the activity-level tests.

At the time this Alert was prepared the definitive guidance on internal control reporting did not express a preference for either approach. In the opinion of the author, directly testing the control environment will lead to more reliable conclusions about its operating effectiveness. Designing and performing these types of tests may be outside the realm of tests normally performed by audit or financial professionals; however, credentialed specialists in organizational development and other disciplines have developed tools and methodologies in this area that may be appropriate for management wishing to gain a direct understanding of an entity's control environment effectiveness.

Testing Activity-Level Controls

Assessing the Effectiveness of Design

Activity-level controls are effective when they can provide reasonable assurance that material financial statement errors will be prevented or detected in a timely fashion. To assess design effectiveness, management should consider:

- The general types of errors that could occur
- The points in the processing stream where errors may be introduced

After gaining an understanding of what could go wrong and where, management will then determine whether the system, as designed, adequately addresses these potential errors and error points.

Assessing Operating Effectiveness

Nature. Management will need to decide about the kinds of tests it will perform. For example, will the entity conduct inquiries, observe controls being performed, or re-perform certain control procedures? The nature of the tests performed depends on the kind of control procedure being tested and whether its performance is documented.

Typically, management will perform a combination of one or more controls to gather evidence about their effective operations. It would be unlikely that one test will provide all the evidence needed to support a conclusion. An opinion about control effectiveness most likely will be formed by the congruence and consistency of the evidence gathered from several sources and kinds of tests.

Typical tests that management may choose from include:

- Tests of transactions
- Re-performance of control procedures
- Tests of computer application controls
- Inquiries
- Direct observation

Timing. The Sarbanes-Oxley Act requires management to report on the effectiveness of internal control as of a point in time, namely, year end. As a practical matter, many tests will be performed in advance of the reporting date. In those situations, management will need to consider the need to perform additional tests to establish the effectiveness of the control procedure from the time the tests were performed until the reporting date. For example, if the entity tests the effectiveness of bank reconciliations as of June 30 and the reporting date is December 31, management will need to consider performing tests to cover the period from July 1 through December 31. These tests may *not* require a repeat of the detailed tests performed at June 30 for the subsequent six-month period. Once management establishes the effectiveness of the control procedure at June 30 it may be able to support the effectiveness of the control at the reporting date indirectly through the consideration of entity-level controls and other procedures such as:

- The effectiveness of personnel-related controls such as the training and supervision of personnel who perform control procedures.
- The effectiveness of risk identification and management controls, including change management.
- The effectiveness of the monitoring component of the entity's internal control.
- Inquiries of personnel to determine what changes, if any, occurred during the period that would affect the performance of controls.
- Repeating the procedures performed earlier in the year, focusing primarily on elements of the control procedure that have changed during the period.

Reporting

The section of this Alert titled "The SEC Rules" describes what management's report on internal control must contain. However, the SEC has not mandated a prescribed form for management's report. Of the items required to be included in management's report, the one that will require the most judgment is that which requires the report to contain:

> Management's assessment of the effectiveness of the company's internal control over financial reporting as of the end of the most recent fiscal year, including a statement as to whether or not internal control over financial reporting is effective. This discussion must include disclosure of any material weakness in the company's internal control over financial reporting identified by management. Management is not permitted to conclude that the registrant's internal control over financial reporting is effective if there are one or more material weaknesses in the company's internal control over financial reporting.

In its commentary to the final rules, the SEC requires management to state whether internal control is functioning effectively or not. "Negative assurance"—in which management states that "nothing came to its attention that would lead it to believe that internal control was not functioning effectively"—is not acceptable.

Material Weaknesses and Significant Deficiencies

Management is required to disclose any "material weakness" in the company's internal control. Further, the existence of one or more material weaknesses precludes management from concluding that its internal control is effective.

The SEC has stated that the term "material weakness" has the same meaning as the definition under generally accepted auditing standards (GAAS). The auditing literature defines material weakness in Statement on Auditing Standards (SAS) No. 60, *Communication of Internal Control Related Matters Noted in an Audit* (AICPA, *Professional Standards*, vol. 1, AU sec. 325). The terms "reportable condition" (as used in the auditing literature) and "significant deficiency" (which the SEC uses in its rules) are synonymous.[8]

The accepted definitions for the two key terms are as follows.

- *Significant deficiency*. An internal control deficiency in a significant control or an aggregation of such deficiencies that could result in a misstatement of the financial statements that is more than inconsequential.
- *Material weakness.* A significant deficiency or *an aggregation of significant deficiencies* that precludes the entity's internal control from providing reasonable assurance that material misstatements in the financial statements will be prevented or detected on a timely basis by employees in the normal course of performing their assigned functions. The

8. The PCAOB's proposed auditing standard relating to the independent auditor's audit of management's report on internal controls addresses the auditor's responsibilities regarding internal control deficiencies, material weaknesses, and related matters. Management may want to consult the proposed standard for further guidance and information.

inability to provide such reasonable assurance results from one or more significant deficiencies 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 errors or fraud in amounts that would be material in relation to the financial statements may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions.

Making Judgments About the Severity of Internal Control Deficiencies

Determining whether an internal control deficiency rises to the level of a material weakness will require management to consider:

- *Likelihood*, that is, the chance that the deficiency could result in a financial statement misstatement. When assessing likelihood, consider:
  - The relative importance of the control and whether the overall control objective is achieved by other control activities or a combination of control activities.
  - If the deficiency is an operating deficiency, the frequency of the operating failure rate. For example, numerous or repeated failures in the operation of a control would be more likely to be considered a significant deficiency than failures that are considered isolated occurrences.
  - Whether the control is automated and therefore could be expected to perform consistently over time.
- *Significance*, that is, the magnitude of potential misstatements resulting from the deficiency. When assessing significance, consider:
  - The nature of the account balance or classes of transactions affected by the deficiency and the financial statement assertions involved.
  - Whether the deficiency relates to an entity-level or activity-level control. Because entity-level controls can affect many account balances, classes of transactions, or finan-

cial statement assertions, weaknesses in entity-level controls that seem relatively insignificant by themselves could result in material financial statement misstatements.

Annual Reporting of Material Weaknesses That Have Been Corrected

Management is required to report on the effectiveness of internal control over financial reporting as of year end. In some cases, management may have identified and corrected a material weakness in internal control during an interim period. At issue is whether that corrected weakness is required to be reported in the entity's annual report on internal control.

To make that determination, management should consider whether the corrected deficiency has been operational for a period of time that is sufficient to draw a reliable conclusion about its operating effectiveness as of year end. Testing the corrected deficiency for design and operational effectiveness would be required to support management's conclusion. Before making its final decision regarding the reporting of a corrected deficiency, management should consult with its SEC legal counsel and the external auditors.

Resource Central

On the Bookshelf

The following publications deliver valuable guidance and practical assistance related to internal control.

- *Internal Control—Integrated Framework* (product no. 990012kk), a paperbound version of the COSO report that established a common definition of internal control different parties can use to assess and improve their control systems. It also includes information on how to prepare external reports and five tools for evaluating each of the components identified in the framework.
- *Financial Reporting Fraud: A Practical Guide to Detection and Internal Control* (product no. 029879kk), a paperbound

publication for CPAs in both public practice and industry. It uses case studies to provide information necessary to minimize fraud exposure for CPAs, employers, and clients.

- *Audit Committee Toolkit* (product no. 991001kk), a practice aid that brings you checklists, matrixes, questionnaires, and other materials that are designed to help the audit committee do the job it needs to do.

AICPA's reSOURCE Online Accounting and Auditing Literature

Get access—anytime, anywhere—to the AICPA's latest *Professional Standards*, Technical Practice Aids, Audit and Accounting Guides, Audit Risk Alerts, and *Accounting Trends & Techniques*. To subscribe to this essential service, go to www.cpa2biz.com.

reSOURCE CD-ROM

The AICPA is currently offering a CD-ROM product entitled *reSOURCE: AICPA's Accounting and Auditing Literature.* This CD-ROM enables subscription access to AICPA Professional Literature products in a Windows format, namely, *Professional Standards*, Technical Practice Aids, and Audit and Accounting Guides (available for purchase as a set or as individual publications). This dynamic product allows you to purchase the specific titles you need and includes hypertext links to references within and between all products.

Educational Courses and Training

The AICPA offers the following continuing professional education (CPE) courses related to internal control:

- *Internal Control Reporting for Public Companies*, a self-study course on CD (product no. 737132kk).
- *Internal Control and Design*, a CPE course (product no. 731850kk) that provides information on regulatory requirements and techniques for meeting them.
- *Internal Control Reporting: Standards for Compliance*, a video CPE course, expected to be available in April 2004.

- *Internal Control Reporting for Public Companies*, a July 17, 2003, Webcast that described what the SEC's final rules require of companies and who is affected. Available on CD-ROM (product no. 737132kk).
- *Internal Controls: Design and Documentation*, a CPE self-study course that explains why internal controls matter to management, auditors, and regulators; what makes up a good system; how internal controls can be both cost-effective and efficient; and how to create useable, affordable documentation. This course is expected to be available beginning February 2004.

Online CPE

The AICPA offers an online learning tool, *AICPA InfoBytes*. An annual fee will offer unlimited access to over 1,000 credits of online CPE in one- and two-hour segments. Register today at www.cpa2biz.com.

AICPA's Antifraud & Corporate Responsibility Resource Center

The AICPA's Antifraud & Corporate Responsibility Resource Center (www.aicpa.org/antifraud/) allows you to select optional ways to learn about fraud. The Center spotlights the new Web-based fraud and ethics case studies and commentaries recently issued; the AICPA antifraud Webcast series; the interactive CPA course *Fraud and the CPA*, and a competency model that allows you to assess your overall skills and proficiencies as they relate to fraud prevention, detection, and investigation, among other topics. In addition, the site offers press releases and newsworthy items on other AICPA courses related to prevention and detection and an overview of the AICPA Antifraud & Corporate Responsibility Program.

AICPA Audit Committee Effectiveness Center

Located at www.aicpa.org/audcommctr/homepage.htm, the AICPA Audit Committee Effectiveness Center presents the guidance and tools necessary to make audit committee best practices actionable. Available at the center is the AICPA Audit Committee Toolkit, the Audit Committee Matching System, Audit Committee e-Alerts, and other guidance and resources.

Member Satisfaction Center

To order AICPA products, receive information about AICPA activities, and find help on your membership questions call the AICPA Member Satisfaction Center at (888) 777-7077.

Hotlines

Accounting and Auditing Technical Hotline

The AICPA Technical Hotline answers members' inquiries about accounting, auditing, attestation, compilation, and review services. Call (888) 777-7077.

Ethics Hotline

Members of the AICPA's Professional Ethics Team answer inquiries concerning independence and other behavioral issues related to the application of the AICPA Code of Professional Conduct. Call (888) 777-7077.

Web Sites

Sarbanes-Oxley Act/PCAOB Implementation Central

Visit Sarbanes-Oxley Act/PCAOB Implementation Central at www.aicpa.org/Sarbanes/index.asp. This AICPA Web site provides extensive, up-to-date compliance information for CPAs.

AICPA Online and CPA2Biz

AICPA Online (www.aicpa.org) offers CPAs the unique opportunity to stay abreast of matters relevant to the CPA profession. AICPA Online informs you of developments in the accounting and auditing world as well as developments in congressional and political affairs affecting CPAs. In addition, www.cpa2biz.com offers all the latest AICPA products, including the Audit and Accounting Guides, the professional standards, CPE courses, practice aids, and alerts.

029200