



# Sarbanes-Oxley Section 404: Management's Assessment Process

Frequently Asked Questions

ADVISORY

# Contents

**1 Introduction**

**2 Providing a Road Map for Management**

**3 Questions and Answers**

3 Section I: Planning and Determining the Scope of the Assessment

8 Section II: Documenting and Evaluating the Design and Operating Effectiveness of Controls

13 Section III: Identifying, Assessing, and Correcting Deficiencies

15 Section IV: Reporting on Internal Controls

**16 Conclusion**

# Introduction

KPMG LLP has prepared this document for management, members of corporate teams working toward Sarbanes-Oxley Act (the Act) section 404 (S-O 404) compliance, and audit committee members. It is designed to help clarify a number of key issues related to management's assessment process as required by S-O 404. Specifically, it addresses frequently asked questions and provides general guidelines that management may use for planning and assessing the effectiveness of internal control over financial reporting.

It is important that readers understand that management is responsible for complying with the provisions of the Sarbanes-Oxley Act, and specifically with section 404. Management should consult with legal counsel, independent auditors, and other professionals in meeting these obligations.

This document contains only a general discussion of the matters included and should not be relied on as advice for any particular company, since no consideration is given to individual facts and circumstances, which could vary greatly from company to company. Some of the discussions in this document are based on the questions and answers issued by the staffs of the Security and Exchange Commission's (SEC's) Chief Accountant and Division of Corporation Finance and by the staff of the Public Company Accounting Oversight Board (PCAOB). The views and opinions of the staffs of the SEC and PCAOB could change in the future.

It is important to note that an example of the evolving nature of this discussion occurred as this document was being finalized for printing. This includes the issuing of a revised set of questions and answers from the SEC staff as well as additional questions and answers from the PCAOB staff. These recently released questions and answers provide further clarification on issues relating to the following matters, among others:

- The scope of internal control over financial reporting as it relates to compliance with laws and regulations
- The effect that the lack of an available Type II Report under the AICPA Statement on Auditing Standards (SAS) 70 from a service organization can have on management's assessment and the independent auditor's reports
- The independent auditor's walkthrough of major classes of transactions processed by a service organization

Ongoing revisions such as these add even more urgency to our recommendation that management should work closely with counsel, the company's independent auditors, and other advisers to determine the potential impact these or any future guidance revisions may have in light of the organization's specific circumstances.



# Providing a Road Map for Management



The Sarbanes-Oxley Act of 2002 (the Act) has changed the face of corporate governance. Many organizations are already at work planning and implementing processes that will help them assess the effectiveness of their internal control over financial reporting (ICOFR). A key aspect of this process has been trying to anticipate and address the questions and issues that might arise as management prepares for an audit of ICOFR.

Recently, the SEC and the PCAOB provided additional guidance to registrants and independent auditors about some of these issues. Using this guidance along with the collective experience already gained by management, we can begin to identify and address some of the questions and issues facing management.

In this document, which is part of our ongoing commitment to helping companies remain current with these issues, we address a number of questions, many of which management already may have encountered.

We also discuss general guidelines that management may use as a starting point to answer questions that arise as they develop and implement their own assessment processes.

## Understanding the Roles: Management and the Independent Auditor

Management is responsible for including an internal control report in its annual report that:

- States the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting
- Contains an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

The independent auditor is responsible for attesting to and reporting on the assessment made by the management of the issuer.

For the independent auditor to satisfactorily complete an audit of internal control over financial reporting, management must fulfill a number of important responsibilities<sup>1</sup>, including:

- Accepting responsibility for the effectiveness of the company's ICOFR
- Evaluating the effectiveness of the company's ICOFR using suitable control criteria, such as the COSO (Committee of Sponsoring Organizations of the Treadway Commission) criteria

- Supporting its evaluation with sufficient evidence, including documentation
- Presenting a written assessment of the effectiveness of the company's ICOFR as of the end of the most recent fiscal year

Management fulfills these responsibilities by undertaking a comprehensive approach that includes thorough planning and evaluation of its system of internal controls. Management should document the company's controls and begin testing their effectiveness. It is important that management allow sufficient time to complete this process in order to provide an appropriate basis for its assessment and to respond to any deficiencies that are identified. Identifying deficiencies early may provide management with sufficient time to correct deficiencies and determine the operating effectiveness of the controls prior to year-end reporting.

There are a number of methods a company may choose in developing an approach to fulfilling its responsibilities related to its assessment of internal control over financial reporting. Regardless of the method chosen, it is management's responsibility to design and implement a process that enables it to meet the requirements of section 404 of the Act.

<sup>1</sup>If the auditor concludes that management has not fulfilled these responsibilities, the auditor should communicate in writing to management and the audit committee that the audit of internal control over financial reporting cannot be satisfactorily completed and the auditor must disclaim an opinion.

# Questions and Answers

***In the following pages we offer answers to common questions that may arise during these steps of the assessment process:***

- *Planning and determining the scope of the assessment*
- *Documenting and evaluating the design and operating effectiveness of controls*
- *Identifying, assessing, and correcting deficiencies*
- *Reporting on internal controls*

*These represent only some of the questions that management may ask. Some may not apply to your organization because of your specific assessment processes. More importantly, these answers are not absolute. They are intended to offer management a starting point from which to develop its own answers to specific assessment questions.*

*In addition, management should review the authoritative literature issued by the SEC for registrants and by the PCAOB for independent auditors to gain a more complete understanding of what is expected of the company. This will also help management better prepare itself for the respective reporting deadlines.*

## Section I. Planning and Determining the Scope of the Assessment

*Regardless of the complexity and breadth of an organization's control structure, evaluating the effectiveness of ICOFR requires careful planning. This plan can include a process that examines the overall approach to documentation, identification of controls and assessment procedures, significant milestones, and anticipated timelines. The plan also may include instituting policies and procedures that will be used in the assessment process and appropriate internal communication processes. Following are some specific issues that may have to be addressed.*

### **Should management document ICOFR for all locations or business units?**

The answer to this question is yes. Companies should have some level of documentation of ICOFR for all locations or business units, including those not considered significant either individually or in the aggregate. The extent of this documentation may vary across locations or business units and often is based on the financial significance of each location or business unit.

Management's documentation may take many forms. These could include various kinds of information, such as:

- Company policy manuals
- Process models
- Accounting manuals
- Memoranda
- Flow charts
- Job descriptions
- Documents
- Forms
- Decision tables
- Procedural write-ups
- Self-assessment reports
- Other documentation as appropriate

No particular form of documentation is required and the form and extent of documentation can vary depending on the company's size, complexity, and documentation approach. However, simply having manuals and policies without any reconciliation to the assessment process may not be enough. Management should be able to demonstrate how it considers the documentation in the assessment process.

### **How does management determine which controls to test for operating effectiveness?**

A key element of management's assessment process is the determination of controls to be tested. Management should document the process used to assess the effectiveness of ICOFR, including the determination of controls to be tested. This documentation will make it easier for the independent auditor to understand management's process and to plan and perform the related audit procedures.

From an independent auditors' perspective, an account balance is considered significant if there is more than a remote likelihood that the account could contain misstatements that could have a material effect on the financial

statements, which, in turn, could result in a risk of overstatement or understatement. This is true whether the account is viewed individually or in aggregate with others. Other accounts may be considered significant based on the expectations of a reasonable user. The assessment as to likelihood is made without giving consideration to the effectiveness of internal control over financial reporting.

Components of a financial statement caption can be subject to differing risks (inherent and control) as well as different controls. These components should be considered separately as potentially significant accounts. Independent auditors may consider separate components of a caption significant due to the company's organizational structure. For example, the "accounts receivable net" caption may be split into at least three separate accounts: domestic receivables, foreign receivables, and the allowance for doubtful accounts. In addition, if a company has a number of separate business units, each with unique management and accounting processes, the components of the captions at each separate business unit or even within a business unit also may be individually considered as potentially significant accounts.

### Can a framework other than COSO be used?

Management may use a framework other than COSO, if the framework selected is a suitable, recognized control framework. This can be defined as a framework that has been established by a body or group following due-process procedures, including broad distribution of the framework for public comment.

Footnote 67 of the SEC's final rules on *Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports* states that "the *Guidance on Assessing Control* published by the Canadian Institute of Chartered Accountants and the *Turnbull Report* published by the Institute of Chartered Accountants in England & Wales are examples of other suitable frameworks."

Other suitable frameworks available for management's assessment on internal control over financial reporting may be developed in the future. As a result, management may want to review these frameworks as they emerge to determine whether they represent more appropriate methods on which to base assessments.

### What is the Enterprise Risk Management Framework? Does this replace the existing COSO framework?

COSO has released a draft of a document entitled, "Enterprise Risk Management Framework." The new study incorporates—but does not replace—the 1992 COSO study on internal control. Also, it is "designed to raise a consistent 'risk and control consciousness' throughout the enterprise and to become a commonly accepted model for discussing and evaluating the organization's risk management processes."

Doug Prawitt of Brigham Young University, a member of the COSO Advisory Council, was quoted as saying, "Many organizations have adopted the COSO control framework, various audit standards rely on that framework, and it looks like the internal control reporting required under Sarbanes-Oxley will be heavily based on the COSO internal control model. So it was absolutely critical that the new risk framework not undermine COSO's earlier work."<sup>2</sup>

### What information technology (IT) systems or applications generally are included in the scope of S-O 404 documentation and testing related to ICOFR?

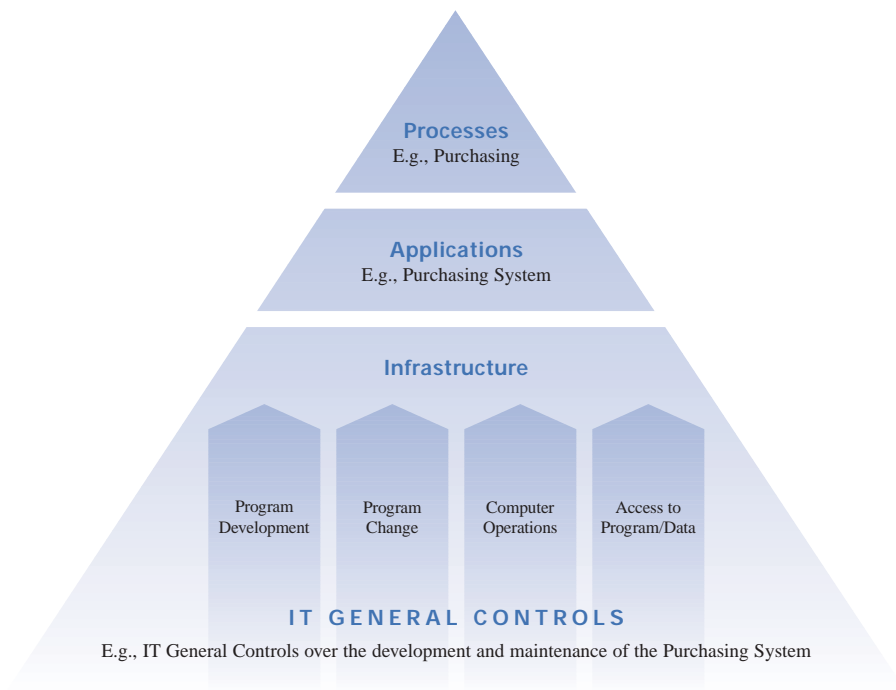
Applications and the related supporting infrastructure that support key processes, control objectives, and relevant assertions related to significant accounts and disclosures in the financial statements should be included in the scope of management's assessment process.

Because IT applications often support the initiation, authorization, recording, processing, and reporting of financial transactions, IT controls may represent an integral part of ICOFR. Financial reporting applications are often supported by many ancillary, or feeder, applications that provide critical financial data, and companies may rely on a large number of applications to meet their objectives.

Once an application is determined to be in the scope of the process, management should (1) document applicable components of the application, (2) identify significant controls designed within the application to achieve specific objectives, (3) gain an understanding of the IT architecture and infrastructure around the application, and (4) test the four components of IT general controls (see the chart on page 5) that have a pervasive effect on the application. As part of its documentation, management should include a sufficient level of detail to describe the in-scope processes and significant controls built within the applications supporting those processes. The chart on page 5 provides an example of how IT general controls can be linked to applications and processes.

<sup>2</sup> "Bringing ERM into Focus," Christy Chapman, *Internal Auditor*, June 2003

## LINKING IT GENERAL CONTROLS TO APPLICATIONS AND PROCESSES



To determine which IT general controls are included in the scope of management's assessment, first identify and document controls at the process level (e.g., purchasing) including the controls that are supported by information technology (e.g., purchasing system) where financial transactions are processed. The scope of IT general controls can then focus on those controls over the development and maintenance of the application.

**Many organizations outsource certain processes, activities, or functions, such as payroll, that are included in the scope of the S-O 404 assessment. How do controls performed at off-site locations affect ICOFR? What's more, how does management determine and document the operating effectiveness of controls at these service organizations?**

If management has determined that a service organization's activities are part of the company's information system, management should evaluate whether the service organization's controls are designed and operating effectively. One starting point is to obtain a

service auditor's report on controls in operation at the service organization. The service auditor's report will be either a Type I or a Type II report under the AICPA Statement on Auditing Standards (SAS) 70:

- **SAS 70 Type I** reports indicate whether the controls described were (1) presented fairly in all material respects and (2) suitably designed to provide reasonable assurance that the control objectives specified in the description would be achieved if complied with satisfactorily. *A Type I report provides no assurance that the controls are operating effectively and provides limited benefits to a 404 assessment.*

- **SAS 70 Type II** reports include the items listed in Type I above and provide a description of the tests of controls and results of those tests performed by the service auditor. They also provide the service auditor's opinion on whether the controls that were tested were operating effectively during the specified period. Under certain circumstances, management may be able to obtain evidence about the operating effectiveness of controls at the service organization by obtaining and reviewing this type of report.

Management should note that there is no assurance that the control objectives specified within the SAS 70 reporting cover everything that would be relevant to the company's internal control over financial reporting. As a result, management should review the reports to determine whether any additional procedures should be performed to support its assessment of all significant control objectives affecting the company. In addition, management is responsible for maintaining and evaluating controls over the appropriate flow of information to and from the service organization. This includes user controls.

Other approaches management may consider for obtaining evidence of ICOFR operating effectiveness related to the service organization include performing:

- Tests of the company's controls over the activities of the service organization (re-performance)
- Tests of controls at the service organization

### How recent should an SAS 70 Type II report from a third-party service provider be in order to be considered reliable?

There is no precise answer as to how recent an SAS 70 Type II report should be to be considered reliable. However, if a significant period of time has elapsed between the end of the time period covered by the service auditor's tests of controls and the date of management's assessment, management should perform procedures to determine whether any information in the SAS 70 Type II report should be updated to reflect significant changes in the service organization's controls since the date of the SAS 70 report. The procedures should cover the period from the end of the time period referred to in the SAS 70 Type II report to the date of management's assessment.

PCAOB Auditing Standard No. 2 states that the independent auditor should inquire of management to determine whether management has identified any changes in the service organization's controls subsequent to the period covered by the service auditor's report. These may include:

- Changes communicated by the service organization to management
- Changes in service organization personnel with whom management interacts
- Changes in reports or other data received from the service organization
- Changes in contracts or service-level agreements with the service organization
- Errors in the service organization's processing

The extent of procedures necessary to update the SAS 70 Type II report will vary depending on the amount of time between the date of the service auditor's report and management's assessment. Also, PCAOB Auditing Standard No. 2 indicates that if management has identified changes, the independent auditor should determine whether management has performed procedures to evaluate the effect of any identified changes on the effectiveness of the company's ICOFR.

### To what extent are taxes included within the scope of management's assessment?

Taxes can be one of the largest expenses on a company's income statement, and tax assets and liabilities (both current and deferred) often are significant to the balance sheet. In addition, taxes can exist at the account-or disclosure-component level in the form of compensation, transaction, and property-based taxes. Because taxes could have a significant impact on financial reporting, management should not ignore tax processes as part of its assessment of ICOFR.

Moreover, there is often an assumption that the scope of tax inclusion in management's assessment should focus only on processes related to income taxes, such as corporate income taxes and the tax provision. In reality, nonincome taxes—such as those related to sales or value-added taxes as well as those related to accounting for intercompany, customs, and cross-border transactions—could be an integral part of other key financial processes.

In their frequently asked questions, the staffs of the SEC's Chief Accountant and Division of Corporation Finance (the SEC staff) indicated they believe the definition of ICOFR

does not encompass a registrant's compliance with applicable laws and regulations, with the exception of compliance with the applicable laws and regulations directly related to the preparation of financial statements. Accordingly, we do not believe that the preparation of tax returns is contemplated in the definition of internal control over financial reporting. However, the SEC staff did indicate that the SEC's financial reporting requirements and the Internal Revenue Code are examples of regulations that are directly related to the preparation of the financial statements.

### How should current-year acquisitions and divestments be treated?

As for *current-year acquisitions*, the SEC staff's frequently asked questions indicated they would typically expect management's report on ICOFR to include controls at all consolidated entities. The SEC staff acknowledged that it might not be possible to conduct an assessment of an acquired business's ICOFR in the period between the transaction consummation date and the date of management's assessment. In these instances, the SEC staff indicated they would not object to management excluding from its evaluation of ICOFR business acquisitions for a period not to exceed one year from the date of acquisition. In these instances, the SEC staff indicated that management should refer to (1) a discussion in the registrant's Form 10-K or Form 10-KSB regarding the scope of the assessment and (2) such disclosure, noting that management excluded the acquired business from management's report on ICOFR. If such a reference is made, however, management must identify the acquired business that was excluded and indicate the significance of the acquired business to the company's consolidated financial statements.

The SEC staff indicated that notwithstanding management's exclusion of an acquired business's internal controls from its annual assessment, a company must disclose any material change to its internal control over financial reporting that is due to the acquisition pursuant to either Exchange Act Rule 13a-15(d) or Exchange Act Rule 15d-15(d). In addition, the period in which management may omit an assessment of an acquired business's internal control over financial reporting from its assessment of the company's internal control may not extend beyond one year from the date of acquisition. Such assessments also may not be omitted from more than one annual management report on internal control over financial reporting. There is currently no guidance from the SEC or PCAOB that specifically addresses how management should treat divestments for the purposes of section 404. However, management's assessment of the effectiveness of the company's ICOFR is "as of" the end of the company's most recent fiscal year. Therefore, to the extent a company divests part of its operations prior to the end of the most recent fiscal year, internal controls over financial reporting at the divested operation would be excluded from management's assessment for purposes of section 404 of Sarbanes-Oxley.

If management chooses to exclude a business unit from documentation and testing due to the business unit's planned divestiture, management should be certain that the divestiture will take place prior to the company's fiscal year-end. Otherwise, the processes and controls for that business unit should be documented, tested, and included in management's assessment as of the the company's fiscal year-end.

### **When a company undertakes an initial public offering, should the company include management's assessment on the effectiveness of ICOFR and a related auditor's report on internal control in an initial registration statement filed on Form S-1?**

No. Form S-1 filed pursuant to an initial registration of securities does not require the inclusion of the information required by Item 308 (Internal Control Over Financial Reporting) of Regulation S-K. The SEC's Final Rule, *Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports*, impacts entities subject to the reporting requirements of the Securities Exchange Act of 1934. Section 404 of the Sarbanes-Oxley Act applies to a registrant for the first annual report after the entity becomes an "issuer" (after consideration of the effective dates of the SEC's Final Rule with respect to accelerated and nonaccelerated filers).

Paragraph 2 of PCAOB Auditing Standard No. 2 indicates that section 404 applies to an "issuer" as defined in section 3 of the Securities Exchange Act of 1934, which includes enterprises that file or have filed a registration statement (i.e., Form S-1) with the SEC that has not been declared effective under the Securities Act of 1933 and has not been withdrawn. While this language has created some confusion, the SEC staff has confirmed that Item 308 of Regulation S-K does not apply to an initial registration of securities filed on Form S-1.

An entity undertaking an initial public offering may voluntarily assess the effectiveness of its ICOFR and ask its independent auditor to perform an audit of ICOFR. In such instances, the audit of ICOFR ordinarily would be performed pursuant to the provisions of PCAOB Auditing Standard No. 2.

### **To what extent is it appropriate for management to discuss areas of the financial accounting and reporting process with the company's independent auditor?**

Consultation with the independent auditor about accounting and reporting issues facilitates audit quality. Accordingly, we believe that it is important for company management to continue to freely consult with the company's independent auditor regarding these kinds of issues. However, the independent auditors' advice cannot serve as a substitute for management performing its own responsibilities. Management remains responsible for the selection and application of accounting policies and practices and the design and effective operation of controls over the entity's financial reporting process.



## Section II. Documenting and Evaluating the Design and Operating Effectiveness of Controls

*The documentation and evaluation of ICOFR is an essential part of management's assessment process. It provides evidence that controls related to management's assessment have been identified, can be communicated to those responsible for their performance, and can be monitored. Additionally, the results of management's evaluation of the design and operating effectiveness of controls must be documented. Some examples of issues that may arise during this step are included here.*

### **Should management test and evaluate all controls that have been identified through ICOFR documentation?**

Management should test those controls that it considers important to its evaluation and assessment of ICOFR. PCAOB Auditing Standard No. 2 indicates that (1) the independent auditor should evaluate management's process for determining which controls should be tested and (2) these controls generally include:

- Controls over initiating, authorizing, recording, processing, and reporting 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 depend
- Controls over nonroutine and nonsystematic transactions, such as accounts involving judgments and estimates
- Company-level controls, including
  - The control environment
  - Controls over the period-end financial reporting process (both annual and quarterly)

To date, many companies have identified a large number of controls during their ICOFR documentation. In some cases, there are multiple controls that address the same control objective and assertion. To help management identify appropriate controls for testing and to support its assertion about ICOFR effectiveness, companies are finding it useful to prioritize controls for testing by designating them “key,” “primary,” or “high, medium, and low.”

The purpose for this control categorization exercise is to identify those controls necessary to provide management with the appropriate level of evidence regarding relevant assertions related to the affected account balances and disclosures in the financial statements. Once the controls are prioritized, management can determine the tests of operating effectiveness necessary to support its assessment of the effectiveness of ICOFR.

To assist with this “categorization” process, many companies are finding it useful to review process flows and other documentation in order to identify the points in the process where errors or fraud are most likely to occur. Once a specific point has been identified, management can select controls at that point or after that point in the flow for testing. After the controls have been selected, management should review all the controls it has identified to verify that relevant assertions for the related account have been satisfactorily addressed.

*Note: Due to the significance of this determination in management's assessment process, it is important for management to have regular meetings with its independent auditor to discuss and obtain agreement on the process that management has used to identify key controls.*

### **What controls are considered to be company-level controls and how should these be evaluated?**

Company-level controls often have a pervasive impact on controls at the process, transaction, or application levels. As part of the assessment process, management should consider the extent to which company-level controls will be documented and tested.

These include the following:

- Controls within the control environment, including tone at the top, authority and

responsibility assignment, policy and procedure consistency, and companywide programs (such as codes of conduct and fraud prevention) that apply to all locations and business units. Also included are board-approved policies that address significant business control and risk management practices.

- Management’s risk assessment process.
- The period-end financial reporting process.
- Monitoring of operations results; internal audit function, audit committee, and self-assessment program activities; and centralized processing, such as shared service environments.

Determining whether sufficient company-level controls exist is a matter of management judgment. However, to make an informed decision, management should follow a two-step process. First, it should determine the nature and extent of controls that need to be in place to accomplish the objectives of the organization. Then it should decide whether these controls are designed and operating effectively.

Management should note that testing company-level controls alone is not sufficient for management to conclude on whether ICOFR is effective.

### How does management determine whether a control is designed effectively?

Tests of design are performed to determine whether controls, if operating properly, can effectively prevent or detect misstatements in the entity’s financial records. Tests of design are usually performed by inquiry and validating observation or inspection of documents, such as reports and completed forms; through on-screen prompts, such as errors or warnings; or, most effectively, by performing a process “walkthrough.”

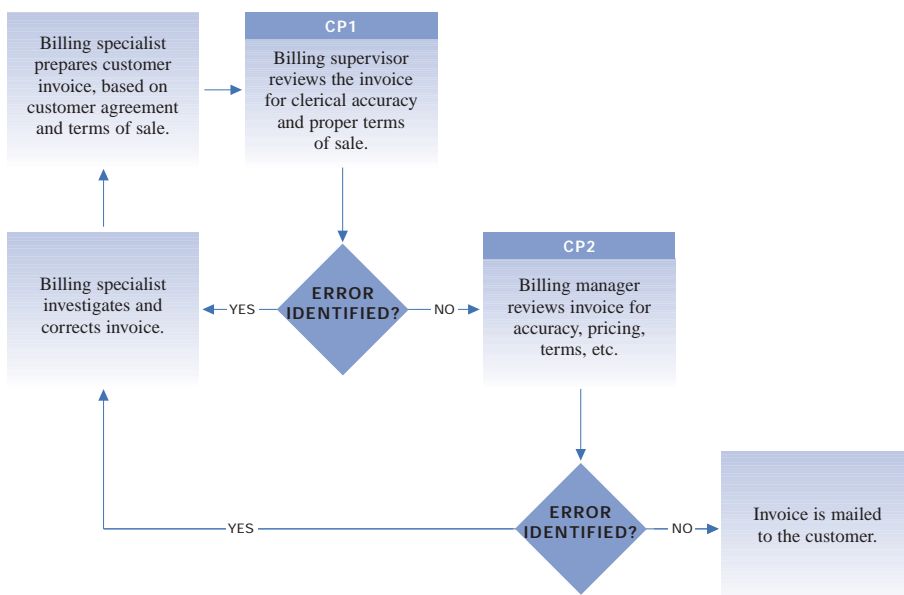
Although management is not required to perform them, process walkthroughs can help management:

- Confirm its understanding of the process flow of transactions
- Confirm its understanding of the design of controls identified for all five components of internal control over financial reporting, including those related to the prevention and detection of fraud
- Confirm that its understanding of the process is complete by determining whether all points in the process at which misstatements related to each relevant financial statement assertion could occur have been identified
- Evaluate the effectiveness of the design of controls
- Confirm whether controls have been placed in operation

Tests of design typically address:

- Control type, including configuration, management review, and authorization
- Control nature (whether automated or manual, preventive or detective)
- Control frequency (daily, weekly, monthly)
- Experience and competence of the individual performing the control

### IDENTIFYING CONTROLS FOR TESTING



As shown in the chart above, management may view control point 2 (CP2) as a strong, reliable control. What’s more, if the CP2 control is operating effectively, testing of CP1 may be redundant and therefore unnecessary. (By the same token, CP1 may be operating effectively, and testing of CP2 may be redundant and unnecessary.) Generally, personnel closely involved with the process and controls should be involved in identifying controls to be tested.

- Error investigation and correction procedures, including the timeliness of such procedures

It is important to note that inquiry alone ordinarily is not sufficient to support design effectiveness.

**When testing operating effectiveness, how much testing should management perform? What testing sample sizes should be used?**

The amount of testing depends on a number of factors. However, it should be comprehensive enough to support management’s assessment of the effectiveness of internal controls. This should include considering all relevant assertions for each account and disclosure included in the scope of management’s assessment. In general, management’s testing should be more extensive than that of the independent auditor. This doesn’t mean that in all cases management’s sample sizes for a single control at a single location would be larger than those of the auditor. It simply means that management’s testing, taken as a whole, should be more comprehensive and potentially cover more processes, controls, accounts, and business units or locations.

When determining the extent of testing procedures to perform, management should take into account the nature of the control, its frequency of operation, and the overall significance of the control.

The extent of testing also depends on the risk of failure of the control being tested. Risk of failure is defined as the risk of a material misstatement arising from the failure of a control. If management believes there is a high risk of failure, management should consider expanding the extent of testing for that control.

Factors that affect whether the control may represent a higher risk of failure include:

- Changes in the volume or nature of transactions that might adversely affect control design or operating effectiveness
- Changes in the design of controls
- The degree to which the control relies on the effectiveness of other controls (for example, the control environment or IT general controls)
- Changes in key personnel who perform the control or monitor its performance
- Whether the control relies on performance by an individual or is automated
- The complexity of the control

It is management’s responsibility to determine the extent of testing—or sample sizes—that it considers sufficient to support its assessment of the effectiveness of internal control over financial reporting.

Management should base its decision on all of these factors. The table on this page illustrates examples of minimum sample sizes for consideration when planning the extent of test work on manual control operating effectiveness. Management’s determination of minimum sample sizes should not be based on the examples shown in the table; management should select sample sizes that will provide it with sufficient evidence based on the company’s specific facts and circumstances.

In situations where a control that is applied to every transaction is automated through the IT system, a system query may be the most appropriate testing technique. With this technique, one query may be an appropriate test for an IT control that would be expected to operate consistently in a well-controlled environment. System query may be used to test operating effectiveness if management is satisfied with the results of the test of design.

System queries can be used to:

- Test whether programmed logic surrounding a control contained within an IT application is operating as expected, that is, whether the system will identify a predefined exception.
- Retrieve information from an IT application about the configuration or designations within the system. For example, management could query the application to determine how tolerance limits were configured or to obtain a list of individuals who have authority to perform a certain function in the system in order to evaluate segregation of duties.

**EXAMPLE MINIMUM TESTING SAMPLE SIZES**

CONTROL OPERATING FREQUENCY	MINIMUM SAMPLE SIZE	CONTROL OPERATING FREQUENCY	SAMPLE SIZE
Annual	1	Weekly	5–10
Quarterly	2–3	Daily	15–30
Monthly	2–4	Recurring manual control (multiple times per day)	30–60

### Does an independent auditor distinguish between testing performed by internal audit and testing performed by management?

The independent auditor must perform enough of the test work supporting its opinion so that the auditor's own work provides the principal evidence for the auditor's opinion. Keeping this principal evidence requirement in mind, the independent auditor also may use the work of others in an audit of ICOFR.

While the independent auditor isn't required to use work performed by others, the independent auditor may, in certain areas, choose to do so based on the:

- Objectivity and competence of the individual who performed the work
- Quality and effectiveness of the work
- Nature of the controls tested by other individuals
- Timing of the work performed
- Results of auditor's re-performance of certain work performed by others

For example, if an individual responsible for a control's operation also tests the control's operating effectiveness testing, this personal self-assessment will not be considered objective. As a result, the independent auditor cannot use this work in performing its independent assessment.

If members of the internal audit department (or other individuals who work under the direction of management and are not responsible for control operation) perform the testing, the work generally will be considered to be more objective than the work performed by those who are responsible for the control operation (e.g., control self-assessment). Of course, the independent auditor still evaluates the objectivity and competence of the individuals performing the work as well as the quality and effectiveness of documentation supporting management's assessment.

Factors generally affecting the independent auditor's decision to use the work of others include aspects of the nature of the control, such as the:

- Materiality of the accounts and disclosures that the control addresses as well as the risk of material misstatement
- Degree of judgment required to evaluate the operating effectiveness of the control
- Pervasiveness of the control
- Level of judgment or estimation required in the account or disclosure
- Potential for management override of the control

There are areas in which the independent auditor cannot use the work of others. These areas include walkthroughs and testing of control operating effectiveness related to the control environment, including controls specifically designed to prevent and detect fraud.

### Many organizations have IT systems and applications that were installed prior to the current year. Should management test the design and operating effectiveness of the program development general IT controls for these systems and applications?

All systems and applications that support financial reporting processes should have the appropriate general IT controls in place, including program development controls. Management should evaluate these program development controls.

When management has the original documentation from the initial installation of an application or system relating to program development controls, this documentation may form the basis of management's assessment and testing. In these cases, management should also have sufficient documentation of the program change controls from the date of installation through the current date.



Consistent with the provisions of PCAOB Auditing Standard No. 2, management should demonstrate that it has a thorough understanding of how all significant classes of transactions are initiated, authorized, processed, recorded, and reported. That understanding should be documented in sufficient detail to facilitate performance of a process or transaction walkthrough. Management should perform sufficient tests of systems installed in prior years to help ensure that significant accounting processes (calculations, postings, etc.) are functioning properly and significant application controls are operating as intended.



### Does S-O 404 require additional controls for flexible ERP reporting, spreadsheets, and other types of end-user computing?

End-user computing applications, such as spreadsheets and reports, may present an organization with a unique set of IT general control needs. This is because providing end users with these types of flexible tools typically increases the risk of misstatements caused by errors due to incomplete or inaccurate data. Since the output from end-user computing processes frequently appears as an authoritative document that management will rely on in its financial reporting, end-user computing applications that support significant internal controls should be identified and included in control documentation.

The organization should support end-user computing with general controls that are consistent with the level of sophistication of the system. General controls should address areas such as access to programs and data, program changes, program development, and computer operations. While end-user computing generally does not require the same rigors of general IT controls as other

systems, these controls should be appropriate to help ensure the completeness and accuracy of reported data, consistency of presentation, proper calculation and validation, and security that is appropriate to the significance and complexity of the report or spreadsheet.

### Which controls should be tested for the period-end financial reporting process?

Since the period-end financial reporting process is so significant, understanding and evaluating it is critical. This process includes the procedures used to:

- Enter transaction totals into the general ledger
- Initiate, authorize, record, and process journal entries in the general ledger
- Record recurring and nonrecurring adjustments to the annual and quarterly financial statements, such as consolidating adjustments, report combinations, and classifications
- Draft annual and quarterly financial statements and related disclosures

As part of its assessment process, management should test controls over each of the items listed above. This testing should be performed on the controls used to produce both annual and quarterly financial information.

Management should take care to identify and test both the manual and automated controls that are included in the period-end financial reporting process. In addition, it should evaluate the nature and extent of oversight by all appropriate parties, including management, the board of directors, and the audit committee.

### How can management judge whether company-level controls are operating effectively?

Ordinarily, it is not possible to test the company-level controls without visiting some or all of the locations or business units over which they operate. The effectiveness of some company-level controls, such as the implementation of a code of conduct or application of accounting manuals, relies on evidence that is obtained outside of the central or corporate office.

The number of locations or business units that are included in the testing is a matter of judgment. When determining the number of locations to visit, management may consider factors such as the degree of centralization of controls, the commonality of process and control design between locations, and the consistency of accounting policies or job descriptions. Obviously, locations that are included in the testing should be representative of the populations of locations or business units that are considered to be important when aggregated. In addition, the extent of the test work should be greater than that performed by the independent auditor.

## Section III. Identifying, Assessing, and Correcting Deficiencies

*Management should establish a process through which all deficiencies in ICOFR across the entire company are identified and accumulated. This will help management conclude its assessment of ICOFR effectiveness by evaluating the severity of all identified deficiencies. Among the questions that may come up during this phase are the following.*

### **Can a material weakness in ICOFR exist when a material misstatement in the financial statements has not occurred or been identified?**

Yes, a material weakness in ICOFR can exist even though a material misstatement in the financial statements has not occurred or been identified. The significance of a deficiency in ICOFR depends on the potential for misstatement, not on whether a misstatement actually has occurred. Thus, management and its independent auditors may conclude that a material weakness in ICOFR exists even if a material misstatement has not occurred or been identified.

### **If management replaces or redesigns a deficient control, how long should the new control operate and how much testing should management perform to determine whether or not it is operating effectively?**

Management should allow sufficient time to evaluate and test controls. If deficiencies are discovered, management may have the opportunity to correct and address these deficiencies prior to the reporting date. However, once a new control is in place, management should allow enough time for its operations to validate the control's operating effectiveness.

The amount of time that a control should be in place and operating effectively depends on the nature of the control and how frequently it operates. Under ordinary circumstances, control remediation that occurs after year-end will not mitigate an identified deficiency for reporting purposes. PCAOB Auditing Standard No. 2 indicates that the independent auditor should disclaim an opinion on management's disclosure about corrective actions taken by the company after the date of management's report. Management should look to its established testing protocols to determine the extent of testing necessary to conclude on the effectiveness of a remedied control.

For example, management may have an established policy governing the extent of testing, such as the size of samples to be tested. Management considers this sample adequate to support its assertion about the effectiveness of internal control over financial reporting. In this example, management's policy states that a manual control that operates daily should have sixty<sup>3</sup> occurrences tested. If management identifies a deficiency and remedies the control, it should allow enough time for at least sixty occurrences of the remedied control to be tested for operating effectiveness.

### **Will a number of multiple significant deficiencies automatically translate into a material weakness in ICOFR?**

Not necessarily. Based on the guidance in paragraph E90 of PCAOB Auditing Standard No. 2, a specific number of significant deficiencies will not necessarily determine the existence of a material weakness in ICOFR. However, all significant deficiencies should be evaluated to determine whether they, individually or when aggregated with other significant deficiencies, result in material weaknesses in ICOFR.

There are a number of factors that might be considered when aggregating deficiencies, including whether the significant deficiencies:

- Affect the same financial statement account or disclosure
- Impact a common assertion in a financial statement account or disclosure

### **Are there any general guidelines that have been developed to define "more than inconsequential" when identifying significant deficiencies?**

PCAOB Auditing Standard No. 2 defines a significant deficiency as a control deficiency or a combination of control deficiencies that result in "more than a remote likelihood" that a "more than inconsequential" misstatement

<sup>3</sup> The sample sizes in this discussion are presented for illustrative purposes only. Management's determination of sample sizes should not be based on the example discussed above; instead management should select a sample size that will provide it with sufficient evidence based on the company's specific facts and circumstances.

of an entity's annual or interim financial statements will not be prevented or detected. The definition of inconsequential includes a combination of concepts from Staff Accounting Bulletin (SAB) No. 99, *Materiality*, and AU section 312. The definition of inconsequential is largely based on the discussion of magnitude in SAB No. 99 and on AU sec. 312 for its directions regarding the consideration of misstatements both individually and in the aggregate as well as the possibility of undetected misstatements. A misstatement is *inconsequential* if a reasonable person would conclude, after considering the possibility of further undetected misstatements, that the misstatement, either individually or when aggregated with other misstatements, would clearly be immaterial to the financial statements. If a reasonable person could not reach such a conclusion regarding a particular misstatement, that misstatement is *more than inconsequential*.

The significance of a deficiency in internal control depends on the potential for misstatement, not necessarily on whether a misstatement actually has occurred. For purposes of evaluating the quantitative significance of potential misstatements that result from internal control deficiencies, one general guideline for determining "more than inconsequential" is whether there are potential misstatements that equal or exceed 1 percent of pretax earnings. In evaluating the magnitude of identified internal control deficiencies, it is important to note that the concept contemplates an analysis of misstatements that *could* occur, not that *have* occurred.

Management also should remember that the determination of whether a significant deficiency exists includes both the quantitative and qualitative analysis of whether the deficiency is more than remote and more than inconsequential. Accordingly, there may be instances when potential misstatement amounts that are less than the quantitative

measure noted above also may be considered "more than inconsequential," depending on management's judgment of these qualitative factors (e.g., potential misstatements involving related-party transactions).

#### **How can management identify controls that relate to safeguarding assets? How are deficiencies evaluated?**

COSO defines "safeguarding" assets as including controls that provide reasonable assurance of preventing or detecting unauthorized acquisition, use, or disposition of the company's assets that could have a material effect on the financial statements. Safeguarding does not refer to the company's business continuity or contingency plans, or to the physical protection of assets or controls over making bad business decisions.

This means it is important to determine whether the use of company assets is authorized, not whether the use was a good or bad business decision. For example, safeguarding assets as defined by COSO does not contemplate losses from providing a service at an unreasonable cost, as long as it is authorized. The same is true of losses from authorized but unproductive research or ineffective advertising.

Management should identify the risks within each key process of unauthorized acquisition, use, or disposition of the company's assets that could have a material effect on the financial statements. It should also test those controls that mitigate those risks, including not only controls over the appropriate signing authorities but also controls to ensure that the proper authorization occurs.

A process can be subject to many safeguarding risks. For example, in capital assets procurement processes, approvals may be required for the business case, request for proposals, vendor selection, purchase orders, receiving reports, invoices, and checks. Each

of these approvals has a valid operational or compliance objective. However, only one of these approvals may provide the necessary safeguarding control for purposes of management's S-O 404 requirements and, accordingly, the extent of testing may vary from control to control.

This does not mean that all authorization controls can be considered safeguarding controls. For example, under ordinary circumstances, authorizing journal entries is not considered a safeguarding control, as failure to authorize the journal entry generally would not expose the company to misuse or misappropriation of company assets. The first consideration in determining if a control is a safeguarding control is whether there is the potential for inappropriate or unauthorized use of company assets. Where this potential exists, the risk related to safeguarding should be documented. In addition, management should recognize such risks when analyzing financial reporting processes.

Once a deficiency in safeguarding controls is identified, the key consideration for the purposes of management's assessment is whether such an action could result in a financial statement misstatement, not whether the financial statements are misstated. The key factor is the magnitude of the potential for unauthorized use of company assets in any particular instance. For example, an employee may be able to enter into a contract binding the company to purchase certain material inventory items without the required management authorization. Even if the purchase is properly recorded in the financial statements, a lack of authorization may constitute a deficiency in internal control over financial reporting.

## Section IV. Reporting on Internal Controls

*Management is required to include its assessment of the effectiveness of the company's ICOFR in its annual report. Management's report on ICOFR is required to include the following:*

- *A statement of management's responsibility for establishing and maintaining adequate ICOFR for the company*
- *A statement identifying the framework used by management to conduct the required assessment of the effectiveness of the company's ICOFR*
- *An assessment of the effectiveness of the company's ICOFR as of the end of the company's most recent fiscal year, including an explicit statement as to whether that ICOFR is effective*
- *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 company's ICOFR*

**Many companies provide their independent auditors with draft financial statements for review prior to company approval. How can a company demonstrate to the auditor that it would have picked up an error noted in the draft financial statements that would otherwise result in a material weakness or significant deficiency?**

Using the guidance issued by the PCAOB staff, the answer to this question depends on the stage at which management presents the draft financial statements to the independent auditor and the independent auditors' knowledge of the company's financial reporting process.

To expedite the audit process and the financial reporting process, many companies provide an early draft to their independent auditor. The independent auditor's comments on the company's draft financial statements are part of the iterative process of completing the audit. If management presents the draft financial statements to the independent auditor at a later stage in the financial reporting process and purports that the company's review process is complete or nearly complete, the independent auditor generally would conclude that material deficiencies in the draft financial statements are indicative of a material weakness in the company's ICOFR.

One way to demonstrate management's belief that the company's controls are operating effectively is by modifying the traditional audit process to provide the independent auditor with just a single draft of the financial statements. However, this process is not necessarily the approach that was expected as a result of the Act. Nor is it very practical in many situations. The PCAOB staff has indicated that such a process might make it difficult for some companies to meet the accelerated filing deadlines for their annual reports. The



PCAOB staff also indicated that when combined with the accelerated filing deadlines, this type of process might put the auditor under increased pressure to complete the audit of the financial statements in too short a period of time. As a result, this approach could impair, rather than improve, audit quality. Therefore, some type of timely information sharing between management and the auditor is preferable.

It is common for management to share interim drafts of the company's financial statements with the independent auditor. In these cases, it is important that management clearly communicate to the company's independent auditor:

- The state of completion of the financial statements
- The purpose for which the company is providing the draft financial statements to the auditor

Question 7 of the PCAOB's Staff Questions and Answers provides additional guidance and examples of appropriate involvement by the auditor when reviewing draft financial statements.

# Conclusion

It is clear that Sarbanes-Oxley section 404 presents management with a number of challenges. We believe that an ideal approach to meeting these challenges is to open a wide-ranging discussion—among management, independent auditors, members of corporate S-O 404 compliance teams, and audit committee members—in which all can come together to develop appropriate guidelines for addressing management's responsibilities in assessing internal control over financial reporting.

We hope this document contributes to that conversation and offers management, directors, and audit committee members a useful perspective in meeting their challenges.

KPMG LLP is the audit, tax, and advisory firm that has maintained a continuous commitment throughout its history to providing leadership, integrity, and quality. The Big Four firm with the strongest growth record over the past decade, KPMG turns knowledge into value for the benefit of its clients, people, communities, and the capital markets. Its professionals work together to provide clients access to global support, industry insights, and a multidisciplinary range of services. KPMG LLP ([www.us.kpmg.com](http://www.us.kpmg.com)) is the U.S. member firm of KPMG International. KPMG International's member firms have nearly 100,000 professionals, including 6,800 partners, in 148 countries.



