

# Defining Issues<sup>®</sup>

KPMG LLP



## SEC Guidance on Internal Control Over Financial Reporting

The SEC's new interpretive guidance for management evaluations of internal control over financial reporting and the related rule amendments are intended to allow management to comply with Section 404 of the Sarbanes-Oxley Act more cost-effectively.<sup>1</sup> The guidance is effective immediately. In a related action, the SEC is seeking comment on the definition of a "significant deficiency" that would apply to management's obligations under the SEC's rules implementing the Sarbanes-Oxley Act.<sup>2</sup>

The SEC's guidance is similar to last December's proposal, but differs in the following ways:

- It maintains that fraud risks are expected to exist at every company and that the nature and extent of the fraud-risk-assessment activities should be commensurate with the company's size and complexity.
- It describes more fully how entity-level controls relate to financial-reporting elements and clarifies that management's evaluation should include the entity-level and pervasive elements of its internal control over financial reporting that are necessary to provide reasonable assurance that financial reporting is reliable.
- It revises the indicators of a material weakness and clarifies that the presence of the indicators alone does not always mean that a material weakness exists.
- It aligns the guidance more closely with PCAOB Auditing Standard No. 5.<sup>3</sup>

Intent and Principles  
Identifying Risks and Related  
Controls  
Evaluating Operating  
Effectiveness  
Reporting  
Evidential Matter to Support  
the Assessment  
Alignment with Auditing  
Standard No. 5  
"Significant Deficiencies"

1  
2  
3  
3  
4  
4  
4  
5

### Intent and Principles

The SEC's guidance is intended to facilitate the exercise of judgment in designing a process for evaluating internal control over financial reporting that is tailored to a company's particular facts and circumstances and that provides management with a "reasonable basis" for its assessment. The guidance is not intended to replace the company's control framework. It requires the annual assessment to be made in accordance with a suitable control framework's definition of an effective system of internal control.

©2001-2007 KPMG LLP, a U.S. limited liability partnership and a member firm of the network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved. KPMG and the KPMG logo are registered trademarks of KPMG International, a Swiss cooperative. 29535NYO

Photo: GettyImages/Digital Vision/Yamada Taro 200408494-001

<sup>1</sup> SEC Releases No. 33-8810, Commission Guidance Regarding Management's Report on Internal Control Over Financial Reporting Under Section 13(a) or 15(d) of the Securities Exchange Act of 1934, June 20, 2007, and No. 33-8809, Amendments to Rules Regarding Management's Report on Internal Control Over Financial Reporting, June 20, 2007, both available at [www.sec.gov](http://www.sec.gov).

<sup>2</sup> SEC Release No. 33-8811, Definition of a Significant Deficiency, June 20, 2007, available at [www.sec.gov](http://www.sec.gov).

<sup>3</sup> PCAOB, Auditing Standard No. 5, An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements, May 24, 2007, available at [www.pcaobus.org](http://www.pcaobus.org).

The guidance is organized by two overriding, related principles. The first is that management should evaluate the design of the controls to determine whether they adequately address the risk that a material misstatement in the financial statements would not be prevented or detected in a timely manner. The guidance describes a top-down, risk-based approach to this principle, including the role of entity-level controls in assessing financial-reporting risks and the adequacy of controls. The approach focuses attention on only the controls necessary to provide reasonable assurance regarding the reliability of financial reporting.

The second overriding principle is that the evaluation of evidence about the operation of controls should be based on assessments of the controls' associated risk. The approach allows management to cost-effectively align its evidence-gathering procedures and the evidence it obtains with its assessment of risk. Management may therefore be able to obtain evidence for its evaluation from more efficient procedures, such as self-assessments in low-risk areas.

Management can apply these two principles to tailor its evaluation methods and procedures. The SEC expects that by following the two principles, companies that vary in size and complexity will be able to comply with the internal-control evaluation and reporting requirements more effectively and efficiently. An evaluation that complies with the SEC's interpretive guidance is one way, but not the

only way, to satisfy the evaluation requirements under the Securities Exchange Act of 1934.

The guidance explains the application of its approach to four areas: identifying risks to reliable financial reporting and the controls that address those risks, evaluating the operating effectiveness of the controls, reporting, and evidential matter to support the assessment.

### Identifying Risks and Related Controls

The guidance directs management to begin its evaluation by identifying the risks to reliable financial reporting that could, individually or in combination, result in a material misstatement to the financial statements. The identification process should vary according to the characteristics of the company, such as its size, complexity, organizational structure, and its processes and financial-reporting environment. The risks to be evaluated include the risk of fraudulent activity (including the improper override of internal controls), which should be evaluated under the assumption that all entities have fraud risk. Management then evaluates whether it has controls in operation that are designed to address the identified risks.

The guidance individually addresses entity-level controls, IT controls, and multiple locations.

**Entity-Level Controls.** The SEC distinguished three types of entity-level controls: (1) those that have an important but indirect effect on the company's ability to prevent or detect a misstatement—for example, certain

control-environment controls, (2) those that are designed to identify possible breakdowns in lower-level controls but do not by themselves adequately address financial-reporting risks—for example, controls that monitor company operations, and (3) those that operate at the process, application, transaction, or account level and may adequately prevent or detect material misstatement on a timely basis. The first and second types of entity-level controls ordinarily would not be relied upon by themselves to control a specific financial-reporting risk for a specific financial-reporting element. Generally, the more indirect the relationship to a financial-reporting element, the less effective the entity-level control will be in preventing or detecting a misstatement.

#### **Automated or IT Dependent Controls.**

Management should consider the design and operation of the automated controls or IT dependent controls and the relevant general IT controls over the applications that provide the IT functionality. General IT controls ordinarily do not directly prevent or detect material misstatements in the financial statements. However, the effective operation of an automated or IT dependent control depends on effective general IT controls. Management would ordinarily consider and evaluate only the general IT controls that are necessary to adequately address financial-reporting risks.

**Multiple Locations.** Management's consideration of financial-reporting risks generally includes all of the locations or business

units. If management determines that financial-reporting risks are addressed by controls that operate centrally, the evaluation process is consistent with that of a business with a single location or business unit.

### Evaluating Operating Effectiveness

Management should evaluate evidence that is sufficient to provide a reasonable basis for its assessment of the effective operation of internal control over financial reporting. The SEC's guidance allows management to support its evaluation from direct tests of controls and from ongoing monitoring activities. Management evaluates the risk characteristics of both the financial-reporting elements and the related controls to determine the evaluation method and procedures necessary to obtain sufficient evidence.

Management's consideration of the risk characteristics of a financial-reporting element includes its materiality and the susceptibility of the underlying account balances, transactions, or other supporting information to material misstatements. Generally, as the materiality of a financial-reporting element increases, the risk for controls associated with that element increases. In addition, the risk of misstating a financial-reporting element generally increases if the underlying account balances, transactions, or other supporting information involves significant judgment, susceptibility to fraud, complexity in the underlying accounting requirements, change in the nature or volume of underlying transactions, or potential effects from technological or economic developments.

The guidance directs management to con-

sider the likelihood that a control may fail to operate effectively. Among the other things that affect the likelihood that a control may fail are these:

- The type of control (i.e., automated or manual) and how often it is used,
- The complexity of the control,
- The risk of management override,
- The level of judgment required to operate the control,
- The competence of the personnel performing or monitoring the control,
- Changes in key personnel performing or monitoring the control,
- The nature and materiality of misstatements that the control is designed to prevent or detect,
- The degree to which the control depends on the effective operation of other controls, and
- The operating effectiveness of the control in prior years.

**Multiple Locations.** If the controls necessary to address financial-reporting risk operate at more than one location or business unit, as opposed to being controlled centrally, management would ordinarily obtain and evaluate evidence of the operation of the controls at the individual locations or business units. If the combined risks of control failure and misstatement of the related financial reporting element at individual locations or business units is assessed as low, management may determine that evidence obtained from self-assessment procedures or other ongoing monitoring procedures, when combined with evidence obtained from a centralized control that monitors the results of operations at individual locations, is sufficient for the

evaluation. However, as these combined risks increase, such as when the controls are complex or judgmental, management needs more evidence to support an assessment that the controls at the location operate effectively. When deciding whether the nature and extent of evidence is sufficient, management should generally consider the risk characteristics of the controls for each financial-reporting element, rather than making a single judgment for all controls at the location.

### Reporting

Management evaluates quantitative and qualitative factors to determine whether any control deficiencies are material weaknesses. The guidance directs management to consider the likelihood that a control will fail to prevent or detect a misstatement and the magnitude of the error that might result from the deficiency. Factors that affect whether there is a "reasonable possibility" that a deficiency will result in a misstatement in a financial-reporting element include:

- The nature of the financial-statement elements involved;
- The susceptibility of the related asset or liability to loss or fraud;
- The subjectivity, complexity, or extent of judgment required to determine the amount involved;
- The interaction or relationship of the control with other controls;
- The deficiency's interaction with other deficiencies; and
- The possible future consequences of the deficiency.

The guidance also presents factors to consider when evaluating magnitude of the mis-

statement that may result from a deficiency. They include the financial-statement amount or total of transactions exposed to the deficiency and the volume of activity in the account balance or class of transactions that relates to the current period or that is expected to affect future periods.

Management should consider all relevant information to determine whether there is a material weakness. This includes determining whether the following situations indicate a deficiency in internal control over financial reporting, and, if so, whether the deficiency represents a material weakness:

- Identification of fraud, whether or not material, committed by senior management,
- Restatement of previously issued financial statements to correct a material misstatement,
- A material misstatement in financial statements identified in the current period in circumstances that indicate it would not have been discovered by the company's internal control over financial reporting, and
- Ineffective audit-committee oversight of the company's external financial reporting and related internal controls.

Management should also determine whether individual or aggregate deficiencies might keep prudent officials from obtaining reasonable assurance that transactions are properly recorded and result in financial statements prepared in conformity with generally accepted accounting principles.

A deficiency that represents a material weakness must be disclosed and precludes an assessment that internal control over financial reporting is effective. Management

should consider including the following in its disclosure of the material weakness:

- The nature of the material weakness,
- Its impact on financial reporting and on internal control over financial reporting, and
- Management's current plans, if any, to remediate the weakness or actions already taken to remediate it.

The guidance states that the disclosure will be more useful to investors if management differentiates the potential effect of the material weakness on the financial statements, distinguishing material weaknesses that may have a pervasive effect on internal control over financial reporting from those material weaknesses that do not.

The guidance explains that if a company restates its financial statements, its management should consider the need to modify or supplement its original disclosures regarding the effectiveness of both internal control over financial reporting and disclosure controls and procedures in order to include any material information necessary to prevent the original disclosures from being misleading.

### **Evidential Matter to Support the Assessment**

Management's evidential matter must provide "reasonable support" for its assessment. An integral part of this support is documentation of the design of the internal controls that address financial reporting risks and others that are necessary for effective internal control over financial reporting. The documentation may take various forms and need not address all controls within every process

that affects financial reporting. The nature and extent of the evidential matter supporting an assessment of the operating effectiveness of internal control over financial reporting will depend on management's assessment of risk of the controls and other circumstances, but will include documentation of the methods and procedures used to gather and evaluate evidence and the basis for the conclusion about the effective operation of internal control over financial reporting.

The guidance describes situations in which management may base its assessment on evidence from its direct knowledge of the effectiveness of controls obtained from its general interaction with its business processes.

Management should consider whether reasonable support for its assessment of operating effectiveness is contained in existing company records and may create limited incremental support beyond a description of how the interaction provided sufficient evidence to support its assertion. For high risk areas, however, management may determine that separately maintained evidential matter supporting the assessment is necessary and will assist the audit committee in exercising its oversight of the company's financial reporting.

### **Alignment with Auditing Standard No. 5**

The SEC's adopted guidance is more closely aligned with the Auditing Standard No. 5 than was its December proposal. However, the guidance acknowledges that there will be differences in the testing approaches used by management and the independent auditor, and suggests that the coordination between



management and auditors will ensure that management's evaluation and the external audit are completed efficiently and effectively.

### **"Significant Deficiencies"**

Section 302(a) of the Sarbanes-Oxley Act requires management to report significant deficiencies to its company's audit committee and independent auditor. The SEC's recent request for comment defines a significant deficiency as "a deficiency, or combination of deficiencies, in internal control over financial reporting that is less severe than a material weakness, yet important enough to merit attention by those responsible for oversight of a registrant's financial reporting."<sup>4</sup> The definition, which is the same as the definition in PCAOB Auditing Standard No. 5, is intended to allow "sufficient and appropriate" management judgment on matters that should be reported to the audit committee and independent auditor.

Interested parties must submit comments on the proposal defining "significant deficiencies" by July 18, 2007.

Registrants should not treat the descriptive and summary statements in this newsletter as a substitute for the text of the SEC's guidance, related rule amendments, and request for comment, or any related rules and proposals. When complying with related filing requirements, registrants should consult the text of all relevant final rules and requirements, consider their particular circumstances, and consult their accounting and legal advisors.

This is a publication of KPMG's  
Department of Professional  
Practice—Audit  
212-909-5600

### **Contributing authors:**

Walton T. Conn, Jr.  
John A. Hawryluk

Earlier editions are available at:  
[www.us.kpmg.com/definingissues](http://www.us.kpmg.com/definingissues)

Defining Issues® is a registered trademark of KPMG LLP.  
© 2001-2007 KPMG LLP, a U.S. limited liability partnership and a  
member firm of the network of independent member firms affiliated  
with KPMG International, a Swiss cooperative. All rights reserved.  
KPMG and the KPMG logo are registered trademarks of KPMG  
International, a Swiss cooperative. 29535NYO

---

<sup>4</sup> See footnote 2 above.