

November 21, 2003

Office of the Secretary  
Public Company Accounting Oversight Board  
1666 K Street, NW  
Washington, DC 20006-2803

Via E-mail to [comments@pcaobus.org](mailto:comments@pcaobus.org)

RE: PCAOB Rulemaking Docket Matter No. 008  
PCAOB Release No. 2003-017, October 7, 2003  
(Proposed Auditing Standard – An Audit of Internal Control over Financial Reporting Performed  
in Conjunction with an Audit of Financial Statements)

Dear Board Members:

We very much appreciate the opportunity to provide comments to the Public Company Accounting Oversight Board's ("Board" or "PCAOB") proposed auditing standard. These comments are offered on behalf of the Information Systems Audit and Control Association (ISACA) and IT Governance Institute (ITGI), in my capacity as the International President of both of these organizations.

ISACA is an international professional, technical and educational organization dedicated to being a recognized global leader in IT governance, security, control and assurance. With members in more than 100 countries, ISACA is uniquely positioned to fulfill the role of a central, harmonizing source of IT control practice standards the world over. Its strategic alliances with other organizations in the financial, accounting, auditing and IT professions ensure an unparalleled level of integration and commitment by business process owners.

ITGI strives to assist enterprise leaders in their responsibility to make IT successful in supporting the enterprise's mission and goals. Its goals are to raise awareness and understanding among, and provide guidance and tools to, boards of directors, executive management and chief information officers (CIOs). The ultimate goal is to ensure that IT meets and exceeds expectations, and its risks are mitigated.

Taken as a whole, we support the draft standard and what it sets out to accomplish. We list below our comments on some of the areas covered in the draft standard. We have made comments in 4 areas:

- IT Controls—We suggest clarification of some of the IT control-related terminology used in the standard.

- IT Control Framework—We suggest an alternative view of IT controls using the *Control Objectives for Information and related Technology* (COBIT) as a formal guidance framework.
- Reliance on IT Internal Audit—We suggest revisiting this area and allowing public accounting firms to rely on the work of IT internal audit.
- Audit Committee Effectiveness—We suggest that additional definition regarding the role of the audit committee in the IT governance area be provided, and that the IT Governance Institute be used as a resource for this.

### **IT Controls**

We note that “IT general controls” are referred to throughout the proposed standard. However, the scope of the IT general controls is not defined. We are concerned that organizations and auditors may focus on only the control activities component of general controls defined in COSO, i.e., “General controls commonly include controls over data center operations, system software acquisition and maintenance, access security, and application system development and maintenance.” We explain below what we feel is a more comprehensive view of IT controls.

We also noted an inconsistency and lack of clarity in the references to application controls within the draft standard. We feel that this should be addressed as well, and provide below a view on how this could be accomplished.

If the scope of IT general and application controls is not further clarified, then there is an increased risk that organizations and their auditors will not consider the entire IT governance framework in their evaluation of the effectiveness of the financial reporting control framework. We believe that further clarification and definition of the term “certain information technology general controls” used within the document should be considered. Once again, we offer the alternative detailed below to cover this concern.

As noted in our recent publication, *IT Control Objectives for Sarbanes-Oxley*, which we have attached to this submission, IT controls apply to all COSO components, not just the control activities component. We believe that the Board may want to consider referencing COBIT within the final guidance, as a framework for the IT control environment, much as COSO has been recommended as the internal control framework (see the Framework section below for further clarification).

COSO identifies five essential components of effective internal control. Below, we highlight, in each of the five COSO component areas, our rationale for requesting further clarification be provided within the standard, by referring to COBIT as the IT control framework. A description of the relationship of IT to all five COSO components follows.

#### 1. Control Environment

The control environment primarily addresses the company level. However, IT frequently has characteristics that may require additional emphasis on business alignment, roles and responsibilities, policies and procedures, and technical competence. The following list describes some considerations related to the control environment and IT:

- IT is often mistakenly regarded as a separate organization of the business and thus a separate control environment.
- IT is complex, not only with regard to its technical components but also in how those components integrate into the company's overall system of internal control.
- IT can introduce additional or increased risks that require new or enhanced control activities to mitigate successfully.
- IT requires specialized skills that may be in short supply.
- IT may require reliance on third parties where significant processes or IT components are outsourced.
- The ownership of IT controls may be unclear.

## 2. Risk Assessment

It is likely that internal control risks could be more pervasive in the IT organization than in other areas of the company. Risk assessment may occur at the company level (for the overall organization) or at the activity level (for a specific process or business unit). At the company level, the following may be expected:

- An IT strategy subcommittee of the company's overall Sarbanes-Oxley steering committee, with the following responsibilities:
  - Oversight of the development of the IT internal control strategic plan, its effective and timely execution/implementation, and its integration with the overall Sarbanes-Oxley compliance plan
  - Assessment of IT risks, e.g., data integrity, security, confidentiality and availability

At the activity level, the following may be expected:

- Risk assessments built throughout the systems development methodology
- Risk assessments built into the infrastructure operation and change process
- Risk assessments built into the program change process

## 3. Control Activities

Control activities primarily address the activity level. Without reliable information systems and effective IT control activities, public companies would not be able to generate accurate financial reports. As general and application controls increasingly replace manual controls, IT general and application controls are becoming more important.

## 4. Information and Communication

COSO states that information is needed at all levels of an organization to run the business and achieve the entity's control objectives. However, the identification, management and communication of relevant information represent an ever-increasing challenge to the IT department. Supporting the other four components of the COSO framework, are the determination of which information is required to achieve control objectives and the communication of this information in a form and time frame that allow people to carry out their duties. The IT organization processes most financial reporting information. However, its scope is usually much broader. For example, the

IT department may also assist in implementing mechanisms to identify and communicate significant information or events, such as regulatory reporting or accounting disclosures.

#### 5. Monitoring

Monitoring, which covers the oversight of internal control by management through continuous and point-in-time assessment processes, is becoming increasingly important to IT management. There are two types of monitoring activities: continuous monitoring and separate evaluations. IT performance and effectiveness are increasingly monitored using performance measures that indicate if an underlying control is operating effectively. Consider the following examples:

- Defect identification and management—Establishing metrics and analyzing the trends of actual results against metrics can provide a basis for understanding the underlying reasons for processing failures. Correcting these causes can improve system accuracy, completeness of processing and system availability.
- Security monitoring—Building an effective IT security infrastructure reduces the risk of unauthorized access. Improving security can reduce the risk of processing unauthorized transactions and generating inaccurate reports, and can ensure a reduction of the availability of key systems if applications and IT infrastructure components have been compromised.

At the company level, the following may be expected:

- Centralized continuous monitoring of computer operations
- Centralized monitoring of security
- IT internal audit reviews. (While the audit may occur at the activity level, the reporting of audit results to the audit committee will be at the company level.)

At the activity level, the following may be expected:

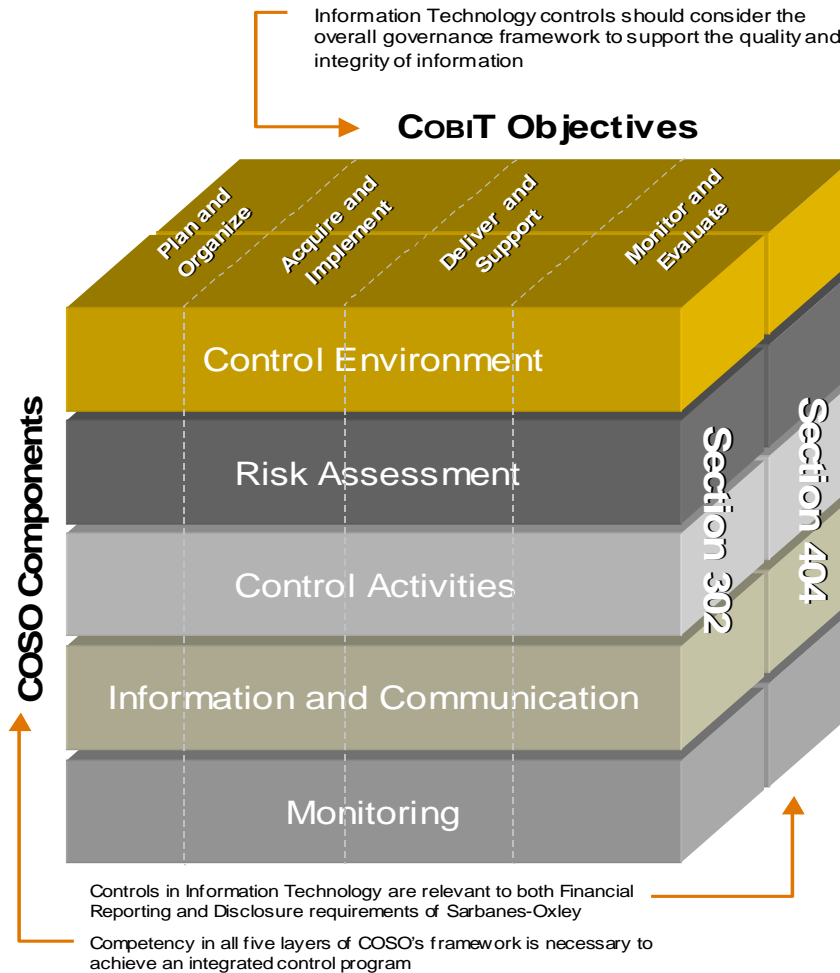
- Defect identification and management
- Local monitoring of computer operations or security
- Supervision of local IT personnel

### **IT Control Framework**

We believe that, where IT is significant to the financial reporting of business enterprises, these enterprises need to use an IT control framework to supplement the overall COSO framework, as illustrated in the attached publication *IT Control Objectives for Sarbanes-Oxley*.

COBIT, originally introduced in 1996, is an open, *de facto* IT governance and control framework, now in its third edition. The framework, which is entirely compliant with COSO, is referred to and used globally by assurance and control professionals, and by business process owners and IT management. Again, we applaud the PCAOB for taking on the issues, especially as they apply to IT controls.

We would like to recommend that the Board adopt COBIT as the IT control framework. While the importance of IT control is embedded in the COSO internal control framework, IT management requires more examples to help document and evaluate controls. COBIT is an IT governance model, which provides both company-level and activity-level objectives and associated controls. Using the COBIT framework, a company can design a system of IT controls to comply with S404 of the Sarbanes-Oxley Act. The following depicts the COSO–COBIT relationship within the requirements of Sarbanes-Oxley.



### **Reliance on IT Internal Audit**

While we agree that a public accounting firm should independently review IT controls within the IT control environment, we do have reservations about the inference that the public accountant cannot use the results of testing performed by management and others within other COSO components. IT audit professionals normally perform this testing. Many of those hold the Certified Information Systems Auditor (CISA) certification, offered by ISACA since 1978 and earned by more than 30,000 professionals worldwide. We suggest that the public accounting firm could determine the adequacy and appropriateness of such testing, based on the competence of the internal auditor and the auditor's positioning and independence, with additional testing being performed as necessary in the circumstances. If reliance cannot be placed on IT general controls testing then no credit can be given to the work that internal audit professionals are carrying out every day. We recommend that the Board consider revising this rule to provide further

clarification on the reliance public accounting firms can place on the work of IT internal auditors.

### **Audit Committee Effectiveness**

Reference paragraph 56:

*“Evaluating the Effectiveness of the Audit Committee’s Oversight of the Company’s External Financial Reporting and Internal Control Over Financial Reporting”*

The company’s audit committee plays an important role within the control environment, including the monitoring components of internal control over financial reporting. Within the control environment, the existence of an effective audit committee is essential to setting a positive tone at the top. Within the monitoring component, an effective audit committee is crucial to challenging the company’s activities in the financial arena.

However we do have the following comments:

- We suggest that the main issue is the effectiveness of the audit committee in overseeing corporate governance over financial reporting, which includes governance over the IT function. Additional emphasis on the spirit of the controls over IT governance should be considered.
- IT governance is such an integral part of corporate governance, including internal control, which we believe boards and the audit committee need to extend governance to IT. Doing so will in turn provide the leadership, organizational structures and processes that ensure that the enterprise’s IT sustains and extends the enterprises strategies and objectives. The current environment, which encompasses the new standard and other issues the PCAOB is addressing, calls for increasing emphasis on a broader corporate governance role for audit committees. The audit committee must deal effectively with IT governance and its implications if it is to deal effectively with processes to monitor risk and ensure that the system of internal control is effective in reducing those risks to an acceptable level.
- The ITGI was created for such reasons, and has been focusing on creating and delivering seminal research to assist in the provision of solutions to deal with these issues. We feel that the ITGI can provide some value going forward to the PCAOB, especially as it deals with the overarching issues of governance and IT. Much of the research and thought-provoking work the ITGI has created is closely linked back to COBIT—the framework for IT governance and control.

Again, we appreciate the opportunity to comment on the proposed standard. Thank you for considering our views. We would be happy to discuss them with you in further detail.

Respectfully submitted,

Marios Damianides, CISA, CISM, CA, CPA  
2003-2004 International President  
ISACA (info@isaca.org) ITGI (info@itgi.org)

Enc. *IT Control Objectives for Sarbanes Oxley*