Navigating the Standards for Information Technology Controls

By Joseph B. O'Donnell and Yigal Rechtman

JULY 2005 - Pervasive use of computers, along with recent legislation such as the Sarbanes-Oxley Act (SOA), has increased the importance of information technology (IT) in attest services. The 2000 report of the Panel on Audit Effectiveness (see www.pobauditpanel.org) recommended that "audit firms place a high priority on enhancing the overall effectiveness of auditors' work on internal control, particularly with respect to the depth and substance of their knowledge about companies' information systems."

Auditors are faced with the challenge of understanding an auditee's IT processing and control environment. Further complicating the situation are various guidelines and standards whose application depends on the nature of the entity: a publicly traded company, a privately held company, or a government agency. In addition, the entity may have operations outside of the United States. Auditing and assurance services for entities in these different situations are regulated by different standards-setting bodies, and understanding these different requirements in the context of information systems processing and controls is critical.

The Auditing Standards Board at the AICPA promulgated what U.S. financial auditors accept as generally accepted audited standards (GAAS). Government auditors follow the Government Accountability Office (GAO; formerly the General Accounting Office) auditing standards, the "Yellow Book," in performing audits of government agencies. The International Federation of Accountants (IFAC) provides auditors with global guidance with its International Standards for Auditing (ISA). Countries that maintain their own auditing standards, such as the United States, the United Kingdom, and Canada, have been reluctant to adopt ISAs, and rely on their own standards. The Public Company Accounting Oversight Board (PCAOB) provides standards for audits of publicly traded companies. These standards apply to audits and assurance services provided to domestic and international companies whose stock is publicly traded in U.S. stock markets.

Generally, the AICPA, GAO, IFAC, and PCAOB standards that refer to IT processes and controls emphasize the importance of IT processes and controls in accessing the client's control environment.

Another organization, the Information Systems Auditing and Control Association (ISACA; www.isaca.org), provides standards and guidance on information technology and information security (IS) assurance services for its members. ISACA issues the Control Objectives for Information Technology (COBIT). COBIT includes IT and IS assurance standards, guidelines, and procedures. Although this guidance is binding only for ISACA members, it could have significant indirect impacts on CPAs. To maintain its members' proficiency, ISACA tests and certifies its members' professional capabilities as a Certified Information Security Auditor (CISA) or a Certified Information Security Manager (CISM).

IT Controls and the CPA

Statement of Auditing Standard (SAS) 94, *The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit*, requires the consideration of the importance of IT processes and controls in the preparation of financial statements. In addition, an auditor must consider whether an IT specialist is required. This decision should be based upon the importance of IT on financial statement processes, the level of reliance on IT controls, and the IT knowledge of the financial auditor.

Under GAAS, auditors are responsible for gaining an understanding of the control environment as part of the financial audit even if the auditor chooses not to rely on the controls. If IT controls are a material component of the control environment, this understanding should include IT controls as well. The auditor's ability to gain the required level of understanding may vary by the type of controls—general or application—involved in the engagement.

General IT controls include the procedures and processes that support the overall processing of business applications of an organization. These controls include areas such as access to programs and data, data center operations, program development, program changes, IT disaster recovery plans, and the proper segregation of duties of information systems department personnel. The general controls are important because they support application processing. Computerized application controls include the controls involving the processing and storing of business transactions. They ensure the completeness, accuracy, authorization, and validity of processed transactions. Application controls include application security, input controls, rejected-transaction controls, transaction-processing controls, and output controls. According to *IT Control Objectives for Sarbanes-Oxley* (IT Governance Institute, April 2004; available at www.isaca.org), both general and application controls "are needed to help ensure accurate information processing and the integrity of the resulting information needed to manage, govern and report on the organization."

The Panel on Audit Effectiveness recommended the "appropriate involvement of information technology specialists in understanding, assessing and testing the information systems and control activities." As Sid M. Edelstein pointed out ("Sarbanes-Oxley Compliance for Nonaccelerated Filers," *The CPA Journal*, December 2004), financial auditors are more likely to understand application controls than general controls. The general controls tend to be of a more technical nature and often involve operational procedures that accountants are not accustomed to; application controls are less technical. The need for additional IT expertise commonly causes the financial auditor to include an IT audit specialist on the engagement team. Alternatively, without testing the IT environment, in certain audits managers can assess a high control risk with respect to IT. This alternative, however, does not apply to all audit standards, such as the GAO's Yellow Book, where test of controls is generally required.

The presence of an IT auditor on the engagement team does not free the financial auditor from responsibility for assessing the adequacy of IT controls. Accordingly, it is useful for the auditor to have a general understanding of guidance used by IT specialist and of the framework, such as COBIT, in which the specialist performs her conclusions.

To simplify the discussion, guidance for IT auditing from sources familiar to CPAs shall be termed "financial auditing–based standards-setting organizations" (AICPA, GAO, PCAOB, and IFAC). These financial auditing–based standards-setting organizations address topics that are both similar to, and different from, ISACA's COBIT. For example, COBIT includes audit-quality provisions such as a due care requirement, audit planning, and management requirements. COBIT differs from GAAS in its focus on all significant IT processes and controls. These include processes that influence financial processing as well as those that do not. Conversely, GAAS is interested only in IT processes and controls that influence the processing of financial information.

Furthermore, COBIT differs from GAAS in the level of service and in the use of technical language that is particular to IT and IS audits. Financial auditing–based standards clearly define the difference in the type of testing and the level of assurance involved in audit and review engagements. COBIT's framework uses the terms "audit" and "review" interchangeably. For CPAs familiar with GAAS, this may lead to misinterpretation of the level of assurance and type of procedures performed. Accordingly, a financial auditor must maintain a certain understanding of the IT auditor's framework and assess the impact of the IT environment on the scope of the audit and the overall assessment of the control environment. Another example of COBIT's difference from GAAS is the closeness of its guidelines, which are not standards, to the standards. Guidelines elaborate on certain standards (e.g., business continuity). The GAAS hierarchy more clearly defines the relationship between concepts, standards, and guidelines.

As mentioned above, ISACA also provides guidelines and procedures, the majority of which focus on IT technical issues. Examples of guidelines include IT governance, the review of virtual private networks, Systems Development Life Cycle Review, and the use of computer-assisted auditing techniques (CAAT). IS auditing procedures, which provide more detailed steps than guidelines, include IS risk assessment, digital signatures, intrusion detection, viruses, and malicious applications. When relying on an IT or IS specialist, the financial auditor may lack sufficient knowledge to understand specific components of the steps performed by the IT auditor. By understanding and familiarizing themselves with IT controls–based standards, however, financial auditors can understand the nature of the testing performed, and the meaning of the test results in light of the COBIT framework and applicable GAAS standards.

COBIT, PCAOB, and GAO Standards

The bodies that regulate financial, operational, and IT audits or examinations have varying degrees of applicability to the auditor and auditee, depending upon the type of engagement performed. At times, two or more standards apply to an engagement; the standards that apply to one type of audit overlap with the standards that apply to other types of audits or examinations. Although this illustration is not authoritative, it is generally held that the GAO and the PCAOB have similarities in their requirements for risk-based audits, while GAO and ISA auditing standards have little in common.

The goals and challenges of public company auditors have become very visible through the pronouncements of the PCAOB, the auditing regulatory arm of the SEC. When auditing financial information where information technologies have any part in executing, processing, recording, or

reporting the results of a company's activities, these standards remain a high level of guidance for considering the IT environment. The only direct reference to IT in PCAOB Standard 2, "An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements," is that financial auditors should perform a "walkthrough" of the information system to be satisfied with the design and operation of the applicable controls.

Performing an electronic walkthrough is not simple, because of the lack of tangible existence of the results of financial activities. An example of this dilemma pertains to records of disbursement activity. These records exist electronically during the approval, execution, and retention steps in the cycle; however, the effect of each step in a disbursement cycle is simply additional information that electronically modifies the appropriate records. Because the cycle is performed electronically, there is ample room for erroneous or intentional duplications, deletions, and modifications that leave no audit trail. In practice, people using these records attempt to maintain the integrity of the underlying data because of its service to them; the substitute of a human control may be the very weakness of the electronic controls and of the auditor's walkthrough.

To be satisfied with the reliability of the information system, an auditor applying ISACA's COBIT can have a well-rounded set of auditing objectives. These objectives can be applied and tested in the IT environment. The framework starts with audit processes that are broken down to audit objectives (in an order of magnitude of 250). Each audit objective relates to several control activities in a way similar to the COSO framework. Finally, each control activity's impact is marked as primary or secondary to the audit objectives; it is also assessed based on its maturity, a six-level rating that ranges from nonexistent to optimal.

For example, according to the COBIT standards, a control activity that relates to software source code modification is titled "Design Approval" and is defined as: "system development ... should require that design specification for all information system development and modification project[s] be reviewed and approved by management, the affected users ... and senior management when appropriate." This control objective applies to the following control activities and their respective
processes:

Control Activity	COBIT Process
Acquire and maintain application software and activity	Acquire and implement
Install and accredit systems implement	Acquire and implement
Manage changes implement	Acquire and implement
Define and manage service levels	Design and support
Ensure systems' security	Design and support
Manage the configuration	Design and support

Each control activity is associated with a list of impact areas. For example, the primary impacts

of the first control activity above are listed as effectiveness and efficiency; integrity and reliability are listed as secondary impacts. In the case of financial statement audits, the auditor must assess the risk that unauthorized software code modifications may cause material misstatements to the financial statements, and must plan the audit engagement accordingly. Part of this process involves mapping control activities to their impact on financial statement items. For example, the auditor must determine if and how managing program code changes in an accounts payable system influences the accuracy of the accounts payable balance on the financial statements.

In a PCAOB audit or a GAO audit, the auditor then has at his disposal a well-rounded set of control activities (with their recommended associated impacts) to select from, and control objectives that apply to them. An auditor examining internal controls under the PCAOB standards can choose from an extensive list of control activities, and select those that apply. The auditor, considering the particulars of the auditee's IT, can then test the controls to see if they meet the objectives. The IT Governance Institute has published IT control objectives for SOA as a recommended guide to applying COBIT to financial statement audits of public companies. Although this guide is useful to the financial auditor, the PCAOB has not commented on its appropriateness for audits of SEC registrants.

COBIT and GAAS Audits

The closest auditing procedure to the IT walkthrough required by the PCAOB standards can be achieved by performing tests on the IT environment and systems. Such tests are clearly defined and discussed in the COBIT framework and can be suitable for financial audit purposes. At the conclusion of applying tests to the COBIT control objectives, each component in the path of the virtual activities is well examined. This knowledge can then allow the auditor to rely on the results of the virtual activity while performing the IT walkthrough.

Although the GAO standards do not require a walkthrough, tests of control for organization under the Yellow Book auditing standards are required. Tests of controls are mandatory even when control risk is assessed at the maximum. As in PCAOB-regulated audits, when reliance on IT has any bearing on the reporting of the financial statements (as well as efficiency and effectiveness in some Yellow Book audits), the test of controls of the IT environment is required. Because auditing "around the computer" is no longer a viable or relevant option, the application of COBIT in a similar fashion to the one described above could satisfy the Yellow Book requirements for test of controls.

An auditor for a nonpublic company who is not performing a PCAOB or GAO audit can make good use of a selection of audit objectives from the COBIT framework, applying them either to obtain an understanding of internal controls or to test internal controls.

Operational Security and Internal Control Assurance

As summarized in the Exhibit, SAS 55, as amended by SAS 94, applies to the use of a specialist when performing a financial audit that involves material use of the IT environment and also uses IT for testing of controls and substantive testing. As in the GAO and PCAOB audits, COBIT's

processes and objectives allow the IT auditor to concentrate her efforts on audit objectives related to the controls that she tests. The financial auditor, using a specialist that adheres to COBIT, may have a more effective approach to translating the technical manner in which IT documentation and testing is done for control objectives that affect the reported financial information. In PCAOB, AICPA, and GAO audits, the results of such translation (from the technical description to the control objectives narratives) can be the basis of management reports or internal controls' attestations.

COBIT for Consulting Engagements

For nonattest engagements, COBIT and its related ISO 17779 (issued by the International Standards Organization and based on British Standard 17779) can become helpful tools to benchmark the use and policies governing a client's IT environment. ISO 17779 is a reduced set of "best practices" that should be adhered to in a generalized IT environment. Although some ideas are not new—such as business continuity and information security—ISO 17779 organizes these best practices into a coherent policy that can be modified to apply to a particular company. COBIT represents a comprehensive set of control processes, objectives, and activities that can be customized to an entity's needs. COBIT's scalability and comprehensiveness enable it to be part of an engagement that serves an entity's complete IT needs, whether by designing, implementing, or reviewing them. The systematic manner in which COBIT can be presented and used creates the opportunity to deliver an efficient and effective consulting engagement. The added value in subscribing to ISO 17779 or to the ISACA best practices can be helpful in creating effective engagement checklists and proving one's technical ability.

***Joseph B. O'Donnell, PhD**, is an assistant professor at Canisius College, Buffalo, N.Y.*
***Yigal Rechtman, CPA, CFE, CITP, CISM**, is a partner of Person & Company, LLP, CPAs, in New York City. Both are members of the NYSSCPA's Technology Assurance Committee.*