Emerging Technical Standards on Financial Audits:
How IT Auditors Gather Evidence to Evaluate Internal Controls

By Tommie Singleton, Ph.D., CISA, CMA, CPA, CITP

There is little doubt that, over the last five years, an increasing emphasis has been placed on the evaluation of internal controls embedded in computerized systems and information technology (IT).

As a result, auditors have a growing responsibility to understand and evaluate internal controls. This article will provide a brief history of this emphasis and some basic, practical tips on how IT auditors can fulfill their role, duties and responsibilities related to the evaluation of internal controls. Specifically, this article addresses a framework for IT auditors to evaluate internal controls in a broad, general sense—that is, an evaluation of the control environment.

History of Internal Controls Standards and Regulations

Internal controls have been a part of certain laws such as, in the US, the securities acts of 1932 and 1933 and the Foreign Corrupt Practices Act of 1977. Auditing standards from the American Institute of Certified Public Accountants (AICPA) have required an assessment of control risk (e.g., the “audit formula”) for years. Beginning in the 1960s, the evaluation of controls became more complicated as computerized accounting systems became prevalent.

However, the current trend in internal controls really had its origin in the Treadway Commission and the subsequent Committee on Sponsoring Organizations (COSO). The Treadway Commission was charged with developing a strategy or technique that would help to stem the rash of scandals that occurred in the savings and loan industry in the 1980s. The Treadway Commission suggested that the best approach to minimizing these scandals was to develop a comprehensive model of internal controls. The resulting model was promulgated by the sponsoring organizations: American Accounting Association, Financial Executives International, Institute of Management Accountants, Institute of Internal Auditors and AICPA. The resulting model of internal controls has become known as the COSO model.

The COSO model essentially provides a framework to think about, analyze or construct an effective internal control system. The five elements are control environment, risk assessment, communication and information, monitoring, and control activities. In the early 1990s, AICPA adopted the COSO model into the financial auditing technical literature as Statement on Auditing Standards (SAS) No. 78, Consideration of Internal Control in a Financial Statement Audit.

The financial frauds over the next decade brought an even greater emphasis on internal controls. The greatest source of emphasis was the passage of the US Sarbanes-Oxley Act of 2002. Most people would agree that the Act was a direct result of the financial frauds of Enron and WorldCom. Section 404 of Sarbanes-Oxley requires management to do an evaluation of internal controls and financial auditors to opine on that evaluation. In addition, the Act created the Public Company Accounting Oversight Board (PCAOB) as an agency to provide oversight of financial reporting for publicly traded companies and report to the US Securities and Exchange Commission (SEC).

PCAOB is the primary issuer or approver of standards related to financial reporting. The first standard issued by PCAOB accepted all previous financial reporting standards. The second (AS2) dealt with compliance with section 404 of Sarbanes-Oxley. In it, PCAOB recognized the COSO model as an effective means to benchmark and evaluate internal controls.

Later that same year, AICPA issued SAS No. 99, Consideration of Fraud in a Financial Statement Audit. It codified some of the objectives of Sarbanes-Oxley and some of the best practices of the antifraud profession as tools and techniques.

This past year, AICPA issued SAS No. 109, Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement. While the title may not be clear, the subtitle is: “Together with SAS No. 100, supersedes SAS No. 55, Consideration of Internal Control in a Financial Statement Audit.” That is, these two standards constitute the latest technical literature on the subject of internal controls in a financial audit.

Effect of Recent Internal Control Literature and Laws on IT Auditors

No one would argue with the fact that the vast majority of internal controls are embedded in automated systems or IT. Therefore, IT auditors have become a vital part of complying with the standards, guidelines and regulations.

Everyone in the audit world is familiar with the previously mentioned historical events, laws and literature related to internal controls. The Big Four accounting firms and the Fortune 500 companies (publicly traded ones) have employed effective IT audit procedures and IT auditors to comply with these standards and regulations.
However, Sarbanes-Oxley requirements are beginning to “trickle down” to entities other than the large publicly traded companies. Certain industries are beginning to adopt Sarbanes-Oxley requirements even though they are not legally required to do so. In addition, the US Congress has selected certain government agencies, such as the Tennessee Valley Authority, to be subject to Sarbanes-Oxley. Even some international firms have had to make adjustments because of their relationship with a US firm. As a result, it is not uncommon to find audit firms, internal audit departments and managers struggling with compliance, especially the IT audit of internal controls.

The auditing profession has recognized that many of the internal controls of financial reporting are dependent upon software applications and information systems controls. That dependence is especially true for critical monitoring controls (e.g., performance reviews). Therefore, it is increasingly necessary for financial auditors, and especially IT auditors working on a financial audit, to be able to evaluate risks associated with IT, automated controls and the long list of suggestions found in SAS 109.

IT Audits and Best Practices

Evaluating internal controls is a bit like peeling an onion: it happens one layer at a time. An effective strategy is to begin with general and broad areas of evaluation and then narrow the audit procedures to more specific areas. In fact, the COSO model suggests a similar approach, if the elements are treated chronologically. The first element is the control environment. How does an IT auditor know where the risks lie in the control environment, and how does an auditor find effective (recognizable) evidence of a “good” control environment?

From the IT world, there are codified “best practices” in several areas that provide some effective tools. The first is IT governance. IT governance provides principles and tools to assure stakeholders that an entity is making efficient and effective use of its resources in relation to the employment of IT. If that statement is true, a proper evaluation of an entity’s level of IT governance is a good measure of the entity’s control environment. In other words, employment of IT governance best practices raises the level of assurance (comfort) that the systems being employed have effective internal controls and that the control environment is “good.” Evidence of IT governance begins at the board level and/or C-level. For example, an entity is employing at least a piece of IT governance if the board has a standing committee on IT or a standing agenda item on IT at each board meeting. The content of minutes (board’s or IT committee’s) provides relevant evidence as to the effectiveness of the board regarding IT governance. Budgets, policies and procedures, a strategic organizational structure chart that includes segregation of duties, and other documentation can also serve as evidence of effective employment of IT governance best practices.

Nobody should know the risks associated with internal control and material misstatements better than management. Thus, it makes sense to begin the evaluation there. Some of the literature depends on a downward causation effect (e.g., the famous “tone at the top” phrase and meaning). Therefore, the control environment, being so close to management, has a trickle-down effect on other aspects of internal controls (e.g., risk assessment, monitoring).

A second area is the employment of best practices related to project management. Project management best practices are useful in ensuring that projects are delivered on time and within budget and are fully functional as prescribed by the system requirements. Many times, the problem with IT projects is that no criteria exist to define exactly what a project is. The implementation of best practices has an impact on the control environment, again indicating a lower level of risks in system development (and controls embedded therein), and lowers the risk of writing off the cost of failed projects. Evidence exists in the presence of experts (Project Management Professional-certified employees), a project management office and documentation from projects (e.g., Gantt charts, work breakdown structures). An IT auditor can have greater assurance of good internal controls if an entity employs best practices of project management.

Third, the IT auditor would like to see the entity employ system development life cycle (SDLC) best practices. Each of the phases of the SDLC provides documentation, and this documentation is evidence that can be evaluated to determine if the entity is employing best practices of SDLC. The effective employment of best practices of SDLC provides some assurance to the IT auditor that the control environment is good.

Financial auditors might see the latter two areas (SDLC and project management) as essentially the same. For all practical purposes, all projects with significant financial risk are related to application development, application changes and data conversion, and all of these follow SDLC processes. However, the best practices of the two areas are different for evaluation purposes.

IT Audits/Internal Controls and COBIT

This article focuses on a broad or general analysis of IT and internal controls for the control environment level. One way to structure that evaluation is to use Control Objectives for Information and related Technology (COBIT®). Of the four domains, the Plan and Organize (PO) domain is the one most applicable to the evaluation of the control environment.

This domain covers strategy and tactics and concerns the identification of how IT can best contribute to the achievement of the business objectives. It also deals with the fact that the realization of the strategic vision needs to be planned, communicated and managed for different perspectives. Finally, it notes that a proper organization and technological infrastructure must be put in place.

The PO domain includes 10 processes (see figure 1). These processes can serve as a framework to structure the collection of evidence regarding the control environment. The three IT areas of operation mentioned previously can provide evidence for all of the 10 processes. In some of those processes, best
controls embedded in IT in a broad and general sense. That approach should enable the IT auditor to develop an effective approach to analyzing the control environment. IT auditors should be able to control environment with best practices from IT governance, acquired from previous knowledge and to define what lower-environment to start scoping and understanding changes in control environment. Financial audits can use the control 404, SAS No. 109 or AS2, it does attempt to illustrate the internal controls and compliance with Sarbanes-Oxley section purposely limited in its scope of addressing the issues of internal controls from this general view. While this article is purposely limited in its scope of addressing the issues of internal controls and compliance with Sarbanes-Oxley section 404, SAS No. 109 or AS2, it does attempt to illustrate the usefulness of these techniques and tools in the general overview part of that evaluation.

It could be argued that the audit begins and ends with the control environment. Financial audits can use the control environment to start scoping and understanding changes acquired from previous knowledge and to define what lower-level risks are out there and how they should be addressed. Based on an evaluation of IT governance, project management and/or SDLC, the IT auditor can accumulate evidence to determine if the control environment is a good one. However, a good control environment does not necessarily mean that any internal controls are built into the systems. Instead, it is a general indicator that the entity has decided to follow these best practices, which usually implies thorough thoughtfulness in other areas of IT, such as the effective inclusion of internal controls—that is, there is usually a downward, positive effect on the controls embedded in IT processes below the higher control environment level.

Other aspects of COSO, COBIT and detailed tests of controls will provide additional evidence about the assurance of internal controls.

Endnotes
1 The IT Governance Institute® (ITGI™) is a leader in IT governance. For more information, please visit the ITGI web site at www.itgi.org.
2 The IT Audit Basics column from volume 5, 2006, of the Information Systems Control Journal features the subject of project management risk. Please refer to it for more information on risk assessment and the relationship between project management and the evaluation of internal controls.
3 The IT Audit Basics column from volume 1, 2007, of the Information Systems Control Journal is a complete article on the subject of SDLC. Please refer to it for more information on how to use SDLC as a means to evaluate internal controls.

Tommie W. Singleton, Ph.D., CISA, CMA, CPA, CITP
is an associate professor of information systems at the University of Alabama at Birmingham (USA), Marshall IS Scholar, and director of the Forensic Accounting Program. Prior to obtaining his doctorate in accountancy from the University of Mississippi (USA) in 1995, Singleton was president of a small, value-added dealer of accounting information systems using microcomputers. In 1999, the Alabama Society of CPAs awarded Singleton the 1998-1999 Innovative User of Technology Award. Singleton is the ISACA academic advocate at the University of Alabama at Birmingham. His publications on fraud, IT/IS, IT auditing and IT governance have appeared in numerous journals, including the Information Systems Control Journal.