How the IT Auditor Can Make Substantive Contributions to a Financial Audit

IT auditors have been making contributions to financial audits almost since the beginning of the IT age, when entities other than governments began to use computers for financial-related business processes. In fact, some of the initial IT auditors were pioneers in creating most of the techniques and procedures they used—many of which have become commonplace, e.g., using IT as an audit tool (reconciling inventory to digital records), segregation of IT duties, integrated test facilities (ITFs), and generalized audit software (also known as computer-assisted audit tools/techniques [CAATs]).

Over the years, financial audit technical literature has added to the importance and need for IT auditors in financial audits, e.g., Statement on Auditing Standards (SAS) No. 94, “The Effect of Information Technology on the Auditor’s Consideration of Internal Control in a Financial Statement Audit.” Obviously, the US Sarbanes-Oxley Act of 2002 also increased the importance of IT auditors in financial audits, especially in assessing controls and integrating the results into a risk-based approach (RBA) audit for publicly traded entities. But, the adoption of the risk-based standards (SAS No. 104-111) in 2006 probably increased the importance of and need for IT auditors more than any other previous standard or event since the advent of the computer into businesses.

This article describes some of the key contributions IT auditors can make in a financial audit. These potential benefits should be reasons to make sure that IT auditors are utilized to the fullest potential possible in financial audits.

TESTS OF CONTROLS

The first contribution is a traditional one, tests of controls (ToC). When the financial audit team plans to rely on one or more controls, those controls need to be tested for assurance that they are operating effectively and were throughout the financial period. Today, that usually means an automated control and, thus, the need for an IT auditor (e.g., a Certified Information Systems Auditor® [CISA®]).

There are some keys to effective employment of ToC that IT auditors need to know and understand. First, there is a high potential benefit to use ToC when an automated control exists whose purpose is essentially the same as the audit objective for some further audit procedure (i.e., they overlap). When this situation exists, there is a potential to gain efficiencies (e.g., less labor) and effectiveness (e.g., testing at 100 percent). Second, if ToC are to be done, the IT auditor must have sufficient assurance of the effectiveness of IT general controls. Third, the risk-based standards require that the relevant IT controls were designed properly and implemented. The IT auditor will need evidence to that effect, which should be in the results of the risk assessment phase of the financial audit. One last important point: It is possible, under the right circumstances, for the IT auditor to conduct a test of only one transaction and be in compliance with technical literature (both the Public Company Accounting Oversight Board [PCAOB]’s Auditing Standards and American Institute of Certified Public Accountants’ SAS).

The specific nature of ToC varies, but could include the need to process a transaction on the operational system (often impractical), obtaining a copy of the software and testing the control on one of the enterprise’s computers (difficult if the software is not a common commercial product), testing in a staging area, or some other effectual process.

CAATS

The use of CAATs is, of course, another traditional and fairly frequent activity for IT auditors in a financial audit. The use of CAATs is often associated with data mining (extracting data) and data analysis. Data analysis is usually associated with either gathering evidence or tests for certain audit objectives (e.g., testing for certain anomalies).
Perhaps no other tool or technique is as valuable to the IT auditor as CAATs. It is also important to note that CAATs continue to advance in their capabilities and functionality. For instance, in the last few months, several CAATs are now able to read PDF files/digital documents and reliably parse data in the extraction process.

It is, therefore, important for IT auditors to develop sufficient skills and abilities using CAATs in order to be positioned to provide maximum benefits to an audit. It auditors need to know the CAATs available in the market, evaluate the needs of the audit, and find an effective fit for the combination of tools and audit objectives.

**SUBSTANTIVE IT-RELATED PROCEDURES**

Substantive IT-related procedures are closely associated with CAATs. They can be used to support, complement or replace substantive procedures for further audit procedures. It is not uncommon for an experienced IT auditor to brainstorm with the audit team as the audit plan and further audit procedures are being developed and for the IT auditor to recognize the opportunity to gain efficiencies or effectiveness by including an IT-related procedure.

It could be as simple as using a CAAT to generate sample data for substantive testing. There have been reports of significant labor reduction by using this technique alone.

It can, of course, be more sophisticated. For example, the IT auditor may suggest a substitution for manual substantive procedures related to subsequent events on testing liabilities. Specifically, the IT auditor could extract all bills paid in the first month of a new fiscal year, use the data set of invoices that were recorded in the prior month (fiscal year being audited) and identify any liabilities that were not recorded properly. The traditional process normally involves hours, even if there is a cutoff amount, of pulling invoices and tracing/auditing transactions. In addition to a likely reduction in labor, this IT approach tests 100 percent of the transactions.

**VALUE-ADD MANAGEMENT COMMENTS**

The benefit of management comments can be overlooked or misunderstood. While IT auditors need to scope their efforts to the risk of material misstatement (RMM) and financial audit in the process of evaluating controls in the risk assessment phase or in conducting procedures in the further audit procedure phase, IT auditors will likely discover something “broken” in the IT space that management would likely want to “fix.” In particular, it seems that security-related issues arise in many audits. It is also likely that should the audit team point out to management a security risk, even one that is irrelevant to the RMM, management will be grateful to have been informed.

For instance, in an entity with excellent access controls at the application level and at the server/network level, but poor controls at the perimeter, it is likely that the IT auditor and audit team would decide the perimeter weakness is irrelevant for financial audit purposes because the access controls closer to the data in the two other areas compensate for the perimeter weakness. However, management would probably appreciate being informed of the nature of that exposure and of any recommendations to mitigate the perimeter risk. These types of comments do add intangible value to the audit.

Because of the nature of IT comments, it usually takes an IT auditor to recognize these opportunities for value-add management comments. Therefore, the IT auditor needs to become an auditor “surgeon” in evaluating the IT space—carve out what is relevant, make a contribution to the audit and leave the rest out—but, simultaneously, examine both parts for potential value to the client via management comments.

**INTEGRATED AUDIT**

IT auditors can often see opportunities for the previously identified benefits of their participation, which financial auditors (without an IT background) may not be able to identify. In fact, some IT auditors have the reputation of always adding value to an audit because of their ability to provide some of the benefits listed previously. Regardless, the IT auditor can always contribute to the financial audit by bringing an accurate assessment of the RMM, inherent risk associated with IT and control risk.

The RBA auditing standards describe a process whereby auditors take a rigorous approach to accurately identifying
the level of risk in account balances, classes of transactions and disclosures. That is, each aspect is evaluated on its own level of risk with no preaudit assumptions. Then, for those aspects with a high RMM, the audit team develops relatively high-powered tests; for moderate risk, moderate power tests; and for low risks, low tests (i.e., the RBA standards require an alignment of risk with the nature, timing and extent [NTE] of further audit procedures). The assumption in the RBA is that the audit team will start with a clean slate each year, albeit prior audits and other information are key to the audit planning phase. A process that insulates or ignores the work of IT auditors in the risk assessment phase, or that overlooks the risk assessment report, clearly violates the spirit of the RBA standards. Therefore, the IT auditor needs to make every available effort to be engaged and involved with the audit planning phase, and to bring evidence, conclusions and information about controls and risks to that process, in order to end up with the optimal audit plan.

The PCAOB is emphatic on this subject: It is one audit, not two.

CONCLUSION
This article attempts to describe some of the major benefits an IT auditor can bring to a financial audit. These benefits include tangible ones, such as labor savings, and intangible ones, such as audit quality and value-add management comments. The list is not intended to be exhaustive, but is illustrative and contains the more common benefits. Generally speaking, IT auditors will want to become familiar with these areas of opportunity to make themselves valuable partners in financial audits and to purposely develop their skills in these areas. Obviously, a key to being successful in these areas is to be persuasive and articulate in presenting these possibilities to audit partners and managers.

ENDNOTES
2 Created by the US Air Force. An article on the subject was published by USAF in 1961.
3 The ITF concept was created by William Perry at Kodak. ITF is a phony business unit embedded in the entity’s systems in which transactions do not affect legitimate financial transactions. Today, a staging area serves the same purpose, but is not embedded in live systems.
4 The seminal tool was AUDITAPE, introduced in 1967 and developed primarily by Ken Stringer of Haskins & Sells.
6 A staging area is a special location where the entity’s system is simulated offline for testing purposes.
7 See Singleton, Tommie W.; “Data Extraction, A Hindrance to Using CAATs,” *ISACA Journal*, vol. 6, 2010, for more information on this key step.
8 The *ISACA Journal* regularly publishes effectual articles on CAATs, and therefore this section does not go into details about how to use CAATs. It merely addresses the high value CAATs have in financial audits in general. For additional information, see ISACA’s IT Audit and Assurance Guideline G3 Use of CAATs, [www.isaca.org/standards](http://www.isaca.org/standards).