General Auditing for IT Auditors

Danny M. Goldberg, CISA, CGEIT, CIA, CPA, is the professional development practice director at Sunera, an international advisory services firm. Prior to joining Sunera in January 2011, he founded SOFT GRC, an advisory services and professional development firm. Goldberg has more than 14 years of audit experience in the Dallas Fort Worth (Texas, USA) area, including five years as a chief audit executive (CAE)/audit director at two diverse companies. He has the rare experience of being an integral part of, or leading, year-one US Sarbanes-Oxley Act compliance efforts at three companies. Additionally, Goldberg has assisted in leading the establishment of three internal audit/ US Sarbanes-Oxley Act departments.

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article, and choose the Comments tab to share your thoughts.

At times, there seems to be a disconnect between the internal audit and IT audit professions. In terms of assessment of risk, coordination, integration of audit approaches, etc., there is an inherent gap in the approaches of each profession. This gap is very evident, and a general lack of understanding where IT audit fits into the overall audit process is a problem with the segregation of audit approaches.

As companies continue to struggle with the recession, auditors seem to be on a permanent diet—auditors are stretched thin. As the field continuously evolves, chief audit executives (CAEs) will continue to look for cross-trained auditors—those who have the ability, training and experience to perform financial, operational and IT audits, possibly even simultaneously. Furthermore, the industry seems to be tending toward integrated, cross-trained IT and general audit teams. Thus, all IT auditors should understand the process and be able to increase their contribution to the overall audit approach.

This article focuses on the general (i.e., financial, controls and operational) audit process, where IT fits into this process and how to bring it all together.

THE ROLE OF IT AUDIT

The primary role of the internal IT audit staff is to independently and objectively assess the controls, reliability and integrity of the company's IT environment. These assessments can help maintain or improve the efficiency and effectiveness of the institution's IT risk management, internal controls and corporate governance. Internal auditors should evaluate IT plans, strategies, policies and procedures to ensure adequate management oversight. Auditors should make recommendations to management about procedures that affect IT controls.[1]

FINANCIAL, OPERATIONAL AND COMPLIANCE AUDITING

IT auditing plays an integral role in financial, operational and compliance auditing; however, the purpose of each approach is different, as explained in the following sections.

Financial Auditing

A financial audit, or, more accurately, an audit of financial statements, is a review of an enterprise's financial statements that results in the publication of an independent opinion on the relevance, accuracy, completion and fairness (RACF) of the presentation of the financial statements. Internal audit does not opine on the company's financial results, but performs substantive tests on financial balances to verify RACF. Through substantive auditing, auditors gather evidence of the completion, validity and/or accuracy of account balances and underlying transaction classes. Confirmation of cash balances, vouching (going from the general ledger to the invoice/proof of purchase) additions to the fixed asset ledger and review of compliance with debt covenants are all examples of substantive testing.

IT auditing is an integral part of this audit approach. The audit team analyzes, reviews and tests the systems; passing the tests decreases the audit's associated risk. A dependable system encourages the auditor to feel confident in its processes and procedures; the numbers become more reliable.

Operational Auditing

Operational auditing is the process of reviewing a department or other unit of a business or governmental or nonprofit organization to measure the effectiveness, efficiency and economy of operations. It is an evaluation of management's performance and conformity with policies and budgets. In this approach, the enterprise and its operations are analyzed, including appraisal of structure, controls, procedures and processes. The objective is to appraise the effectiveness and efficiency (E&E) of a division, an activity or an operation of the entity in meeting organizational goals.

In today's challenging economic environment, operational auditing is becoming more and more important. Why? Operational auditing, as described here, reviews a process for E&E that can be a great asset to a company, allowing internal audit to be viewed as a revenue generator/cost reducer rather than an overhead cost.

When assessing the E&E of a process, it is important to review the IT systems. An antiquated system can significantly affect E&E. Furthermore, nonoptimized system usage hampers the process's efficiency. For example, if an enterprise installs a new cost management system, but does not activate all the system's control enhancements, the process will remain manual and inefficient.

Compliance Auditing

A compliance audit is a comprehensive review of an organization's adherence to regulatory guidelines. What is examined in a compliance audit will vary depending upon whether an enterprise is a public or private company, what kind of data it handles, and whether it transmits or stores sensitive financial data. For instance, US Sarbanes-Oxley Act requirements designate that the entity must utilize an IT control framework (e.g., COBIT) as a foundation for IT systems and processes. Health care providers that store or transmit electronic health (e-health) records, such as personal health information, are subject to US Health Insurance Portability and Accountability Act (HIPAA) requirements. Financial services companies that transmit credit card data are subject to Payment Card Industry Data Security Standard (PCI DSS) requirements.[2]

IT auditing plays a significant part in compliance auditing. As previously indicated with financial and operational auditing, IT controls and processes are part of compliance, and these pieces are integrated into the overall compliance plan. IT audit must be involved in all facets of compliance auditing.

DIFFERENCES IN APPROACH

The main differences among financial, operational and compliance auditing are:

- The purpose of the audit
- Inclusion of nonfinancial areas
- Cost/benefit vs. verification

As stated previously, the purpose of each audit varies greatly. Financial auditing verifies that the numbers in the financial statements are reported accurately. Compliance auditing reviews adherence to regulations and rules. Operational auditing reviews processes for E&E. In most cases, compliance and operational auditing are pretty much the same process, but operational auditing takes the next step and focuses on E&E. Financial audits, as their name denotes, focus on an enterprise's financial results. On the other hand, compliance and operational audits can focus on hidden numbers and costs that could be reduced—once more demonstrating a strict focus on adherence, efficiency, effectiveness and improvement of the process. In a nutshell, financial audits focus on verification of the reported numbers, operational audits focus on cost vs. benefit, and compliance audits focus on strict adherence to rules and regulations.

ASSESSMENT OF RISK

The audit[3] risk assessment[4] is the stage in the audit planning process in which an auditor[5] determines the likelihood of audit risk.[6] This, in turn, is defined as the possibility of recording an inappropriate opinion on an audit because of a misstatement in the documents examined. An audit risk assessment is the beginning piece used to manage the integrity of an audit and to determine when and how audits should be conducted and by whom.

The IT component is an integral part of the assessment. Either a separate IT assessment or, more appropriately, an integrated assessment, should be completed. The IT component can significantly drive the overall assessment.

In terms of financial auditing, the key financial system's reliability directly, with an inverse relationship, affects the amount of testing necessary. The more reliable a system, the less testing (both IT and general) is necessary. Conversely, in unreliable systems, a significantly greater amount of testing is necessary. If the IT general controls for a system are not reliable, all of the controls must be substantively tested. For example, if access security cannot be relied upon, all access to the system must be tested throughout the year.

IT plays a key role in the assessment of risk both in the planning stage of the audit year and in each audit. With a more reliable system comes less inherent risk in the audit. Additionally, during the preliminary work of an audit, IT contributes to a deeper, more specific review prior to fieldwork.

PRELIMINARY WORK

Basically, preliminary work is everything that the audit team does to set the foundation of the audit and prepare for an efficient and effective audit process. Preliminary work includes the following steps:

1. **Audit objectives**—Determine the reason(s) for performing the audit and the specific goals that the enterprise intends to meet.
2. **Knowledge gathering**—Gather any knowledge relevant to the audit, including prior-year audit files, policies and procedures, narratives, and audit reports issued.
3. **Authoritative research**—Refer to relevant knowledge on the subject matter of the audit in general, including guidance from ISACA and The Institute of Internal Auditors (The IIA), industry guidance, and best practices on the area under review.
4. **Management interviews**—Conduct interviews to garner the scope and assist in creating the risk assessment for the audit; this is a key part of preliminary work.
5. **Internal controls**—Identify current internal controls; this is important to establish a control baseline for the area/division under review.
6. **Walk-throughs**—Take a sample through the process under review to determine whether the process is functioning as intended; walk-throughs are integral to verifying controls and process details.
7. **Preliminary risk analysis**—Develop this through all of the previously mentioned steps; this guides the audit as to where resources should be focused.

Throughout the preliminary work, IT plays an integral role in the assessment of risk. Many auditors separate general and IT audits, a practice that is hard to comprehend. The preliminary process should be completed concurrently for both audits, as the steps can significantly overlap. Regardless of the audit type, all of the steps of preliminary work are necessary for each, either separately or as an integrated audit approach. Excluding IT from a general audit or *vice versa* would limit the knowledge of the audit and audit process and, consequently, limit the effectiveness of the audit approach.

> "Regardless of the audit type, all of the steps of preliminary work are necessary."

AUDIT FIELDWORK

As discussed previously, IT audit and general audit must work hand in hand with each other to complete an efficient and effective audit. The main area in which this will occur is during audit fieldwork.

Audit fieldwork is the process of actually performing the audit. This includes:

- Requests for documents
- Additional and more in-depth interviews
- Completion of audit work program steps (testing)
- Documentation of audit work
- Supervisor review

Audit fieldwork is arguably the most important step of the audit process. This is the step in which the actual work is completed, conclusions are created and supported, and the substance behind the audit report is completed.

Once more, the fieldwork for both the general audit and IT audit should be completed concurrently because there is overlap in the areas and because issues identified could affect the audit approach. In many cases, general auditing and IT auditing are not completed concurrently. For example, if security on a key system is tested and deemed ineffective, substantive procedures may have to be conducted to verify that significant issues or findings did not occur.

CONCLUSION

The world of auditing is moving toward a more integrated approach to the internal audit. The importance of a comprehensive approach to auditing and of auditors becoming

more well rounded and learning all facets of the audit process will continue to be key to departmental and personal growth.

IT auditors should continue to further their ability to conduct general audits and financial, operational or compliance audits. As the industry continues to evolve, the strict line between audit specialties will continue to dissolve because separating each audit approach is neither efficient nor effective. An integrated audit approach will help all types of audit teams gain effectiveness as each audit plays off the other. Accordingly, all auditors should continue to enhance their skill sets and step out of their comfort zones. This will make for better auditors and give these professionals the experience to conduct better audits.

ENDNOTES

[1] Federal Financial Institutions Examination Council (FFIEC), "Audit Booklet," *Information Technology Examination Handbook*, USA, 2003, *www.ffiec.gov/ffiecinfobase/booklets/audit/audit.pdf*

[2] *SearchCompliance.com*, "What Is a Compliance Audit?," 15 January 2009, *http://searchcompliance.techtarget.com/definition/compliance-audit*

[3] Smith, S.E.; "What Is an Audit?," wiseGEEK, *www.wisegeek.com/what-is-an-audit.htm*

[4] Crystal, Garry; "What Is Risk Assessment?," wiseGEEK, *www.wisegeek.com/what-is-risk-assessment.htm*

[5] Tatum, Malcolm; "What Is an Auditor?," wiseGEEK, 19 January 2011, *www.wisegeek.com/what-is-an-auditor.htm*

[6] Sernel, Kimberly; "What Is an Audit Risk?," wiseGEEK, *www.wisegeek.com/what-is-an-audit-risk.htm*