What Every IT Auditor Should Know About Scoping an IT Audit

Tommie W. Singleton, Ph.D., CISA, CITP, CMA, CPA, is an associate professor of information systems (IS) at the University of Alabama at Birmingham (USA), a Marshall IS Scholar and a 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 IS using microcomputers. Singleton is also a scholar-in-residence for IT audit and forensic accounting at Carr Riggs Ingram, a large regional public accounting firm in the southeastern US. 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 articles on fraud, IT/IS, IT auditing and IT governance have appeared in numerous publications, including the *ISACA Journal*.

One of the great things about a career in IT audit is the number of different ways those skills can be applied. As a part of the internal audit function, IT auditors audit the IT portfolio of an entity. The larger the entity, the more diverse and interesting the "IT space,"[1] and the more different types of audits an IT auditor can perform. As a part of a public accounting firm, IT auditors audit the portion of IT space related to financial reporting, in a variety of businesses, which should be interesting and, undeniably, is great experience. That would include, for publicly traded companies, US Sarbanes-Oxley Act section 404 audits of controls and, for all entities requiring financial audits, IT controls over financial reporting. An IT auditor may also work as a forensic specialist (cyberforensics) where the objective is usually directed toward potential crimes or nefarious deeds. For example, cyberforensic specialists might work for a public accounting firm or forensic accounting firm, and be responsible for fraud cases where they seek evidence in digital form. Or, a cyberforensic specialist might do the same thing for a government or law enforcement agency, for example, both the US Federal Bureau of Investigation (FBI) and US Office of Inspector General (OIG) use such specialists. There are, of course, many other ways to use the skills, knowledge and abilities associated with IT audit, including consulting and executive management (e.g., CIO).

This article focuses on the difference in IT scope between the first two perspectives, and especially looks at IT audit from the external audit perspective. One of the flaws young IT auditors make is to not recognize a distinction between IT audit in a financial audit vs. IT audit of IT (usually from the internal audit function or consulting), and that usually results in an improper scope of IT in a financial audit, generally on the excessive side.

IT AUDIT OF IT: APPLYING IT AUDIT PRINCIPLES AND PRACTICES

The difficulty in scoping IT in an external audit arises from the fact that an effective IT auditor needs to know a lot about the IT space and its components. This includes a sufficient list of best practices, benchmarks, prescriptive states and models associated with each of those components, and a sufficient knowledge of a variety of technologies (i.e., a need to be an expert in computers and technologies). For instance, IT auditors are knowledgeable about systems development life cycle (SDLC), IT governance, project management, access controls/IT general controls (ITGC), networks, software and business continuity (disaster recovery). As an example, in the case of the latter, IT auditors need to know all of the multiple points or benchmarks that need to be tested: the written plan, assignment of duties, offsite storage of data backups, facility backup, supplies backup, O/S backup, application backup, rank order of restoring applications and data, copies of technical manuals, testing the plan, and documenting the test. IT auditors generally are trained to perform procedures related to those best practices, such as a review of documents (the plan, job assignments, test results, etc.); inquiries of key personnel; reperformance (data restoration); and a verification of the backup facility, supplies, technical manuals, O/S, applications, etc., in an IT audit of IT.

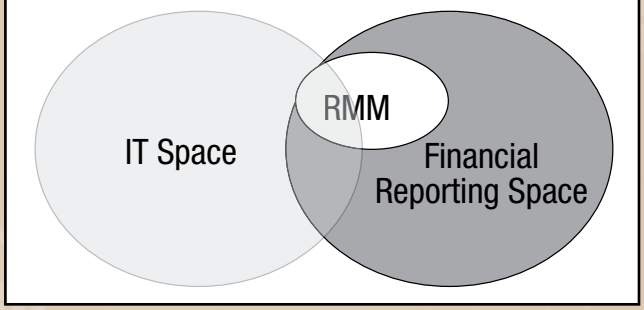
If the context of the IT audit is audit of IT for IT sake, be it internal or consulting, and assuming the entity has a large and/or highly complex IT space, the previously outlined full set of testing points is applicable. The same kind of thing applies to IT audits of virtual machines, information security, and a host of other aspects or components of IT space. IT auditors are aware that ISACA's CobiT® is the leading model and tool in assisting IT auditors in these kinds of audits. But what if the context is a financial audit? Does anything really change?

IT AUDIT IN A FINANCIAL AUDIT: APPLYING RISK-BASED AUDIT PRINCIPLES

IT auditors will be tempted in a financial audit to want to use all useful knowledge in performing their duties. If IT auditors are not careful, they will overdo it—i.e., perform a relatively excessive number of procedures and tests—because it is the nature of IT auditors to be thorough in applying their specialized knowledge and skills. IT auditors sometimes struggle with a proper scope in the IT audit portion of a financial audit and do not realize they have developed an excessive set of procedures. An excellent way to ensure that the scope is proper, not too little and not too much, is to apply risk-based audit (RBA) principles, rather than solely relying on the prescriptive states or best practices of that area.

A RBA begins by defining the financial reporting space (see **figure 1**). What manual and automated systems are used in financial reporting? What accounts, classes of transactions and disclosures are associated with financial reporting? What processes, manual and automated, occur in the financial reporting cycle?

Figure 1—Scoping IT Audit in a Financial Audit



Then there needs to be an assessment of the IT space to determine precisely what components are relevant. It can be tempting to begin the audit without a conscientious effort to examine and define the relevant space, and just do IT audit based on some other premise (habits, past audit procedures, personal judgment, etc.). The simple truth is not all of the IT space is relevant to the financial audit. The only part of the IT space that is relevant is that part that overlaps with the financial reporting space (see **figure 1** where the two Venn circles overlap). From a practical standpoint, it would include identifying all of the data associated with financial reporting and all IT related to capturing, processing, storing or transferring those data; these components would be relevant.[2]

But that is just the first crucial step in a proper scope of IT in a financial audit. It is limited a second time by the risk of material misstatement (RMM). RMM is defined in the AICPA's risk-based standards for nonissuers (SAS No. 104-111), and the principles therein are referred to as RBA.[3] The RMM includes control risk (CR) associated with IT and inherent risk (IR) associated with the entity in various ways (e.g., ITGC). Basically, the IT auditor's responsibility is two-fold: (1) to determine what risks exist as a result of the effect of IT on financial reporting, and (2) to identify risks (i.e., RMM) associated with controls embedded in IT. If an entity develops its own software applications, and one of those applications processes the financial reports, then risk is introduced into financial reporting as a result of something in the IT space—the development of that software application.

But the question becomes, is that risk relevant? It is relevant if the risk leads to RMM. If not, it is irrelevant. For example, IT auditors are concerned about firewalls when internal systems are connected to the gateway that leads to the Internet. Since systems associated with financial reporting are connected to the Internet, this part of the IT space overlaps with the financial reporting space. But if access or other controls exist around the financial reporting data, and those controls have been tested and found to provide adequate assurance of integrity, the firewall becomes irrelevant and not necessary to test (that is, although it lies on the first overlap, it does not lie within the RMM overlap). If good access controls exist on the layer above the financial reporting data (application controls or access controls), many things on the perimeter become irrelevant. So the overlap of IT space and financial reporting space is further constricted by the overlap of the RMM space. That overlap is based on the level of risk associated with the IT space and the RMM in the financial reporting space (i.e., it could lead to a material misstatement, or put another way, it has a high level of assessed risk).

RBA requires the IT auditor to consider the appropriate level (inclusion) of the subspace in the financial audit plan, which could lead to a reduction of the amount that is relevant. This reduction of the IT space component is very different from the audit of IT for IT's sake. There one would include all of the subspace associated with the object.

There is one last issue about the Venn diagram and proper scoping of IT. It is the issue of scope based on sophistication of IT.[4] The size of the overlap ring or area between financial reporting space and IT space will be greater the more

sophisticated the IT space becomes; the larger the overlap, the larger the scope of IT procedures necessary and *vice versa*.

AN EXAMPLE

For example, if a midsized business uses Microsoft Dynamics, and has a few servers and US $25 million in revenues, that entity has a different level of IT sophistication from that of Coca-Cola, a global company using an enterprise resource planning (ERP) system, with billions of dollars in revenues. In the first instance, an overlap certainly exists, but obviously the IT auditor will have less to do in that scenario than in the second (Coca-Cola).

In the first scenario, the IT auditor will not need to spend a lot of effort testing the software because it is commercial software that has been around for years. At most, the IT auditor would see if a relatively current version is being employed. In the second scenario, even though it is commercial software, the level of sophistication would most likely introduce some level of risk associated with software that is greater than the first scenario. So the IT auditor would likely do some testing different from tests conducted in the first scenario, for example, change management testing, even if it is limited to changes in the configuration of the ERP system. Regardless, the (size of) overlap between IT space and financial space would be greater in the second scenario because of the difference in the level of IT sophistication.

If the audit objective is business continuity in both scenarios, then, in the first case, the scope or extent of what the IT auditor would do, generally speaking, would be significantly less than in the second case because of the difference in the level of IT sophistication.

A third scenario exists where the difference becomes dramatic. Suppose the client is a small company with US $2 million in revenues, a single server, 15 workstations, using only commercial software. What would the IT auditor do regarding business continuity? Certainly the testing (reperformance) of backup data becomes irrelevant because of the low level of IT sophistication. Thus, in this case, the IT auditor may make inquiry of key personnel about data backups and such, and may make an independent verification that data backups are made regularly and stored safely offsite (observation or inquiry). This scope of procedures matches the level of risk (RMM) associated with IT and this business entity; based on RBA and a risk assessment, the level of risk associated with business continuity is low so the level of test to be performed should be low. In the case of Coca-Cola, if the ERP fails, then IT introduces a significant risk to the financial reports. Therefore, the assessed level of IT-related risk (RMM) and the IT sophistication are far greater than with the small client, in which case it is appropriate to develop a much more sophisticated set of procedures (i.e., high RMM requires high level of test).

CONCLUSION

When IT auditors are functioning in the role of financial audit, they must be careful to develop an appropriate scope of IT audit. That scope is affected by (1) the degree of overlap between the financial reporting space and IT space; (2) the degree of IT sophistication, which affects the size of the overlap; and (3) the overlap of RMM and the IT space. In one respect, the outcomes are common-sense decisions that do not compromise compliance with auditing standards. In reality, it is the conscientious, deliberate application of RBA principles to the client at hand. That is, a proper assessment of the level of risk drives the nature, extent and timing of further audit procedures (IT tests of controls in particular) and, more important, helps determine which ones even exist. A proper assessment of risk not only leads to a more effective audit (high risks are assigned high tests) but also could lead to audit efficiencies. The scope of the IT audit portion of the financial audit is only as large as it needs to be, and not unintentionally too large.

ENDNOTES

[1] The author is using the term “IT space” to refer to all components of IT within the entity. IT governance refers to the same thing as does the IT portfolio. The term “IT space” is meant to cover all aspects of technologies and systems within an entity.

[2] For additional information, see the IT Audit Basics column in volume 2, 2009, related to this subject; in a financial audit, it is all about the data.

[3] Public Company Accounting Oversight Board (PCAOB) is working on a compatible set of standards for issuers.

[4] Statement on Auditing Standards (SAS) no. 94 (“The Effect of IT on the Auditor’s Consideration of Internal Control in a Financial Statement Audit”), superseded by the RBA standards, made this same distinction about IT sophistication and stated that it was not size of entity that mattered but the level of sophistication of the IT.