Auditing the IT Auditors

Every time an IT auditor engages in an IT audit/assurance project, at least one person reviews the work. The audit profession in general has developed structures and processes to make sure audits and similar projects are subject to an appropriate degree of review before being released to the sponsor. That process often involves multiple layers of review. The more risk associated with the project, the stricter the review process becomes and the more layers the structure contains.

The review process is designed to make sure the final product is appropriate given the original request, the results of tests and procedures, and technical literature and guidance on the subject matter. Tenure is important for a quality review to occur, and naturally requires a level of skill and knowledge to perform. The bottom line is that someone who is a subject matter expert (SME) in terms of the type of IT audit being performed will be the reviewer. Thus, for a Payment Card Industry (PCI) audit, the reviewer is likely to be certified Payment Card Industry Data Security Standard (PCI DSS), have years of experience, and be knowledgeable of technical literature and guidance on PCI audits. For a financial audit, the reviewer is likely to be a partner who is knowledgeable about IT, knows the client, knows the technical literature and guidance, and has years of experience.

Everyone involved in the project wants a quality review done internally prior to being released. The questions addressed herein are: What should an IT auditor new to the profession expect in terms of the type of IT audit being performed will be the reviewer. Thus, for a Payment Card Industry (PCI) audit, the reviewer is likely to be certified Payment Card Industry Data Security Standard (PCI DSS), have years of experience, and be knowledgeable of technical literature and guidance on PCI audits. For a financial audit, the reviewer is likely to be a partner who is knowledgeable about IT, knows the client, knows the technical literature and guidance, and has years of experience.

The first thing to understand about the review process is that the structure and process are highly correlated with risk. That is, the more risk associated with an IT audit project, the higher the level of scrutiny in the review process and the higher the likelihood of multiple layers of review. Therefore, if a project has a lot of risk associated with it for one reason or another, the IT auditor knows up front that the project will be reviewed more closely and probably by more professionals than otherwise.

Sometimes the type of entity drives that same intense review. Audits of financial institutions, larger entities (e.g., publicly traded companies) or entities highly dependent on IT are often considered in need of a higher level of review.

A level of importance based on other issues may also lead to a higher level of review. For instance, an internal audit of the entity’s perimeter for a high-profile organization could be seen as vitally important in today’s environment and, thus, may lead to a higher level of review.

Generally speaking, even entry-level IT auditors have a sense of this elevated need for review and recognize a project that is likely to take on that process. If risk is relatively high, more caution is needed in tests and procedures, documentation and work papers, and communications and reporting.

SCOPE AND RISK

The first thing to understand about the review process is that the structure and process are highly correlated with risk. That is, the more risk associated with an IT audit project, the higher the level of scrutiny in the review process and the higher the likelihood of multiple layers of review. Therefore, if a project has a lot of risk associated with it for one reason or another, the IT auditor knows up front that the project will be reviewed more closely and probably by more professionals than otherwise.

Sometimes the type of entity drives that same intense review. Audits of financial institutions, larger entities (e.g., publicly traded companies) or entities highly dependent on IT are often considered in need of a higher level of review.

A level of importance based on other issues may also lead to a higher level of review. For instance, an internal audit of the entity’s perimeter for a high-profile organization could be seen as vitally important in today’s environment and, thus, may lead to a higher level of review.

Generally speaking, even entry-level IT auditors have a sense of this elevated need for review and recognize a project that is likely to take on that process. If risk is relatively high, more caution is needed in tests and procedures, documentation and work papers, and communications and reporting.

RELEVANT AREAS FOR IT IN A REVIEW

A review obviously covers many aspects of the project/audit other than those that are IT-related. The general (non-IT) aspects include planning, technical proficiency of the team members, sufficient independence, methodology and using the work of others, among others. The areas in a review that can be related to IT are described in the following sections.

Technical Training and Proficiency

IT members of an audit or project are treated the same as others in terms of assessing an adequate level of technical abilities and proficiency sufficient for a particular project. One of the differences is the number of subsets of IT that exist and the need to have experts in them from time to time.
For instance, a medium-sized company could be employing e-commerce via a web site, using a service organization to take care of payments (subject to PCI compliance and federal and state laws), using cloud services and involving a host of other IT-related influencers. These present the need for several specialty areas of IT that could arise for this single entity.

A second issue is the need to keep skills and abilities adequate and up to date. It goes without saying that once a person chooses to be in the IT audit profession (or any other IT profession), the person is committed to life-long learning. IT changes so rapidly that a person’s skills and abilities can become obsolete in a few years. Thus, one aspect of assessing risk for the IT function in an entity is the level of training and professional education people obtain each year, both on the corporate and individual levels. The same is true for IT auditors.

Controls: ICFR
Controls are always a part of an IT audit or assurance project, but they can be different sets of controls depending on the nature of the project and the audit objectives. Thus, each of the controls aspects that follow may or may not apply to a specific IT audit (i.e., when applicable, use them).

When the audit project involves financial reporting, the internal controls over financial reporting (ICFR) are a critical component of what the reviewer(s) want to examine. Thus, the IT auditor must take care in a financial audit to identify the relevant IT controls for ICFR and make sure to gain a proper understanding of applications, transactions and infrastructure that impact the financials.

The reviewer’s checklist for this item should generally look something like figure 1. In some manner, the items in figure 1 should be mapped to authoritative guidance and work papers. This ensures compliance with standards and a sufficient scope of checklist items and facilitates the review process.

The reviewer’s checklist for ELC should generally look something like figure 2. Once again, the items usually are mapped to authoritative guidance and work papers. Often, and probably usually, an analysis of the ELC would require a walk-through to see if these controls have been designed properly and are implemented. Testing of these controls may become necessary later in the IT audit theoretically, but are sometimes done simultaneously with the up-front identification and analysis.

Controls: Entity Level
Another aspect of internal controls that affects the IT auditor is entity-level controls (ELC). These are controls at the higher levels of the entity that can impact the objective(s) of the IT audit or project. These would include board-related controls (e.g., IT governance), executive-related controls (e.g., managing the IT function by the CIO) and other broad controls relevant for the entity.

Controls: IT General Controls
IT general controls (ITGCs) have been one of the hot topics in IT and controls over the last few years. ITGCs have an effect on financial audits, all internal IT audits, all external IT audits and IT governance.

One of the things IT auditors need as a foundation is a good understanding of what constitutes an ITGC, how they are measured, what their risks are, and how to identify controls and assess their effectiveness. A great beginning is to read the IT Audit Framework (ITAF) from ISACA, section 3630, Auditing ITGCs.
ITAF describes 17 different areas of ITGC. The Public Company Accounting Oversight Board (PCAOB) describes three. The American Institute of Certified Public Accountants (AICPA) has five. Figure 3 provides these lists. It is fairly easy to map these three taxonomies to each other; thus, there is basically a consensus as to the ITGCs. The difference is in the details of the items.

IT auditors need to understand that a significant weakness in an ITGC not only affects the ITGC, but also everything it affects. An ITGC is considered to be an entity-level control by the PCAOB, and thus it affects almost everything in the IT function and much, if not all, of the information systems, applications and technologies. It is for this reason that the PCAOB and AICPA guidance states that if the ITGC has significant deficiencies, the auditor cannot rely on application controls, which in reality reside beneath the ITGCs.

The reviewer’s checklist for ITGCs would generally look something like figure 4. It is based on authoritative guidance and work papers.
Controls: Application

Application controls are, by definition, automated controls, or hybrid controls, which make sure transactions are properly initiated, authorized, recorded, processed and reported. The more the control objective is driven by manual controls being melded, the higher the failure rate of the control. As IT professionals know, a fully automated control does the same thing over and over again. Once it has been tested, and as long as integrated technologies are unchanged, it will keep producing the same results as designed.

The IT auditor needs to know when it is appropriate to include application controls, which controls are relevant, how to test the control, how to assess its level of reliability and assurance provided, and how to fit all of that with the overall audit plan and program. The reviewer will be looking for that kind of information.

The reviewer’s checklist for ITGCs would generally look something like figure 5.

Figure 5—Sample Reviewer’s Checklist for Application Controls

- Did the audit engagement team and the IT audit team agree to specific application software automated controls that are identified as key controls to be the responsibility of the IT audit team to test?
- Did the IT audit team perform appropriate tests of ITGCs over in-scope application software (i.e., the application software identified to contain key automated controls, as described previously)?
- Did the IT audit team perform testing to verify the design and operating effectiveness of the identified application software automated controls, including the use of appropriate sample sizes, as agreed to with the audit engagement team?
- Did the IT audit team work with the audit engagement team to complete the aggregation analysis of any identified ITGC deficiencies?

Work Papers/Documentation

All auditors understand that the audit tests and procedures, and other aspects of the audit program, must be documented. The body of work papers, in particular, becomes the body of evidence to support the audit report and findings.

In addition, work papers become a key factor in the review process. The reviewer usually has not been privy to the daily information being gathered and handled during the audit process. Therefore, the reviewer is dependent on a body of information to pick up and fully understand, for example, what was done, the results, whether a sufficient body of tests and procedures was done, and whether the proper conclusions were drawn from the body of evidence. In fact, it is not uncommon in the first review for the reviewer, who is generally one level above the team leader internally, to have a question or need something else done to the evidence or need something else done for the audit program. In such a case, this is done with some form of written instructions (i.e., notes). When this happens, the process is pushed back to the team leader to clear up whatever the reviewer requested—usually referred to as “clearing notes” in a financial audit. It then goes back to the same reviewer. The efficiency and effectiveness of this process, including the loop, are highly dependent on the work papers’ quality, completeness and clarity (for reader’s understanding).

Report

Lastly, there is a report. The report is definitely subject to review. The report must be in conformity with the entity’s methodology and any technical requirements. It is probably the most important document to get reviewed.

PROCESS

Some of the process has been explained, but it will flow something like the following:

- Team leader reviews the documentation, work papers and report before sending it up the review chain.
- Someone above the team leader reviews the audit. If problems or issues are found, the package is returned to the team leader, who addresses them.
- Often, the review then goes to yet another person up the review chain—or parallel to it—for a second review.
To help make the process go smoothly and to avoid “loop backs” to clear up issues from the reviewer, IT auditors need to be diligent in performing their duties. In particular, it is important to self-check the audit when they believe they are done, asking:

- Were all of the audit objectives addressed?
- Were the tests and procedures robust enough given the risk involved?
- Were all the relevant laws and regulations considered?
- Is the body of evidence sufficient to support the conclusions and findings?
- Do the work papers tie back to the audit objectives and conclusions properly?

While most newer (to the profession) IT auditors may need some time and experience to adequately address the guidance provided here, they need to at least understand who audits the auditors, how that process works, and how to make that process efficient and effective.

**ENDNOTES**

1 The checklists herein are based on checklists that might be used in a financial audit. Thus, they would be somewhat different for an internal IT audit for application controls, infrastructure audits, etc., but the principles should be similar.

2 All checklists have those two same factors: mapped to authoritative literature in some manner (e.g., reviewer mentally scanned the relevant literature requirements) and mapped to workpapers, usually physically on the form.

3 ISACA, IT Assurance Framework (ITAF), www.isaca.org/itaf

4 Hybrid refers to a combination of manual and automated controls to perform the control objective. This type of control is referred to as IT-dependent by the PCAOB and others.

5 *Op cit*, ISACA