The Core of IT Auditing

Tommie Singleton, CISA, CGEIT, CPA, is the director of consulting for Carr Riggs & Ingram, a large regional public accounting firm. His duties involve forensic accounting, business valuation, IT assurance and service organization control engagements. Singleton is responsible for recruiting, training, research, support and quality control for those services and the staff who perform them. He is also a former academic, having taught at several universities from 1991 to 2012. Singleton has published numerous articles, coauthored books and made many presentations on IT auditing and fraud. After nine years writing the *Journal*'s IS Audit Basics column, Singleton will make this volume 6, 2014, column his last.

With the advent of the latest wave of information technologies such as big data, social media, technologies as a service and the cloud in general, it is worth taking the time to revisit the basics of IT audit. Usually, when such new technologies arise, the issues are the same as something in the past, and the way to address the emerging technology is to do what IT auditors always do when faced with challenges of new technologies. We go back to the core of IT auditing and what IT auditing is all about. It is about identifying risk and the appropriate controls to mitigate risk to an acceptable level.

THREE THINGS AN IT AUDIT IS NOT

But first, especially for those new to the profession and for those outside our profession, it should be noted what IT auditing is not. It is *not* about ordinary accounting controls or traditional financial auditing. That knowledge and skill set served the audit profession well from the beginning of auditing in the middle ages (with exchequers and other forms of auditing) until the introduction of computing systems in the 1950s. In fact, before 1954, it was possible for an auditor to use a very similar audit program from day one of his/her career until he/she retired. To put it simply, the use of computers in accounting systems introduced a new source of risk associated with accounting processes and information (i.e., data). And, it introduced the need for those who understand this new "thing" to identify and mitigate the risk.

IT auditing is also *not* compliance testing. Some believe IT auditors are about making sure people conform to some set of rules—implicit or explicit—and that what we do is report on exceptions to the rules. Actually, that is management's job. It is not the compliance with rules that is of interest to IT auditors. IT auditors are examining whether the entity's relevant systems or business processes for achieving and monitoring compliance are effective. IT auditors also assess the design effectiveness of the rules—whether they are suitably designed or sufficient in scope to properly mitigate the target risk or meet the intended objective.

Compliance failures are important to IT auditors, but for reasons beyond the keeping of rules. A compliance failure can be, and often is, the symptom of a bigger problem related to some risk factor and/or control, such as a defective system or business process, that can or does adversely affect the entity. Thus, to the IT auditor, compliance failures are much more about risk (ultimately) than the rules themselves.

It is also passé to automatically or casually consider IT considerations of an audit to be out of scope because it is not explicitly related to some stated requirement, or to consider an audit to be a waste of time. The fact is IT can and does adversely affect business processes or financial data in ways of which management may not be adequately aware.

UNIQUE INHERENT RISK

IT presents risk factors that are unique to accounting, auditing and systems. That is, IT itself brings risk to the entity regarding its systems, business processes and financial/accounting processing. That risk is unique to IT and without IT being present, that risk would not exist—at least not to the same level. It takes a professional, such as an IT auditor, to identify and assess the inherent risk associated with IT.

ISACA thanks Tommie for his years of service to the Journal *and the association. Your words have influenced many professionals and will continue to do so. Wishing you the very best as you end this chapter and begin the next!*

Those risk factors include systems-related issues, such as systems development, change management and vulnerabilities, and other technology-specific factors. Apart from the IT professional, such risk can go unnoticed, to the detriment of the entity. For example, a university had the following experience related to its financial aid systems.

The university's IT department wrote its own code for financial aid. The university had a great deal of financial aid available as a private institution, leading to the majority of students receiving some form of aid. The experienced IT auditor, seeing these facts, identified certain inherent risk associated with financial aid including the accuracy of the code, the possibility of a bug in the code, and the possibility of fraudulent code that needed to be addressed, examined and mitigated. However, management of the university did not recognize any risk and assumed the IT department had done its due diligence and everything about the financial aid code was acceptable. A few years later, the university accidentally discovered a bug in the code that was causing calculations of financial aid to be overstated. Millions of dollars of financial aid had been awarded over those years in error, and the institution had some financial problems causing it to abandon some of its programs. This case is offered to illustrate the need to identify and assess the inherent risk associated with IT to the entity.

Given that almost all entities employ some level of IT, the day has come when these entities truly need an IT auditor to evaluate their inherent risk of IT. IT auditors are particularly trained and skilled at doing that task. IT auditors are capable of identifying the nature and risk of IT technologies and systems.

> "The day has come when almost all entities truly need an IT auditor to evaluate their inherent risk of IT."

Back to the emerging technologies issues, the place to start with them is to properly assess the nature, specificity and assessed level of risk. Once this process is thought through diligently, the IT auditor and others can begin to put together adequate controls to satisfactorily mitigate risk.

THE ROLE OF CONTROLS

One of the main reasons for a control is to mitigate some identified risk. The way to deal with an inherent risk that is at a level higher than what is acceptable is to implement an effectual control to mitigate that risk to an acceptable level.

Enjoying this article?

- Refer to *Information Systems Auditing: Tools and Techniques*.

www.isaca.org/audit_tools_techniques

That being said, there are some points to remember about controls and the role they play in IT auditing, or auditing in general. First, IT auditors need to be wary of false security by a control that is effective enough to mitigate the risk to an acceptable level. While experienced IT auditors are generally good at this exercise, management and others may not be as adept at understanding the reality of a control.

On the other hand, IT auditors should remember and keep in mind that controls introduce a cost and a benefit. The cost is almost always in real dollars—cost of identifying, designing, implementing and managing the control. The cost can also be an impact cost of inconvenience or operational efficiency in slowing down a process. Some of the latter is not so much a concrete observation as it is an understanding of, and taking into account, the impact of a control. A key for IT auditors has been seeking a balance between these costs (real/concrete and impact) and benefits. Benefits can also be real and concrete—understanding the relative difference in having the control operate effectively and doing without it. That balance is easier to describe than to discern effectually.

For instance, an organization wants to implement an effective password policy for the length of life for passwords. The common wisdom is that the life should be inversely correlated with the amount of risk associated with unauthorized access. That is, if there is a high risk associated with unauthorized access, the life should be short (e.g., 90 days for an online bank account). However, once that policy is implemented, there could be an unintended cost associated with forgotten passwords due to the frequency of changes in them. The result could be users frequently forgetting passwords and having to use entity resources for assistance in obtaining access—a cost that includes delays and frustration, among other results. Thus, the key is due diligence in assessing the real net benefit of a control.

Another consideration is that an entity has a business or purpose for which it is in operation. That purpose needs to be part of the consideration. It is easy to lose sight of the unintended impact on operations.

Generally speaking, the higher the inherent risk, the higher the interest should be in a control to mitigate that risk. IT auditors need to, therefore, consider the level of inherent and residual risk when conveying recommendations for controls.

Last, controls are often embedded in technologies or systems. That fact alone suggests that IT auditors need to be involved in assisting with the design where independence allows it. It also suggests a high importance for using IT auditors to assess the effectiveness of the internal control system. How can the control embedded in IT be properly assessed without an IT subject-matter expert providing assistance in understanding how effectively the control operates?

UNDERSTANDING THE REAL RESIDUAL RISK

One of the issues with analyzing risk is that it is usually relative and subject to judgment. All constituents want controls to be "good enough" so that things will be "okay." But, what is "good enough" and what is "okay"? Risk is not usually subject to an absolute measurement.

Bad managers have a tendency to misjudge or misapply controls and risk. Concerned with surviving and making a profit, they sometimes do not see the reality of residual risk and rush ahead only to encounter a bad result. Or, they get paranoid and avoid a perfectly acceptable risk and take no action to their detriment. Good managers, however, understand the reality of residual risk, and usually make the right decisions and often have a contingency plan should the risk come to the forefront. One of the challenges for IT auditors is to help managers be good or great managers by understanding the real residual risk and taking the appropriate action related to it.

One challenge in understanding the reality of residual risk is to properly assess risk and controls holistically. First, some controls are not IT and there is a tendency by some to overlook a manual control that has the potential to mitigate an IT-related risk. For instance, review and reconciliation by a controller may adequately reduce/mitigate the risk of unauthorized access to data and databases. That is, if someone were able to compromise the access controls, or lack thereof, and compromise data in a financial/accounting database, any error or fraud created would be caught promptly and corrected. Thus, the residual risk may be relatively low considering the manual control.

Second, a residual risk that exists in one area may be addressed by an effective control in another area. For instance, it may be that a firewall has inadequate protection against an outsider coming through the perimeter and hacking into the system. It would be easy to jump to conclusions about the high-level residual risk related to financial data and financial reporting, for example; however, if the entity has strong access controls at the network layer (e.g., a strong Active Directory control matrix and logical segregation of duties), at the application layer, and over the operating system and database access, what are intruders going to do once they gain access through the perimeter? Therefore, it is crucial to do a mental walk-through of how the perceived residual risk will play out if it becomes reality, to determine if it is a real residual risk. This example assumes the audit objective was related to financial reporting. Obviously, if this situation were one where the audit objectives were related to systems in general (internal audit) or the firewall in particular, the residual risk would be real and need attention. Either way, the firewall is broken and probably needs to be fixed.

Scoping the residual risk means the IT auditor also needs to have a mental map of all the broken things in the IT space and which ones are real/relevant and which ones are broken; but out of scope. (The truth is, all IT audits will likely unveil several things, but they may not all be in scope.)

It is also crucial that the IT auditor develop a rational argument for why something found in the IT audit needs to be addressed and remediated, and ensure that it makes sense from a business perspective. The tendency of IT auditors is to find broken things and want them all fixed because they are broken. However, IT auditors need to examine from a business perspective what really needs to be fixed. The rationale should be a reasonable, realistic, business-oriented scenario of a relatively high risk that would come to fruition.

These issues illustrate the need for IT auditors to be effective communicators.[1]

CONCLUSION

What IT auditors do is usually contained in risk and control arenas. Therefore, it is critical that IT auditors be adept at understanding, analyzing and communicating results related to risk and controls and what we do.

ENDNOTE

[1] Singleton, Tommie; "Beyond the IT in IT Audit," *Information Systems Control Journal*, vol. 3, 2008, *www.isaca.org/archives*