Why Everyone Dislikes the IT Auditor and How to Change It

Tommie Singleton, CISA, CGEIT, 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 1991-2012. Singleton has published numerous articles, coauthored books, and presented many sessions on IT auditing and fraud. He authored the *ISACA® Journal*'s IS Audit Basics column from 2005-2014.

Well, to be truthful, not *everyone* dislikes the IT auditor. But there have been a lot of remarks made over the years, and some personal observations, that indicate some dissonance between the IT auditor and management or users of IT audit services. Some of them are beyond our ability to affect a change. But some can be remediated with an appropriate effort on our part. This article will address some of the more common criticisms made about IT auditors and what we, as professionals, can do to address them.

CRITICISM 1—IT AUDITORS ARE DIFFICULT TO UNDERSTAND

There are some who rely on or use IT auditors yet have a difficult time understanding what they are trying to say when recommendations or reports come back. Some individuals are not familiar with IT and will be unable to fully understand much about the results in technical jargon. Some, if not many, of those people will simply rely on the IT auditor with blind faith. *IT auditors can address this issue.*

It is important to recognize that our profession is a highly technical field (with a limited number of professionals who understand it well) and we have our own language. To complicate our language, we use many acronyms. And to complicate the knowledge base, it is constantly changing. Combine those factors, and there is a probability, at some level, that our communications will be a challenge to many who use IT auditors.

Therefore, IT auditors should make a concerted effort to tailor their communication to the audience. Take time to know where the audience is in its understanding of IT and in its ability to understand our language, concepts and technologies. When the hearers are not literate in IT and do not understand our words, concepts, terms and acronyms, we need to become the interpreters of our own communications for them. When communicating with management, take the time to understand their perspective and needs and strategically formulate communications with those needs in mind. If it is a general user, keep in mind that they are less likely to understand our information, so convert it to a more simplified level for the more general reader. I know of one person who talked to his eight-year-old daughter while preparing a major report and kept revising his information until she understood it. He later claimed that it was his most successful presentation ever.

We should strive to present our reports and recommendations in "plain English." Some suggestions to consider:

- Do not use acronyms (except within our own profession).
- Use relatable anecdotes or stories to demonstrate your point.
- Compare your results or recommendations with things the audience already understands—such as current events or stories in the news.

Also, we should take opportunities to improve our communication craft.[1]

CRITICISM 2—IT AUDITORS WASTE RESOURCES (OVER AUDIT)

I have heard this comment several times, usually from professionals who do not have a positive relationship with IT. It is said in different ways, but the point being made by this group appears to be related to their perception that IT auditors spend a lot of time providing services, but with a disproportionate benefit to the firm, user or client in the end. There are several points we should keep in mind and, when appropriate, gently remind others of these circumstances.

First, for public accounting, our technical literature requires the use of an IT auditor (or auditor trained in IT assurance) in the financial audit, except where internal controls are assessed at the maximum weakness (i.e., controls cannot be relied upon at all). The truth is that very few clients have systems where controls cannot be relied upon at all in financial audits. Certified public accountants (CPAs) cannot simply

ignore the technical literature because it makes sense to do so for some reason (e.g., from a budget or perceived benefit perspective). It is a requirement.

Second, the risk related to IT in a financial audit is real and growing. These risk factors have an impact on the risk of material misstatement (RMM). It may be true that most of the time IT risk does not materially affect financials, but one does not know that without going through a diligent process with integrity and professional care. For example, how many companies use a spreadsheet to do some part of the financial reporting process? Does the fact that a spreadsheet is used in financial reporting cause the associated risk (i.e., RMM) with the technology and *not* the accounting transactions or processes *per se*? Yes! In addition, IT auditors can add value to an audit even when the conclusion is that IT risk has a nominal or limited effect on RMM (e.g., client relations).

Third, one thing the IT assurance profession can do to diminish this criticism is to be sure to properly scope engagements related to IT. There is a temptation for IT assurance professionals to get involved in assessing all of the "broken" things in the IT space and to lose track of their proper scope. For instance, in a financial audit, the IT auditor will be tempted (due to natural tendencies) to identify *all* of the things that are "broken" in the IT space and report on *all* of them, without considering the RMM for each one. There is a temptation to spend time evaluating IT that is, in reality, out of scope and, thus, results in "over auditing" IT. Thus, if IT auditors are not careful, they can inadvertently create an atmosphere to justify the criticism of wasting resources. The truth is that all IT spaces will have several things that are "broken," but IT auditors need to filter through them with the audit objectives of the service being provided and not include something just because it is "broken." That being said, broken things need to be fixed.[2]

Lastly, IT auditors should be careful to add value to each audit, either through client relations or internally to the entity. Referring back to IT things that are broken and need fixing, those items that are excluded for scope purposes are still prospective items to be communicated to the client or entity, even if it is "off the record." Most of the time, management is interested in learning about IT deficiencies or security holes, whether they are in scope or not.

There are a lot of other ways IT auditors can add value to the service beyond the testing and formal reporting processes. IT auditors can explain IT risk by using easy-to-understand illustrations to help make the point. Adding value to the team, such as using IT to facilitate the team processes or even to gain efficiencies, is another way.

CRITICISM 3—IT AUDITORS LIVE IN A DIFFERENT WORLD

IT auditors live in the world of IT; it is full of things most people do not understand and we do use a language that is foreign to most people. But it does not have to lead to this criticism. We can speak in "plain English," relate findings to our audience and generally make an effort to relate to those involved in our services.

That relating can start with considering existing business risk, goals, strategies, etc., not only in performing our services, but in communicating with others during and after completion of those services. IT auditors can also avoid this criticism by being realistic about IT risk. For instance, a firewall that is ineffective, broken and needs to be fixed is definitely a security breach waiting to happen. But that broken firewall needs to be considered in light of the scope of the service. If it is a financial audit and logical access controls at the server and application layers are good, then the firewall becomes irrelevant in light of the RMM. That is, if someone does break through the firewall, what are they going to do to financial data? It is true the intruder can go around the application by accessing the data, but if that happens, will other controls (manual or automated) be able to recognize a material misstatement and make a timely correction? If so, then the broken firewall is irrelevant to the RMM. However, it is relevant to client relations, and the IT auditor would want to mention it to management, probably off the record, so it can be fixed.

> "IT auditors should always use a realistic assessment about risk."

Another point using the same scenario is that IT auditors should always use a realistic assessment about risk. Specifically, that assessment should include the magnitude of the risk (should the risk lead to a deleterious fruition) and the likelihood that the risk will lead to a "bad" event. Sometimes IT auditors focus solely on the magnitude without a realistic appraisal of the likelihood. That approach leads to this criticism of living in a different world. For small businesses

with a low public profile, the likelihood that a hacker will break through that firewall and do something bad is quite low. In fact, it may be so low as to be reasonably ignored. It is true that if someone breaks through the firewall, they can do something bad, but specifically, what will the hacker do, and, specifically, how would that be a violation in light of the service being provided? If the service is internal audit evaluating security, it is in scope and is an exception that should be reported and remediated; however, realistically, there is a low probability of a breach. If the service is external audit, the firewall risk can be reasonably ignored in most cases.

Lastly, it is a valuable exercise to practice good social skills when working with clients and management. Being nice to people always leads to benefits for both parties.

CRITICISM 4—IT AUDITORS ARE TOO RESTRICTIVE AND PROTECTIVE

Sometimes people in our profession are quick to respond to certain requests with a curt remark. When management asks about doing X, IT auditors need to avoid using the phrase "X cannot be done." IT auditors need to think through the request and seek alternative solutions. In some rare cases, X does not need to be done, but even then, we should seek an alternative response such as, "I wish we could do X, but here are some concerns I have…." Then try to work through the responses to come up with a reasonable, secure, appropriate, alternative solution.

Another frequent response some IT auditors use is "That is a security risk," and then they resist doing anything related to the request. It may be a security risk, but we need to first use the magnitude X likelihood approach mentioned above to determine if it is necessary to seek an alternative solution that has an acceptable level of (residual) risk, as opposed to just saying, "No, it is a security risk."

For instance, in a recent scenario, an IT auditor was told that management planned to have its customers access their proprietary data in the entity's database remotely, whereupon the IT auditor said, "No way. The customer could potentially access anyone's data and that is a privacy issue." While that is theoretically true, the response was totally focused on the magnitude without consideration of likelihood. In addition, the response came without discussing some reasonable compensating controls that could be employed to remediate the privacy risk.

IT auditors need to avoid any response or actions that appear to be those of a control freak. We do not need to sacrifice our responsibilities in our role as IT audit professionals, but we also do not need to alienate management or clients when a different, responsible and reasonable response or alternative solution is possible.

A basic principle that can be used to avoid this criticism is to stop and think about cost-effective solutions that take into consideration magnitude and likelihood instead of seeking absolute perfection in solutions. After all, no solution is truly perfect in the IT space. A suitable response goes back to a principle above: Make sure to understand the needs and purposes users/management have for their request before dismissing it unilaterally without due diligence in seeking reasonable alternatives.

> "Stop and think about cost-effective solutions that take into consideration magnitude and likelihood instead of seeking absolute perfection in solutions."

CONCLUSION

Some criticisms that are aimed at IT auditors can sometimes make us feel like everyone dislikes the IT auditor. Some of those criticisms cannot be avoided because of attitudes that are not susceptible to efforts to the contrary. But often we can mitigate those criticisms, make people appreciate us and even cause users/management to like the IT auditor.

ENDNOTES

[1] Singleton, T.; "IT Audit Basics: Beyond the IT in IT Audit (Part 2)," *ISACA Journal*, vol. 4, 2014, *www.isaca.org/archives*

[2] Singleton, T.; "IT Audit Basics: What Every IT Auditor Should Know About Scoping an IT Audit," *ISACA Journal*, vol. 4, 2009, *www.isaca.org/archives*