IS Audit Basics

The Logical Reason for Consideration of IT

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 that 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.

The need for consideration of IT in internal and external audits seems intuitively obvious. This is emphasized by the fact that the vast majority of individuals are immersed in IT—from smart phones to complex TV/media systems to work technologies. Yet there are still gaps from time to time where entities or individuals have not completely thought through the reasons why IT needs to be continually evaluated by senior management, and examined by internal and external auditors.

PERVASIVENESS OF IT

Most, if not all, would agree that IT has become prevalent, including among accounting and finance functions and in financial reporting. Some of the effects and needs related to this pervasiveness include:

- 24/7 requirement of IT
- Need to detect errors early
- More automated controls, fewer manual controls
- Complexity—integration of multiple technologies
- Electronic work flow
- Paperless transactions (e.g., electronic data interchange [EDI])
- Networks that extend beyond the entity

The complexity issue is a particularly acute one. Complexity needs to be broken down and understood by auditors to effectively perform the larger realm of audit (e.g., the financial audit for Certified Public Accountants [CPAs]). But, the very nature of complex IT makes that process difficult; thus, the need for lifelong learning and constant continuing education by IS auditors.

Another acute issue is the increase in electronic work flow and paperless systems. If customers at a gas station pump their own gas and say "no" to the receipt option, how does an auditor audit that class of transaction? Aside from an IS auditor using IT tools (e.g., computer-assisted audit tools [CAATs]), it would require someone to print the data for examination and there would still be an inherent lack of confidence in the data.

To compound the other issues, entities have welcomed customers into their networks via customer relationship management (CRM) tools, welcomed their vendors via supply chain tools, and increased the risk associated with both systems and financial data.

The point being made is not just the pervasiveness of IT, an obvious conclusion, but the associated increase in IT-related risk to the business and to audits. Thus, there is a need for IS auditors and their knowledge, skills and abilities to assess risk, address risk and develop adequate mitigating controls for risk.

CRITICALITY OF IT

IT is often critical to a business or entity. Easy examples include eBay.com and Amazon.com, but traditional brick-and-mortar companies are also sometimes extremely dependent on IT. Walmart and the airline industry are two obvious examples. There is a very long list of entities that find IT critical to their products or services.

Thus, for those entities, it is important to understand IT and how it relates to the business processes to gain an adequate understanding of the entity. That would be a particularly important for a CPA doing a first-year audit, for example.

IT can affect any of the following, and other things not on this list, regarding an entity:

- Business model
- Goals, objectives and plans
- Competiveness
- Business risk
- Transaction flows
- Data flows
- The whole business process stream
- Transaction reporting
- Accounting and financial reporting risk

For example, in applying COBIT® to an organization, most, if not all, items on the previous list would be considered. That said, many of them would not be simple to evaluate and/or understand adequately without a great deal of effort and possibly some research or serious assessment of IT.

And, because of its criticality, IT likely increases a variety of business risk factors associated with these items.

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.

Go directly to the article:

IMPLICATIONS OF IT: THE "DARK SIDE"

One way to analyze risk implications is to think about the various aspects of IT general controls (ITGCs). While there are a variety of taxonomies for ITGCs, the following are discussed to illustrate risk, but are not intended to be an exhaustive analysis.

IT Environment

The IT environment is defined basically as effective oversight and management of the IT function by the organization. That oversight includes things like:

- Managing IT problems and issues; help desk
- Monitoring usage and problems
- Competency of IT staff
- Continuing training of IT staff
- Sound project management practices for major IT projects
- Effective IT governance
- Proper segregation of duties (SoD) for IT staff/department
- Effective policies and procedures (P&P) integrated with the entity's P&P
- Effective use of, or return on investment (ROI) for, IT
- Effective integration of IT with planning and organizing of the organization

Some of the more common deficiencies include:

- Lack of independence of critical IT decisions
- Lack of subject matter experts (SMEs) on the board of directors (BoD)
- Inadequate management of one or more ITGC areas

One common mistake of organizations is to relegate decision making for all IT decisions to the chief information officer (CIO) or IT director. That structure is not the most effective way to manage the IT function. In fact, sound IT governance would suggest that either the BoD or an IT steering committee have oversight of things such as capital budget decisions regarding IT.

One common oversight of organizations is the presence of an SME on the BoD. Perhaps the dearth of SMEs available accounts for at least some of that absence. But, it is difficult to implement sound IT governance without one or more SMEs being involved with planning and decision making.

Managing the IT function is a difficult task for any management team. IT keeps changing. Competitors find new ways to gain advantage using IT. IT keeps getting more and more complex and, thus, harder to comprehend. But, healthy organizations find a way to manage most of their IT most of the time.

Change Control

Change control is something that should be evaluated on every financial audit, and many internal audits. The scope of change control varies within different organizations based on facts such as custom programming (including middleware) and complexity of the organization's IT.

> "Healthy organizations find a way to manage most of their IT most of the time."

Some common deficiencies include:

- Lack of control over access to coding
- Lack of control over changes to programs
- Ineffective decisions in replacing or upgrading IT

The last issue is one that is common to all organizations regardless of size. In fact, smaller entities are probably more likely to forego formal processes of change management and even sometimes make changes based on poor decision making simply because a smaller entity is less likely to have a wealth of IT knowledge.

Application Development (AppDev)

Generally speaking, AppDev is part of change management, but it is a special case. Some applications make significant calculations automatically within the application. If the application is custom developed in-house, this is particularly risky and dangerous.

For instance, it is fairly common for cost of goods sold (COGS) to be calculated by the application as part of the posting of a sales transaction. If COGS is a material account, and it usually is, the entity should be careful to make sure it has an effectual level of assurance over that calculation.

There is one example where a utility wrote its own code and had a simple mistake in an if-then-else statement. For fewer than 1,000 units the rate was US $x.xx/unit. For 1,000-5,000 units, the rate was a flat US $yy.yy plus US $z.zz/unit in that range. The variable, having been set to zero before the if-then-else, was left at zero for those fewer than 1,000 units (note that no customer complained). This led to a US $37 million understatement of revenues.

Entities should take extra care with material automated calculations.

Logical Access Controls

Logical access control is another area that should be evaluated on every financial audit and many internal audits. The previous

discussion alluded to pervasiveness and expansion of IT and the nature of systems causing the need for effective logical access controls to become paramount.

Some common deficiencies include:

- Weak access controls over financial applications
- Failure to take advantage of effective SoD using least privileges in access controls
- Elevated privileges that do not return to normal
- Terminated users whose credentials remain active

Thus, access controls represent a fairly robust area of risk. Because of the complexity of systems and networks, and the expansive nature of those systems, there is usually a need for an IS auditor to evaluate access controls in most organizations.

Third-party Providers

More and more organizations are specializing in services that entities are outsourcing to them. Add to that the proliferation of cloud services, which are third-party providers as well, and there is an increase in the number of business processes or functions that are being outsourced.

This adds risk to the business process stream as a whole. How does the entity have reasonable assurance that adequate controls are in place at the third-party provider? Would those controls be better if the process was internal? The point, once again, is the increase in risk and the presence of IT.

Business Continuity Planning and Disaster Recovery Planning

With regard to business continuity planning (BCP) and disaster recovery planning (DRP), risk has increased over the disaster aspect. With cloud computing and the increased complexity of systems, there is greater probability of a system failure that can affect computer operations. Thus, risk involves both incurring such a failure and being able to properly restore computer operations.

The bottom line for the discussion thus far is that there are many aspects of IT that represent an inherent risk (IR) with a relatively high assessment. That IR is generally independent of traditional risk factors, such as those associated with the risk of material misstatement.

IMPLICATIONS OF IT: "THE FORCE BE WITH YOU"

There is a bright side to the IT invasion. IT is a two-edged sword: It is able to inflict wounds on the entity, but able to defend the entity as well.

The following is a short list of some of the beneficial uses of IT:

- The potential to identify efficiencies in audit procedures
- The potential to rely on effective automated controls
- The potential to leverage CAATs to perform IT-substantive procedures over more expensive manual procedures
- The power of data analytics in effective decision making and management
- The ability to identify beneficial feedback to management (e.g., value-added management comments)

As part of my dissertation, "The History of EDP (IT) Auditing," I interviewed about 45 pioneers of the IS audit profession.[1] Without exception, they believed the event with the largest impact was the advent of CAATs. Not only can IS auditors analyze financial data, but they can also analyze nonfinancial data. IS auditors can draw inferences about the operational effectiveness of controls, or even the presence of controls, by examining the right kind of data. Usually, IT-substantive tests are less expensive overall than manual substantive tests.

> "Most, if not all, organizations have something broken in the IT space that needs to be fixed."

The last point on the list is important because most, if not all, organizations have something broken in the IT space that needs to be fixed.

CONCLUSION

Admittedly, there are a number of challenges related to IT. Much of this article focused on the increase in risk associated with IT in the current-day environment. Those challenges are elevated by rapid changes in IT, including the complexity of IT, for both new/emerging systems and existing systems. One key point is the presence of IR related to IT that needs to be identified, assessed and mitigated.

However, there is good news. First, the adequately prepared IS auditor can be a huge asset to any organization by being able to assess and mitigate risk. Second, that same IS auditor can also leverage IT to provide efficiencies and effectiveness to the organization, e.g., the use of data analytics in a business entity or the use of a CAAT in an audit. Last, the environment is not likely to change for the foreseeable future; therefore, there will be a need, whether acknowledged or not, for IS auditors for a long time to come.

ENDNOTES

[1] Singleton, Tommie; "The History of EDP Auditing," dissertation, University of Mississippi, 1995