The Trusted Professional
The online news resource of the New York State Society of Certified Public Accountants

Back to basics in IT risk assessment

By Yigal Rechtman, CPA

Information technology has taken a starring role in the risk assessment process that accompanies the planning, execution and conclusion of the audit, now that the capturing, processing, storing and reporting of information have become almost exclusively computerized. Given how central its use is, it’s always a good idea to review the basics and understand just what the audit standards say with respect to IT.

Fortunately, the requirements for auditors, as detailed in Statement on Auditing Standard (SAS) 109, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*, are very clear. According to the SAS, “the use of IT also affects the fundamental manner in which transactions are initiated, authorized, recorded, processed, and reported.” Accordingly, auditors are *required* to comply with SAS 109’s basic premise: “The auditor *must* obtain a sufficient understanding of the entity and its environment, including its internal control, to assess the risk of material misstatement of the financial statements whether due to error or fraud, and to design the nature, timing and extent of further audit procedures.”

What SAS 109 says to auditors is that by reviewing these areas of risk, they can produce a higher quality audit, defend their audit process and provide additional value to clients in the form of recommendations and support, not only during the audit, but throughout the year.

What does IT control?
Just as there are manual controls—those tasks and checks-and-balances that are performed by people (e.g., bank reconciliation), there are automatic controls that are preprogrammed and performed by machines (e.g., allocating expenses between departments). In its widest scope, there are two types of IT controls: processing controls and general controls. An example of a processing control could be that the allocation of expenses between departments is always equal to 100 percent of the allocable basis. Having such a control may sound like common sense, but if a program has an error in it, the result could be that the total allocated to all departments is something other than 100 percent, which means that at the end of the day, the financial reporting would be erroneous.

General controls, on the other hand, are what makes the whole IT environment work. The auditor, in evaluating general controls, would be interested in several areas. Chief among these areas are the *availability* of the IT environment and *access controls*. The availability risk is the risk that the information would not be available. This may be trivial for some clients but, for others, it could result in severe consequences. For example, if the previous year’s or legacy systems’ data are not available for inspection by a regulatory agency, there could be consequences for the company. The auditors are typically even more interested in the general controls of *access*. Access controls determine whether a solid segregation of duties is maintained within the IT environment. So for example, even if 10 people are situated in 10 offices throughout the United States, if their access controls are not properly configured, an auditor should be able to evaluate that the level of segregation of duties is diminished, increasing the control risk.

Other general controls include hardware maintenance, operating system updating, network and middleware configuration, software development change control, business continuity and disaster recovery planning, physical controls, and training and human monitoring.

Auditors, in compliance with SAS 109, should recognize that the risk assessment of the IT environment is critical for the overall risk assessment process. A properly designed IT environment could give the coveted “comfort” to auditors that the client is running a tight ship. Of course, only testing these controls could actually enable the auditor to reduce control risk—

and these tests are becoming more commonplace, in part because auditors are maturing in their understanding of these systems, and in part because the tests are relatively easy to implement.

Delivering value

Beyond the compliance with Generally Accepted Auditing Standards, auditors are also in an excellent position to deliver the good and bad news about the design of the IT environment. At times, there are weak points that could be strengthened, and the person who knows how to deliver this news to the client now becomes a trusted and valuable adviser. Auditors, who completed a deep analysis of their clients' IT environment, are in an excellent position to provide such feedback and, at times, may be required to do so. For example, if a client's firewall is so poorly designed that it imposes an immediate risk to the client's database of customers and their banking information, the auditor should inform the client right away, and further, issue a comment as required by SAS 115 for a control deficiency, significant deficiency or a material weakness (the discussion of SAS 115 is beyond the scope of this article).

At the end of the day, a back-to-basics approach when it comes to the risk assessment in the information technologies environment could result in more efficient audits, more compliant audits and more valuable advice to clients.

Yigal Rechtman, CPA, CFE, CITP, CISM, is the Senior Manager for Forensics and Litigation at Grassi & Company. He is a past chair of the NYSSCPA's Technology Assurance Committee.

The Technology Assurance Committee will present a CPE session entitled "Back-to-Basics in IT Risk Assessment" on Feb. 21. For more information, visit nysscpa.org