How much IT compliance is enough?

One of the most pressing business issues of corporate executives today is the amount of attention and effort required in reviewing automated IT systems. Not only do executives need to contend with figuring out how much attention should be spent on reviewing IT compliance issues but also what to review, how to review it and determining sufficiency.

Determining how much review is required of IT systems would appear to be a finite task but unfortunately has become a real challenge considering the requirements of Sarbanes-Oxley (SOX) in the US and Bill 198 in Canada. The challenge squarely rests on the different stakeholders' assurance needs. The extent of review of automated IT systems is complicated by macro and micro level issues and influences. On the macro level, the issues of business efficiency, the number of regulatory and standard setting bodies and the different review objectives between company and its auditor complicates and affects the level of review. On the micro level, review issues focus our attention on what and how to review. This article contemplates a series of questions in reviewing automated IT systems, potential solutions and addresses the reality of human invention impacting automated systems and compliance.

Macro level challenges to compliance

The need for efficiency and minimal regulation has always been top of mind and valued by corporate executives. However, with the recent number of accounting scandals to hit public companies, regulators created the SOX Act to help curb fraudulent acts and to protect the investment public. As part of the SOX Act, the Public Company Accounting Oversight Board (PCAOB), a US regulatory body, issued broad guidance regarding the necessity of IT review for public accountants and public companies. After three years into the Act, and millions of dollars spent on compliance matters, the requirements have left some executives feeling SOX is too burdensome and sacrifices efficiency and productivity. What executives have long forgotten is the negative impact these accounting scandals made on the capital markets by wiping out billions of dollars of investments and savings of the investing public while creating of mistrust of corporate executives and financial information provided by their companies. The issue of concern is whether corporate America should sacrifice public confidence in the capital markets at the expense of efficiency. In other words, should burdensome safeguards and well documented processes be necessary over lean and mean systems? The argument of sacrificing efficiency shouldn't be at issue considering most world class companies have well documented safeguards and processes. Those executives narrowly focusing on performance don't realize that performance is a function of the work of efficient processes which leads to better performance. Clearly, these executives are putting the cart before the horse.

The second issue complicating the extent of IT review is number of standard setting bodies and the number of standards created by them. What is the minimum standard required for reviewing automated IT systems and who should set that standard? For public companies, they must follow various standard setting bodies for each country and for particular parts of GAAP and compliance. For instance, in Canada, there are three major accounting bodies (CMA, CA, CGA) and a provincial regulatory body. In the US, there are over 10 major accounting bodies including, AICPA, FASB, COSO, ISACA, SEC, PCAOB etc. with many regulatory bodies including the SEC, PCAOB with several regulatory frameworks, e.g. COSO, ERM COSO, COBiT. The challenge for public companies is to distinguish and interpret the maze of guidance from multiple standard setting bodies creating turf wars amongst these organizations and layering of regulations.

The third issue is the difference in review levels between public company executives and their external auditors. The dilemma stems from the comfort level the audit firms are seeking due to litigation concerns from shareholders while feeling the pressures from the regulators critical of their performance of IT audits. The challenge arises from the results after the first year of public audits under SOX regulation. Public companies want less regulation and review of IT systems while audit firms are uncompromising due to their fears and scrutiny.

Again, the extent of review of automated IT systems is complicated due to the divergent needs of various stakeholders' and the views of corporate executives who feel detailed reviews are of limited value. Can we get around this dilemma and how so?

How much review of systems is enough?

In answering this question, we need to remind ourselves, the purpose of our review is to ensure both users and providers of financial information have clear and transparent information to make sounds decisions. For providers of information, the value of automated IT systems is to help streamline their work while improving the quality and consistency of data it produces.

On a pragmatic level, the amount of review for IT automated systems is not clear cut because of the unique nature of each company. Many factors including the size of company, its appetite for risk, the way it is organized, the talent level of its employees, and the amount of resources all have a bearing on how much time and attention a company should spend on its efforts. The goal is to find a balance between conformance and performance.

A part of the challenge in the review process is deciding what the scope of review should be and identifying critical and non critical systems to prevent the decision making from being mired in compliance efforts. Also it is necessary to identify the number and types of systems and the level of integration between them. Finally, we need to understand the extent of human processes that make up the entire business process compared to the level of automation.

Potential solutions

On the whole, the extent of IT review is dependent on the level of automation that exists within a company's accounting environment. If a company functions in an environment with heavy human intervention in its business processes, more compliance efforts will be required to validate controls and information. Conversely, if the company's environment is made up of business processes which function in an automated environment, the extent of the review can be lessened while the degree of assurance increases due to consistency of processing.

A potential solution to reducing compliance efforts is re-engineering business processes from manual to automated processes. The benefit from having a highly automated environment is that it keeps most of the transaction data and controls within the processing systems, such as an ERP system, while lessening the amount and type of human intervention in processing data. However, the challenge this solution faces is that it is resource intensive and change management oriented. For larger companies, it requires a cultural shift in thinking and working. For smaller companies, because of their limited resources, automated solutions are unaffordable.

Another automated solution which has the potential to improve compliance efforts is Extensible Business Reporting Language (XBRL). The flexibility and functionality of XBRL, which is a subset of XML language, can be used to help re-configure parts or entire business processes to be more efficient and produce transparent financials while assisting external auditors to perform better and faster audits by allowing them to examine the source data and financial information clearer. This is one of the main reasons why the major audit firms have gravitated towards XBRL technology; it will save them time, money and efficiency. Similarly, regulators will be able to receive the same benefits during their reviews.

The final benefit automation provides is less internal audit resources. However, companies will require higher skilled auditors to perform the compliance work to reap the efficiency benefits.

The reality of automated systems

If we assume for the moment, that automation appears to be the right answer and we focus our efforts in that direction, unfortunately a certain amount human intervention will remain. For instance, in order to implement these automated solutions, human intervention is required in configuring these systems. If by chance the systems are incorrectly configured at its inception, the automated controls we are relying on become ineffective. Hence, the importance and necessity for reviewing IT application controls.

Unfortunately, this leads us to the conclusion that there will be a certain degree of human intervention required regarding automated systems and compliance efforts. The question then becomes where and how do we want to have the human intervention; on the front end during the set up of automated systems or on the back end during review of manual accounting controls? The choice is up to management. It can choose to pay now via investment in automated systems or pay later through intensive compliance efforts.

With asking the right questions, you can find balance by determining how much time to devote to compliance issues and reviewing IT automated systems. Unfortunately, the standards established today are guidelines and not a defined set of best practices.

Jay Roy, CMA, MBA, is president of Strategic Compliance Group, Inc. (jay.roy@strategiccompliancegroup.com), which specializes in conformance and performance enhancement.