nformation Systems Control Journal, Volume 1, 2002

IT Audit Basics

The IS Audit Process

By S. Anantha Sayana, CISA, CIA

In response to requests from *Journal* readers, columnists Fred Gallegos and S. Anantha Sayana will explore the basics of the IT audit field in each issue of the *Journal* in 2002.

To contact S. Anantha Sayana, the author of this issue's colun, with any comments or questions, e-mail sas-pia@powai.ltindia.com.

Information systems audit is a part of the overall audit process, which is one of the facilitators for good corporate governance. While there is no single universal definition of IS audit, Ron Weber has defined it (EDP auditing--as it was previously called) as "the process of collecting and evaluating evidence to determine whether a computer system (information system) safeguards assets, maintains data integrity, achieves organizational goals effectively and consumes resources efficiently."[1]

Information systems are the lifeblood of any large business. As in years past, computer systems do not merely record business transactions, but actually drive the key business processes of the enterprise. In such a scenario, senior management and business managers do have concerns about information systems. The purpose of IS audit is to review and provide feedback, assurances and suggestions. These concerns can be grouped under three broad heads:

1. Availability: Will the information systems on which the business is heavily dependent be available for the business at all times when required? Are the systems well protected against all types of losses and disasters?
2. Confidentiality: Will the information in the systems be disclosed only to those who have a need to see and use it and not to anyone else?
3. Integrity: Will the information provided by the systems always be accurate, reliable and timely? What ensures that no unauthorized modification can be made to the data or the software in the systems?

[*Author's note*: Of course there are other concerns that IS audit should look at, such as effectiveness, efficiency, value for money, return on investment, culture and people related issues. Such concerns will be addressed in IT Audit Basics columns in future issues of the *Journal* in 2002.]

Elements of IS Audit

An information system is not just a computer. Today's information systems are complex and have many components that piece together to make a business solution. Assurances about an information system can be obtained only if all the components are evaluated and secured. The proverbial weakest link is the total strength of the chain. The major elements of IS audit can be broadly classified:

1. **Physical and environmental review**--This includes physical security, power supply, air conditioning, humidity control and other environmental factors.
2. **System administration review**--This includes security review of the operating systems, database management systems, all system administration procedures and compliance.
3. **Application software review**--The business application could be payroll, invoicing, a web-based customer order processing system or an enterprise resource planning system that actually runs the business. Review of such application software includes access control and authorizations, validations, error and exception handling, business process flows within the application software and complementary manual controls and procedures. Additionally, a review of the system development lifecycle should be completed.
4. **Network security review**--Review of internal and external connections to the system, perimeter security, firewall review, router access control lists, port scanning and intrusion detection are some typical areas of coverage.
5. **Business continuity review**--This includes existence and maintenance of fault tolerant and redundant hardware, backup procedures and storage, and documented and tested disaster recovery/business continuity plan.
6. **Data integrity review**--The purpose of this is scrutiny of live data to verify adequacy of controls and impact of weaknesses, as noticed from any of the above reviews. Such substantive testing can be done using generalized audit software (e.g., computer assisted audit techniques).

All these elements need to be addressed to present to management a clear assessment of the system. For example, application software may be well designed and implemented with all the security features, but the default super-user password in the operating system used on the server may not have been changed, thereby allowing someone to access the data files directly. Such a situation negates whatever security is built into the application. Likewise, firewalls and technical system security may have been implemented very well, but the role definitions and access controls within the application software may have been so poorly designed and implemented that by using their user IDs, employees may get to see critical and sensitive information far beyond their roles.

It is important to understand that each audit may consist of these elements in varying measures; some audits may scrutinize only one of these elements or drop some of these elements. While the fact remains that it is necessary to do all of them, it is not mandatory to do all of them in one assignment. The skill sets required for each of these are different. The results of each audit need to be seen in relation to the other. This will enable the auditor and management to get the total view of the issues and problems. This overview is critical.

Risk-based Approach

Every organization uses a number of information systems. There may be different applications for different functions and activities and there may be a number of computer installations at different geographical locations.

The auditor is faced with the questions of what to audit, when and how frequently. The answer to this is to adopt a risk-based approach.

While there are risks inherent to information systems, these risks impact different systems in different ways. The risk of nonavailability even for an hour can be serious for a billing system at a busy retail store. The risk of unauthorized modification can be a source of frauds and potential losses to an online banking system. A batch processing system or a data consolidation system may be relatively less vulnerable to some of these risks. The technical environments on which the systems run also may affect the risk associated with the systems.

The steps that can be followed for a risk-based approach to making an audit plan are:

1. Inventory the information systems in use in the organization and categorize them.
2. Determine which of the systems impact critical functions or assets, such as money, materials, customers, decision making, and how close to real time they operate.
3. Assess what risks affect these systems and the severity of impact on the business.
4. Rank the systems based on the above assessment and decide the audit priority, resources, schedule and frequency.

The auditor then can draw up a yearly audit plan that lists the audits that will be performed during the year, as per a schedule, as well as the resources required.

The Audit Process

The preparation before commencing an audit involves collecting background information and assessing the resources and skills required to perform the audit. This enables staff with the right kind of skills to be allotted to the right assignment.

It always is a good practice to have a formal audit commencement meeting with the senior management responsible for the area under audit to finalize the scope, understand the special concerns, if any, schedule the dates and explain the methodology for the audit. Such meetings get senior management involved, allow people to meet each other, clarify issues and underlying business concerns, and help the audit to be conducted smoothly.

Similarly, after the audit scrutiny is completed, it is better to communicate the audit findings and suggestions for corrective action to senior management in a formal meeting using a presentation. This will ensure better understanding and increase buy-in of audit

recommendations. It also gives auditees an opportunity to express their viewpoints on the issues raised. Writing a report after such a meeting where agreements are reached on all audit issues can greatly enhance audit effectiveness.

Key Challenge

IS audit often involves finding and recording observations that are highly technical. Such technical depth is required to perform effective IS audits. At the same time it is necessary to translate audit findings into vulnerabilities and businesses impacts to which operating managers and senior management can relate. Therein lies a main challenge of IS audit.

End Notes

1 Weber, Ron, *EDP Auditing--Conceptual Foundations and Practice*

S. Anantha Sayana, CISA, CIA
is deputy general manager of corporate audit services with Larsen & Toubro Limited, India. He has over 12 years of experience in IS audit and internal audit in banking, manufacturing and services industries spanning a variety of applications and technical platforms. He also is a past president of the ISACA Mumbai Chapter.