Monitoring Security and Auditing of IT Operations

Compiled By:
A.N.M. Tawhidul Islam, AVP
AB Wing, HO, IBBL

IT Security System, Monitoring of IT Security System

IT Security System

Information security (sometimes shortened to InfoSec) is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (electronic, physical, etc.)

Below are the typical terms you will hear when dealing with information security:

IT Security: Sometimes referred to as computer security, IT Security is information security when applied to technology (most often some form of computer system). It is worthwhile to note that a computer does not necessarily mean a home desktop. A computer is any device with a processor and some memory (even a calculator). IT security specialists are almost always found in any major enterprise/establishment due to the nature and value of the data within larger businesses. They are responsible for keeping all of the technology within the company secure from malicious cyber attacks that often attempt to breach into critical private information, or gain control of the internal systems.

The **CIA triad (confidentiality, integrity and availability)** is one of the core principles of information security.

There is continuous debate about extending this classic trio.[citation needed] Other principles such as Accountability have sometimes been proposed for addition – it has been pointed out[citation needed] that issues such as Non-Repudiation do not fit well within the three core concepts, and as regulation of computer systems has increased (particularly amongst the Western nations) Legality is becoming a key consideration for practical security installations.

In 2002, Donn Parker proposed an alternative model for the classic CIA triad that he called the six atomic elements of information. The elements are confidentiality, possession, integrity, authenticity, availability, and utility.

1. **Confidentiality:** Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems. For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. Confidentiality is necessary (but not sufficient) for maintaining the privacy of the people whose personal information a system holds.
2. **Integrity:** In information security, integrity means that data cannot be modified undetectably. Integrity is violated when a message is actively modified in transit. Information security systems typically provide message integrity in addition to data confidentiality.
3. **Availability:** For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks.

4. **Authenticity:** In computing, e-Business, and information security, it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim to be.
5. **Non-repudiation:** In law, non-repudiation implies one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction.

IT Auditing System

An information technology audit, or information systems audit, is an examination of the management controls within an Information technology (IT) infrastructure. The evaluation of obtained evidence determines if the information systems are safeguarding assets, maintaining data integrity, and operating effectively to achieve the organization's goals or objectives. These reviews may be performed in conjunction with a financial statement audit, internal audit, or other form of attestation engagement.

IT audits are also known as "automated data processing (ADP) audits" and "computer audits". They were formerly called "electronic data processing (EDP) audits".

CAAT- Computer Assisted Auditing Tools

Purpose of IT Auditing

An IT audit is different from a financial statement audit. While a financial audit's purpose is to evaluate whether an organization is adhering to standard accounting practices, the purposes of an IT audit are to evaluate the system's internal control design and effectiveness. This includes, but is not limited to, efficiency and security protocols, development processes, and IT governance or oversight. Installing controls are necessary but not sufficient to provide adequate security. People responsible for security must consider if the controls are installed as intended, if they are effective if any breach in security has occurred and if so, what actions can be done to prevent future breaches. These inquiries must be answered by independent and unbiased observers. These observers are performing the task of information systems auditing. In an Information Systems (IS) environment, an audit is an examination of information systems, their inputs, outputs, and processing.

Types of IT audits

Various authorities have created differing taxonomies to distinguish the various types of IT audits. Goodman & Lawless state that there are three specific systematic approaches to carry out an IT audit:

1. **Technological innovation process audit**. This audit constructs a risk profile for existing and new projects. The audit will assess the length and depth of the company's experience in its chosen technologies, as well as its presence in relevant markets, the organization of each project, and the structure of the portion of the industry that deals with this project or product, organization and industry structure.
2. **Innovative comparison audit**. This audit is an analysis of the innovative abilities of the company being audited, in comparison to its competitors. This requires examination of company's research and development facilities, as well as its track record in actually producing new products.
3. **Technological position audit**: This audit reviews the technologies that the business currently has and that it needs to add. Technologies are characterized as being either "base", "key", "pacing" or "emerging".

IT Audit process

The following are basic steps in performing the Information Technology Audit Process:

1. Planning
2. Studying and Evaluating Controls
3. Testing and Evaluating Controls
4. Reporting
5. Follow-up

Advantages of IT Auditing over conventional Auditing System

1. IT auditing is the process of evaluating and assessing IT assets and processes to insure the implementation of best practices. IT Audits validate evidence to determine whether IT systems have been designed to effectively and efficiently support an organization.
2. Traditional auditing is about the evaluation of an organization's financial systems and processes. The primary objective of traditional auditing is to detect fraud. Traditional auditing focuses mostly on integrity of the financial transactions and compliance to the policies and procedures of an organization.
3. While IT Audits includes revenue recognition, accounts receivable, and account payables business processes, the audit itself is often automated using some third-party tools or home-grown customized IT applications.
4. IT audit is a paradigm shift for auditors who are usually involved in traditional auditing.
5. Traditional auditing is a multi-year, periodic procedure to assess the way organizations carry out their business that impacts the financial statement.
6. Traditional auditing is time consuming and highly manual. A financial audit is an intensive project going over several thousand records focusing on compliance of the transactions to organization's policies.
7. Traditional auditing is done to ascertain the validity and reliability of information presented to shareholders, investors and regulatory agencies.
8. In contrast, IT auditing is not often about identifying issues.
9. Traditional auditing is sometimes expanded to different domains including accounting, quality, energy, etc.
10. As there are several vendor-based built-in solutions or plug-in tools available to identify IT vulnerabilities, it makes sense to use these tools to assess IT environments.
11. Many IT auditors may not have up-to-date training or expertise for executing a configuration audit of a complex environment such as an ERP (Enterprise Resource Planning) system. The complexity and the variations of IT system implementation render itself for an automated scanner to verify the settings per vendor recommendations, best practices and other standards.
12. As more and more organizations are moving from implementation of new technologies to more maintenance mode, IT audit focuses not so much on finding problems. IT audit is focused on fresh look at processes and setup comparing the way the organization's IT is run with the industry peers, and the recommended best practices by subject-matter-experts and vendors.
13. In essence, an end-to-end IT audit identifies opportunities for improvement in implementing best practices and introducing or fine-tuning business policies, processes and procedures. In

the case of regulatory compliance, rules governing the law requires an assessment of IT systems internal controls by an independent auditors.

14. The focus of traditional auditing is financial accounting. Integrity of financial transactions is audited to create a comfort level for the organization's stakeholder. In IT audit, the focus is only the IT systems that are in scope for the audit objective. As more and more business processes are being automated using sophisticated end-to-end IT systems, IT audit is an integral part of the audit.

Areas	Traditional Audit	IT Audit
Objective	Detect Fraud	Assess IT Systems
Scope	Financial, Energy, Tax, etc.	Technology Practices
Required Expertise	Finance, Domain Specific	IT & Audit
Approach	Risk-based	Risk-based and best practices
Method	Manual	Semi-automated

Effective Managerial Decisions from IT Auditing

Below we discuss five key areas in which IT auditors can add value to organizations for effective managerial decisions. Of course, the quality and depth of a technical audit is a prerequisite to adding value. The planned scope of an audit is also critical to the value added. Without a clear mandate on what business processes and risks will be audited, it is hard to ensure success or added value.

1. IT audit Reduce the risk of branch and HO IT operation. The planning and execution of an IT audit consists of the identification and assessment of IT risks in an organization.

IT audits usually cover risks related to confidentiality, integrity and availability of information technology infrastructure and processes. Additional risks include effectiveness, efficiency and reliability of IT.

In short, the organization needs to know where the risks are and then proceed to do something about them.

2. Strengthen controls (and improve security). After assessing risks as described above, controls can then be identified and assessed. Poorly designed or ineffective controls can be redesigned and/or strengthened.

3. Comply with regulations. Wide ranging regulations at the federal and state levels include specific requirements for information security. The IT auditor serves a critical function in ensuring that specific requirements are met, risks are assessed and controls implemented.

4. Facilitate communication between business and technology management. An audit can have the positive effect of opening channels of communication between an organization's business and technology management. Auditors interview, observe and test what is happening in reality and in practice. The final deliverables from an audit are valuable information in written reports and oral presentations. Senior management can get direct feedback on how their organization is functioning.

5. Improve IT Governance and Decision. IT Governance is the responsibility of executives and board of directors, and consists of the leadership, organizational structures and processes that ensure that the enterprise's IT sustains and extends the organization's strategies and objectives.

The leadership, organizational structures and processes referred to in the definition all point to IT auditors as key players. Central to IT auditing and to overall IT management is a strong understanding of the value, risks and controls around an organization's technology environment. More specifically, IT auditors review the value, risks and controls in each of the key components of technology - applications, information, infrastructure and people.

Another perspective on IT governance consists of a framework of four key objectives which are also discussed in the IT Governance Institute's documentation:

- IT is aligned with the business
- IT enables the business and maximizes benefits
- IT resources are used responsibly
- IT risks are managed appropriately

IT auditors provide assurance that each of these objectives is met. Each objective is critical to an organization and is therefore critical in the IT audit function.

To sum up, IT auditing adds value by reducing risks, improving security, complying with regulations and facilitating communication between technology and business management. Finally, IT auditing improves and strengthens overall IT governance.