COURSE FACILITATOR

CHRISPUS ALUKWE AKHONYA – CEH|MSc|BSc|CSCU:

alukchris@gmail.com
+254720474923 | +254780474923
caakhonya@usiu.ac.ke

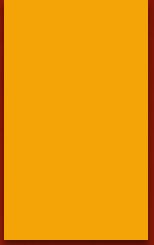CEH-Alukwe - 0720474923 | 0780474923 | caakhonya@kabarak.ac.ke | alukchris@gmail.Com

Introduction

Definition and Objectives

- ▶ IT audit is the examination and evaluation of an organization's information technology infrastructure, policies and operations.

- ▶ Process of collecting and evaluating evidence to determine whether a computer system

safeguards assets, maintains data integrity,

- ➢ Allows organizational goals to be achieved effectively and uses resources efficiently.

The objectives of IS audit include assessment and evaluation of processes that ensure:

i. Asset safeguarding –'assets' which include the following five types of assets;

➢ Data objects in their widest sense, (i.e., external and internal, structured and non- structured, graphics, sound, system documentation etc).

- Application system is understood to be the sum of manual and programmed procedures.

- Technology covers hardware, operating systems, database management systems, networking, multimedia, etc.

- Resources to house and support information systems, supplies etc.

- Staff skills, awareness and productivity to plan, organize, acquire, deliver, support and monitor information systems and services
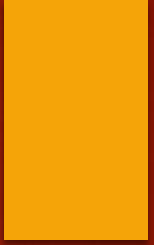
The objectives of IS audit Cont….

- Information systems are the lifeblood of any large business.

- 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:

ii. **Ensures that the following seven attributes of data or information are maintained:**

➤ **Effectiveness** - deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner.

➤ **Efficiency -** concerns the provision of information through the optimal (most productive and economical) usage of resources.

➤ **Confidentiality -** concerns protection of sensitive information from unauthorized disclosure.

➤ **Integrity** - relates to the accuracy and completeness of information as well as to its validity in accordance with the business' set of values and expectations.

➤ **Availability -** relates to information being available when required by the business process, and hence also concerns the safeguarding of resources.

➢ **Compliance** - deals with abiding with those laws, regulations and contractual arrangements to which the business process is subject; i.e., externally imposed business criteria. This essentially means that systems need to operate within the ambit of rules, regulations and/or conditions of the organization.

Phases of the Audit Process

1. **Planning.**
2. **Definition of audit objectives and scope.**
3. **Evidence collection and evaluation.**
4. **Documentation and reporting.**

Planning

1. *Preliminary assessment and information gathering.*

2. *Understanding the organization.*

The IT auditor has to gather knowledge and inputs on the aspects of the entity to be audited ;

- IT audits are also known as "automated data processing (ADP) audits" and "computer audits".

- They were formerly called "electronic data processing (EDP) audits".

- 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.

1.1 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. " or "emerging".

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 reviewstechnologies that the business currently has and that it needs to add the.

Technologies are characterized as being either "base", "key", "pacing" or "emerging".

Others describe the spectrum of IT audits with five categories of audits:

Systems and Applications:

An audit to verify that systems and applications are appropriate, are efficient, and are adequately controlled to ensure valid, reliable, timely, and secure input, processing, and output at all levels of a system's activity.

1.Information Processing Facilities:

An audit to verify that the processing facility is controlled to ensure timely, accurate, and efficient processing of applications under normal and potentially disruptive conditions.

2.Systems Development:

An audit to verify that the systems under development meet the objectives of the organization and to ensure that the systems are developed in accordance with generally accepted standards for systems development.

3.Management of IT and Enterprise Architecture:

An audit to verify that IT management has developed an organizational structure and procedures to ensure a controlled and efficient environment for information processing.

4.Client/Server,Telecommunications, Intranets, and Extranets:

An audit to verify that telecommunications controls are in place on the client (computer receiving services), server, and on the network connecting the clients and servers.

Elements of IS Audit

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:

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).* To organize the audit, an audit plan shall be developed.

Q & A

Planning IT Audit