BBC3 - ISA - INFORMATION SYSTEMS AUDIT CONCEPTS

Subchapter 1: Introduction to Information Technology/System Audit

1.1. Introduction Definitions:

Auditing

Auditing is a systematic process by which a competent, independent person objectively obtains and evaluates evidence regarding assertions about an economic entity or event for the purpose of forming an opinion about and reporting on the degree to which the assertion conforms to an identified set of standards

An audit is a systematic, objective examination of one or more aspects of an organization that compares what the organization does to a defined set of criteria or requirements.

IS Audit/ IT Audit

- *"a systematic and independent examination of information systems environment to ascertain that computer system safeguards assets, maintains data integrity, allows organizational goals to be achieved effectively and uses resources efficiently".*

- *Information systems audit is a process to collect and evaluate evidence to determine whether the information systems safeguard assets, maintain data integrity, achieve organizational goals effectively and consume resources efficiently*

- *An IT audit can be defined as any audit that encompasses review and evaluation of automated information processing systems, related non-automated processes and the interfaces among them.*

An information system (IS) audit or information technology (IT) audit is an examination of the controls within an entity's Information technology infrastructure. Information technology (IT) auditing examines processes, IT assets, and controls at multiple levels within an organization to determine the extent to which the organization adheres to applicable standards or requirements. These reviews may be performed in conjunction with a financial statement audit, internal audit, or other form of attestation engagement.

1.1.1. IS Audit Versus Financial Audit

An IS audit is not entirely similar to a financial statement audit. An IS audit, tends to focus on determining risks that are relevant to information assets, and in assessing controls in order to reduce or mitigate these risks. An IT audit may take the form of a "general control review" or an "specific control review". Regarding the protection of information assets, one purpose of an IS audit is to review and evaluate an organization's information system's availability, confidentiality, and integrity by answering the following questions:

1. Will the organization's computerized systems be available for the business at all times when required? (Availability)
2. Will the information in the systems be disclosed only to authorized users? (Confidentiality)
3. Will the information provided by the system always be accurate, reliable, and timely? (Integrity).

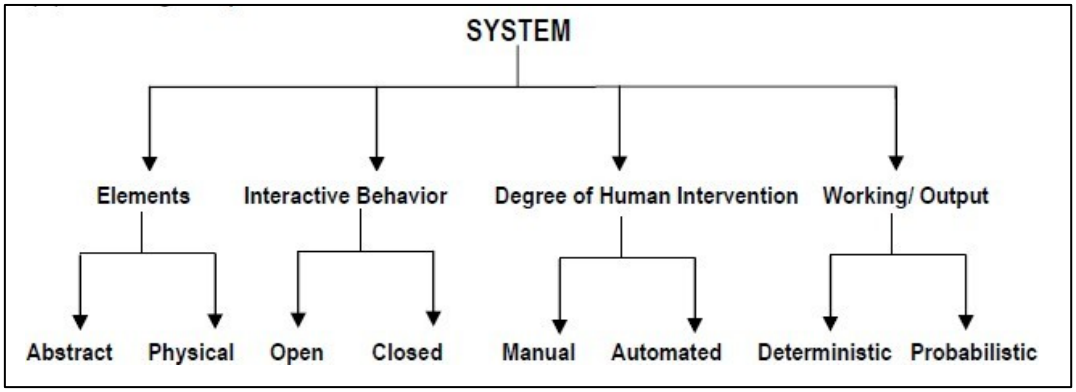
1.2. Information Systems Concepts

The term system may be defined as an orderly arrangement of a set of interrelated and interdependent elements that operate collectively to accomplish some common purpose or goal.

A computer based information system is also a system which is a collection of people, hardware, software, data and procedures that interact to provide timely information to authorized people who need it.

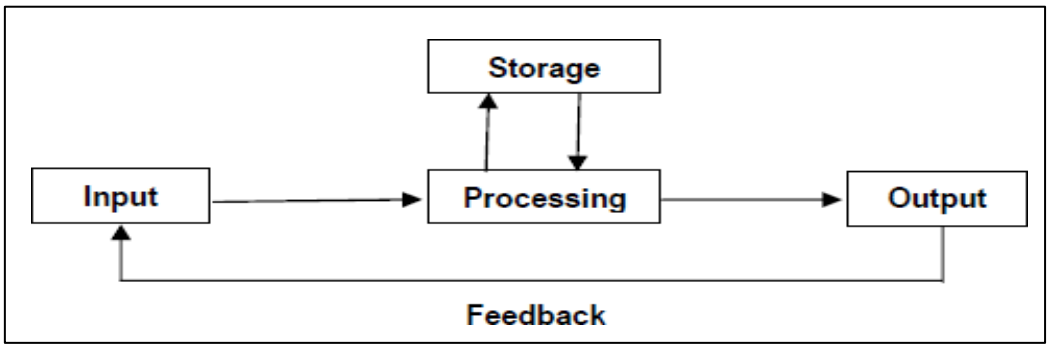
Information Systems can be classified on the basis of following parameters:

1) Elements
2) Interactive Behavior
3) Degree of Human Intervention
4) Working / Output



1.2.1. General Model of a IS

A general model of a physical system is input, process and output.



1.2.2. Information Systems Components

IS Component include

1) Hardware.
2) Software
3) Procedures
4) Data
5) People/Users

1.2.3. Information System Environment - Components

1) System Boundary: All systems function within some sort of environment, which is a collection of elements. These elements surround the system and often interact with it.
2) Subsystem: A subsystem is a part of a larger system. Each system is composed of subsystems, which in turn are made up of other subsystems, each sub-system being delineated by its boundaries. The interconnections and interactions between the subsystems are termed Interfaces. Interfaces occur at the boundary and take the form of inputs and outputs.
3) Supra-System: A Supra-System refers to the entity formed by a system and other equivalent systems with which it interacts.

1.2.4. Information System and its role in management

An Information System can be considered as an arrangement of a number of elements that provides effective information for decision-making and/or control of some functionalities of an organization. Information is an entity that reduces uncertainty about an event or situation. Some of important implications of information system in business are as follows:

1) Information system helps managers in effective decision-making to achieve the organizational goal.
2) Based on well-designed Information system, an organization will gain edge in the competitive environment.
3) Information systems help take right decision at the right time.
4) Innovative ideas for solving critical problems may come out from good Information system.
5) Knowledge gathered though Information system may be utilized by managers in unusual situations.
6) Information system is viewed as a process, it can be integrated to formulate a strategy of action or operation.

1.3. IS Audit Purpose/ Goals

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. Information systems audit is an ongoing process of;

a) Evaluating controls;
b) Suggesting security measures for the purpose of safeguarding assets/resources and Maintaining data integrity,
c) Improving system effectiveness and system efficiency for the purpose of attaining organization goals.

IS auditing considers all the potential hazards and controls in information systems. It focuses on issues like operations, data, integrity, software applications, security, privacy, budgets and expenditures, cost control, and productivity. The Goals is to ensure;

a) **Safeguarding IS assets:** The Information systems assets of the organization must be protected by a system of internal controls. It includes protection of hardware, software, facilities, people, data, technology, system documentation and supplies.
   IS assets includes;
   1. Data; Data objects in their widest sense, i.e., external and internal, structured and non-structured, graphics, sound, system documentation etc.
   2. Application Systems; Application system is understood to be the sum of manual and programmed procedures.
   3. Technology; Technology covers hardware, operating systems, database management systems, networking, multimedia, etc.
   4. Facilities; Resources to house and support information systems, supplies etc.
   5. People; Staff skills, awareness and productivity to plan, organize, acquire, deliver, support and monitor information systems and services.

b). **Ensuring Data Integrity**: Data integrity includes the safeguarding of the information against unauthorized addition, deletion, modification or alteration. Ensures that the following attributes of data or information are maintained.
   1) 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.
   2) Efficiency - concerns the provision of information through the optimal (most productive and economical) usage of resources. Deals with System efficiency – efficient systems use optimum resources to achieve the required objectives
   3) Confidentiality - concerns protection of sensitive information from unauthorized disclosure.
   4) 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.
   5) Availability - relates to information being available when required by the business process, and

hence also concerns the safeguarding of resources.

6) Compliance - deals with complying 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 organisation.
7) Reliability of information - relates to systems providing management with appropriate information for it to use in operating the entity, in providing financial reporting to users of the financial information, and in providing information for reporting to the regulatory bodies regarding compliance with laws and regulations.
8) Accuracy: Data should be accurate. Inaccurate data may lead to wrong decisions and thereby hindering the business development process.
9) Completeness: Data should be complete

c). Achieve organizational goals effectively and consume resources efficiently.

Guidelines are available to assist auditors in their jobs, such as those from Information Systems Audit and Control Association (ISACA)

1.4. Information Systems Audit Objectives

IS audit evaluates the adequacy of the security controls and informs the management with suitable conclusions and recommendations. The Objectives of an information systems audit is to achieve the following nine objectives:

1) Ensure adequacy and effectiveness of internal controls.
2) Ensure that resources are allocated to constituents of information systems in an efficient and effective manner.
3) Provide assurance that systems-related assets are safeguarded.
4) Ensure that information is accurate, available on request, and reliable.
5) Provide reasonable assurance that all errors, omissions, and irregularities are prevented, detected, corrected, and reported.
6) Review the systems to ensure compliance to policies, procedures, standards, and legal requirements.
7) Review application and operation systems to ensure that needs of the users are met, necessary compliances are achieved, audit trails are incorporated, documentation is completed, and systems data integrity and security are maintained.
8) Identify and recognize potential threats that can compromise confidentiality, integrity, and availability of information assets.
9) Ensure that management takes appropriate detective, corrective, and preventive actions.

1.5. Categories and Types of IS Audits

There are several types of information system audits and assurance services mostly related to the areas of availability, confidentiality, and integrity. The IS audit is a systematic approach that aims to provide reasonable assurances, on test-basis, regarding the adequacy of the controls used in the governance over IT resources.

Categories

There are three basic kinds of IS Audits that may be performed:

1) General Controls Review: A review of the controls which govern the development, operation, maintenance, and security of application systems in a particular environment. This type of audit might involve reviewing a data center, an operating system, a security software tool, or processes and procedures (such as the procedure for controlling production program changes), etc.
2) Application Controls Review: A review of controls for a specific application system. This would

involve an examination of the controls over the input, processing, and output of system data. Data communications issues, program and data security, system change control, and data quality issues are also considered.

3) System Development Review: A review of the development of a new application system. This involves an evaluation of the development process as well as the product. Consideration is also given to the general controls over a new application, particularly if a new operating environment or technical platform will be used.

Types

Common types of IS Audit Includes;

a) **System Audits:** A system audit is an audit of the controls designed and implemented into the system to ensure the integrity of the data processed by the system and maintain the proper functionality of system processes.

b) **Application Audits:** The audit of an information system application is an audits of the controls placed over an enterprise information system which are usually designed to ensure the Effectiveness, Efficiency, Confidentiality, Availability, Reliability, and Compliance of information and processing in an enterprise IT environment.

c) **Compliance Audits:** Compliance audits provide management with tool for the internal review of compliance in their operating units. The audit program one or many compliance areas. Each area may be applicable to a particular operating unit, depending on its activities, funding, regulatory administrative rules, or any other pre-defined criterion.

d) **Security Audits:** Security audits are aimed to provide comprehensive and cost-effective network vulnerability assessments by disclosing number of vulnerability tests, provide detailed and comprehensive report on weaknesses found, and depending on the classification of the system as to "mission critical", suggest remedies, solutions, and preventive measures to reduce or eliminate vulnerabilities. The audit will also provide program(s) to update the list of vulnerability and perform testing on an ongoing basis.

e) **Performance Audits:** Performance audits entail an objective and systematic examination of evidence to provide an independent assessment of the performance and management of a program against objective criteria as well as assessments that provide a prospective focus or that synthesize information on best practices or cross-cutting issues.

1.6. Benefits of IS Auditing

a) Strategic Benefits:
   - Integrity of Data produced by the Organization.
   - Enhanced Customer Confidence.

b) Operational Benefits:
   - Increased Employee Productivity and Morale.
   - Integrity of Data enables Management to make informed and accurate decisions.

c) Financial Benefits:
   - Increased Hardware Performance.
   - Cost of theft of IS Assets is reduced.

d) Technical Benefits:
   - Management Decisions on Computer-Processed Data are reliable.
   - Business Partners trust Organization's Management Control and distribution of sensitive Data

1.7. IS Audit Requirements

Critical requirements of an information systems audit in terms of both input and delivery includes;

1.7.1. Risk Analysis

The scope of an information systems audit includes verifying the existence and performance of controls. The selection of the controls to test remains a critical decision for the information systems auditor and will have a major role in determining the quality of the audit. In order to ensure adequate coverage of testing, the auditor is required to prioritize testing of controls. Prioritization essentially depends on the corresponding loss exposure to the auditee in the event of the failure of a specific control. The likelihood of a control failing, and even being activated, is uncertain. This calls for a risk analysis exercise on the part of the auditor.

Risk factors inherent in business operations include the following nine examples:

a) Access risk, referring to the risk of an unauthorized user securing access to information assets.
b) Business disruption risk, or the risk of non-availability of services from information systems resources.
c) Credit risk, such as the failure of a counterparty honoring their payment obligation.
d) Customer service risk, referring to the risk of customers being deprived of services.
e) Data integrity risk, or the risk of a possible compromise of data integrity that may arise for various reasons,including unauthorized access.
f) Financial/external report misstatement risk, referring to the risk that reports prepared by the entity contain misstatements and errors.
g) Fraud risk, referring to the risk of losses arising out of fraud committed using information systems resources.
h) Legal and regulatory risk, referring to risk of noncompliance to legal and regulatory requirements and consequences thereof.
i) Physical harm risk, referring to the risk of suffering from bodily harm.

The auditor needs to understand how control failure in information systems can lead to a vulnerable environment. In order to successfully conduct risk analysis, there is need to understand the concepts of threats, vulnerabilities, exposure, likelihood, and attack in an information system.

1.7.2. IS Threats, Vulnerability, Exposure, Likelihood, and Attacks

Understanding threat, vulnerability, exposure, likelihood, and attack forms the basis of an information systems audit requirement.

a) A threat is the potential event that could exploit vulnerability in a system, leading to the entity being exposed to chances of suffering a loss. The harm to an information system may be in the form of a compromise in the confidentiality, integrity, or availability of an information systems resource.
b) Vulnerability is the weakness in the system that can potentially be exploited by threats. The weakness may be in design, technology, implementation, or any other aspect of the information systems assets. Extent of safeguards implemented often determines the level of vulnerability. Determining vulnerabilities involves security evaluation of the system, including inspection of safeguards implemented, testing their response, and conducting penetration analysis.
c) Exposure is the extent of loss an entity is likely to face when a risk materializes. The loss may not be restricted to the immediate future but may also occur in the long run. Examples of loss include loss of business, loss of reputation, compromise of privacy, and even injury or loss of human life.
d) Likelihood is an estimation of the probability that the threat will attempt to exploit the vulnerability and, upon being able to successfully exploit it, cause loss to the entity. The presence and strengths of threats, and the effectiveness of safeguards, influence the likelihood of the threat successfully exploiting the vulnerability.
e) Attack is the act of the threat seeking to exploit the vulnerability through a set of actions to

compromise confidentiality, integrity, and availability of an information systems asset. Attacks seek to overcome the safeguards and controls implemented by the auditee. The extent to which the safeguards are compromised by the attack will determine the extent of consequential loss.

1.7.3. Information Systems Control Objectives

Information assets have a value in the entity and are required to be suitably protected. Information security has the following three characteristics:

a) Confidentiality: Ensuring accessibility only to those authorized to have access.
b) Integrity: Ensuring that information is accurate and complete throughout the cycle of input, processing, and output.
c) Availability: Ensuring need-based access to information for all authorized users.

In order to ensure that security of information systems is preserved, the entity needs to ensure that usage of information systems assets and related processes, whether computerized or manual, is governed by an internal control system.
Controls objectives will be discussed in chapter 3

1.7.4. Information Systems Audit Objectives

As discussed in 1.3. above

1.7.5. System Effectiveness and Efficiency

During the course of information systems audit, an auditor is often required to comment on the effectiveness and efficiency of a system. An information systems auditor is required to know the difference between the two, which is described below.

1) Effectiveness evaluation determines whether the system is achieving its objectives and whether the system should be continued, modified, upgraded, or scrapped. Effectiveness analysis may be done at the design stage to ensure that user needs are being fulfilled and the system is achieving its implementation objectives.
2) Efficiency of a system is reflected by usage of the minimum amount of resources to achieve its objectives. The resources may be of different kinds, including machine time, peripherals, system software, application software, and human resources.

1.7.6. Information Systems Abuse

Information systems abuse may manifest itself in various ways. This may include the following:

1) Destruction of assets: Hardware, software, networking infrastructure, data, facilities, documentation, files, and so forth may be destroyed.
2) Theft of assets: Illegal removal of hardware, software, data, documentation, or peripherals may take place.
3) Modification of assets: Unauthorized access and modification of hardware, software, data, or documentation may affect safeguarding and security of information systems assets. Often unauthorized modification of assets may lead to unknown incompatibility with other components, which can seriously compromise functionality of the system.
4) Privacy violation: Privacy of data relating to a person or an organization may be compromised, which could have a far-reaching impact, including loss of business. One of the most common examples is compromise of confidentiality of customer data.
5) Disruption of operations: Day-to-day operations of the information systems functions may be disturbed, and at the extreme this could temporarily disrupt the working of the entire system.
6) Unauthorized use of assets: Hardware, software, data, facilities, documentation, peripherals, or supplies may be used for unauthorized purposes that may cause losses to the organization.

1.7.7. Asset Safeguarding Objective and Process

One of the primary problems associated with safeguarding information assets is identification of the same. The problem of identification is accentuated by the fact that often these assets are intangible in nature. The task of having an information systems asset safeguarding mechanism in place involves a series of functions and procedures, including the following four areas:

a) Compiling a functional information technology asset list:
b) Information technology systems detailing: Detailed information includes names of hardware, software, network platform, applications with vendor details, installation location, year of installation, major upgrade history, and so forth.
c) Asset safeguarding: This process focuses on whether information systems assets could be used or have been used for unauthorized purposes and the consequent losses that have occurred or could have occurred.
d) Assigning probabilities: The entity needs to assign probabilities to different losses that could arise out of failure or a compromise of safeguarding mechanisms of the information assets.

1.7.8. Evidence Collection and Evaluation

An area of concern for an information systems auditor is collection of evidence during audit. Auditors have to interact with the system to collect necessary evidence of the existence and efficiency of internal controls.

1.8. Systems Environment and Information Systems Audit

Computerization is a tool that gives organizations the capability to provide better customer service, to conduct better housekeeping, and so on, to enable optimization of the use of resources. To ensure that computerization takes care of existing and emerging needs of the organization, the following nine issues must be considered:

1. Standardization of hardware, operating systems, system software, and applications: Failure to ensure such standardization creates complex technology management issues, which often manifests through involvement of multiple systems in a single process instead of an integrated process ensuring non- duplication of functions.
2. Use of software to facilitate interconnectivity of systems intensifies the need for a systems audit to ensure that information flow is smooth and not compromised.
3. The need for high levels of security not only calls for technical competence but also requires continuous testing of efficiency and searching for new, emerging vulnerabilities as well.
4. Communication and networking involving the use of networks facilitate establishing a centralized database and distributed processing on one hand, but on the other hand expose the entity to the risk of security breach from multiple sources. Consequently the scope of a systems audit enlarges and involves more complex testing.
5. A technology infrastructure with periodic up grades often leads to migration from one system to another. The information systems audit is required to keep pace with not only the technology but also the maturity of the organization. A more matured organization entrusts more critical resources to the information system and at the same time becomes more susceptible to a systems breach.
6. The need for business process reengineering is a consequence of the evolution of business complexity, which necessarily calls for an enlarged role of the information systems. Such reengineering brings about serious challenges to smooth migration and maintenance of data integrity.
7. Issues of human relations in a computerized environment are perhaps one of the greatest challenges for an information systems audit. Unpredictable and indispensable as they are, human resources define the fine line differentiating the success or failure of an information technology project. The information systems auditor finds the task of assessing adequacy and efficiency of such controls extremely difficult and often subjective.
8. Sharing of technology experiences between organizations and between various levels of an organization enriches the quality of performance as it ensures that the same mistake is not repeated

twice. The comfort level of an information systems auditor is greater in an organization that enables a system of internal learning.

9. An information systems audit assumes greater importance in the face of the increased use of credit and debit cards and e-commerce interface in the regular functioning of an entity. These are activities that require closer monitoring as well as the assurance that the access and security aspects of these systems are well laid out.