

3. Control objectives

Information Systems Controls

The increasing use of information technology in large number of organizations has made it imperative that appropriate information systems are implemented in an organization. Control is defined as Policies, Procedures, practices and enterprise structure that are designed to provide reasonable assurance that business objectives will be achieved and undesired events are prevented or detected and corrected.

Need for Control and Audit of Information System

Due to technology impact in business that increased the ability to capture, store, analyze and process tremendous amounts of data and information by empowering the business decision maker. So safeguarding assets to maintain data integrity to achieve system effectiveness and efficiency is a significant control process.

Factors influencing an organization toward control and audit of computers and the impact of the information system audit function o organization are displayed as below

1. Organizational cost of data loss
2. Incorrect decision making
3. Costs of computer abuse
4. Value of computer hardware, software and personnel
5. High costs of imputer error
6. Maintenance of privacy
7. Controlled evolution of computer use
8. Information systems auditing
9. Asset safeguarding objectives
10. Data integrity objectives
11. System effectiveness objectives
12. System efficiency Objectives

Effects of Computers on Internal Controls

The internal controls within an enterprise in a computerized environment the major areas of impact with the goal of assets safeguarding, data integrity, system efficiency and effectiveness are discussed below

1. Personnel: Skilled and experienced staff for carrying out their work with objectives
2. Segregation of Duties: it is a key control in an information system. Segregation basically means that the stages in the processing of a transaction are split between different people, such that one person cannot process a transaction through from start to finish.
3. Authorization procedure: to ensure that transaction are approved.
4. Record Keeping: the controls over the protection and storage of documents, transaction details, and audit trails etc.
5. Access to assets and records: A client's financial data may be uses by unauthorized person form the remote location so data system security is must for business.
6. Management Supervision and Review: helps to deter and detect both errors and fraud.
7. Concentration of Programs and data: Transaction and master file data may be stored in a computer readable form on one computer installation or on a number of distributed installations.

Internal controls used within an organization comprise of the following five interrelated components.

1. Control environment
2. Risk assessment
3. Control activities
4. Information and communication
5. Monitoring

Effects of Computers on Audit

The two basic functions are carried out for the effects of computers on audit are discussed as below.

1. Changes to evidence Collection:

Changes in the audit trail say the existence of audit trail is key financial audit requirement, since without an audit trail, the financial auditor may have extreme difficulty in gathering sufficient, appropriate audit evidence to validate the figures in the client's accounts. The performance of evidence collection and understanding the reliability of control involves issues like

- a. Data retention and storage
- b. Absence of input documents
- c. Lack of visible trail
- d. Lack of visible output
- e. Audit evidence
- f. Legal issues

2. Changes to evidence evaluation

Evaluation of audit trail and evidence is to trace consequences of control strength and weakness through the system the evidence evaluation function of information systems leads to identify periodic and deterministic errors.

- a. System generated transactions
- b. Systematic error

The IS audit process

The audit of IS environment to evaluate the systems, practices and operation may include one or both of the following

- I. Assessment of internal controls within the IS environment to assure validity, reliability, and security information.
- II. Assessment of the efficiency and effectiveness of the IS environment in economic terms.

Responsibility of IS Auditor

The audit objective and scope of has a significant bearing on the skill and competence requirements of an IS auditor. The set of skill that is generally expected of an IS auditor include

1. Sound knowledge of business operations, practices and compliance requirements,
2. Sound possess the requisite professional technical qualification and certifications,
3. An good understanding of information risks and controls.
4. Knowledge of IT strategies, policy and procedure controls.
5. Ability to understand technical and manual controls relating to business continuity, and
6. Good knowledge of professional standards and best practices of IT controls and security

Functions of IS Auditor

IT auditors review risks relating to IT systems and processes, some of them are

1. Inadequate information security
2. Inefficient use of corporate resources or poor governance
3. Ineffective IT strategies, policies and practices
4. IT-related frauds (Phishing, Hacking etc.)

Categories of IS audits

1. Systems and applications
2. Information processing facilities
3. System development
4. Management of IT and enterprise architecture
5. Telecommunications, Intranets and extranets

Steps in Information Audit Technology

Different audit organization goes about IT auditing in different ways and individual auditors have their own favorite ways of working. It can be categorized into six stages

1. Scoping and pre-audit strategy: the auditors determine the main Areas/s of focus and any areas that are explicitly out-of-scope, based normally on some form of risk-based assessment.
2. Planning and processing: during the scope is broken down into greater level of detail, usually involving the generation of an audit work plan or risk-control-matrix.
3. Fieldwork: gathering evidence by interviewing staff and managers, reviewing documents, printouts and data, observing processes etc.
4. Analyses: SWOT, PEST(political, Economic, Social, Technology) techniques used for this
5. Reporting
6. Closure

Control Objectives for Information related technology (COBIT)

COBIT is a framework of generally applicable information systems security and control practices or IT control. The framework address the issue of control from these three vantage points or dimension

1. Business objectives: to satisfy business objectives, information must conform to certain criteria that COBIT refers to as business requirements of information
2. IT resources, which include people, application system, technology, facilities and data
3. IT procedures, which are broken into four domains: planning and organization, acquisition and implementation, delivery and support, and mentoring

Information Systems Control techniques

The basic purpose of information system controls in an organization is to ensure that the business objectives are achieved and undesired risk events are prevented or detected and corrected.

Categories of IT control

Based on the objective with which controls are designed or implemented, controls can be classified as

1. Preventive Controls:

Preventive control are those inputs, which are designed to prevent an error, omission or malicious act occurring. An example of a preventive control is the use of passwords to gain access to financial system. The board characteristics of preventive controls are

- I. A clear-cut understanding about the vulnerabilities of the assets
- II. Understanding probable threats
- III. Provision of necessary controls for probable threats from materializing

2. **Detective Control:** these controls are designed to detect errors, omissions or malicious acts that occur and report the occurrence. A example of a detective control would be a use of automatic expenditure profiling where management gets regular reports of spend to date against profiled spend.
 3. **Corrective Controls:** Corrective controls are designed to reduce the impact or correct an error once it has been detected.
 4. **Compensatory Controls:** controls are basically designed to reduce the probability of threats, which can exploit the vulnerabilities of an asset and cause a loss to that asset.
- Another Classification of controls is based on the nature of such controls with regard to the nature of IS resources to which they are applied
 1. Environmental Control: relating to housing IT resources such as power, A.C. etc
 2. Physical access control: relates to physical security of the tangible IS resources and intangible data stored in tangible resources
 3. Logical access control: operating system controls, software boundary controls etc
 4. IS operational Control: operation and its management related
 5. IS management Controls
 6. SDLC Controls: related to planning, design, testing, implementation of SDLC
 - Further, another category of control based on their functional nature
 1. Internal accounting control
 2. Operational control
 3. Administrative control

Organizational Control

Organization control techniques include documentation of

- a) Reporting responsibility and authority of each function
- b) Definition of responsibilities and objectives of each function
- c) Policies and procedures
- d) Job descriptions
- e) Segregation of duties

Management Controls

The control adopted by the management of an enterprise is to ensure that the information systems function correctly and that they meet the strategic business objectives. The control to consider when reviewing the management control of an IS system shall include

- a) Responsibility
- b) An official IT structure
- c) An IT steering Committee

Financial Control Techniques

These controls are generally defined as the procedures exercised by the system user personnel over source, transaction origination, documents before system input. The financial control techniques are numerous. A few examples are highlighted as below

- a) Authorization
- b) Budgets
- c) Cancellation of documents
- d) Documentation
- e) Dual control
- f) Input/output verification
- g) Safekeeping
- h) Segregation of duties
- i) Sequentially numbered documents
- j) Supervisory review

Audit Trails

Audit trails are logs that can be designed to record activity at the system, application, and user level. When properly implemented, audit trails provide an important detective control to help accomplish security policy objectives. Audit trail controls attempt to ensure that a chronological record of all the events that have occurred in system is maintained. The main objectives of audit trail are as follows

1. Detecting unauthorized access to the system
2. Facilitating the reconstruction of events, and
3. Promoting personnel accountability.

Boundary Control techniques

The major controls of the boundary system are the access control mechanisms. Boundary control techniques are as below

1. Cryptography: deals with programs transforming data into codes that are meaningless to anyone who does not possess the authentication to access the respective system resource or file.
2. Passwords
3. Personal Identification number
4. Identification Cards

System Development and Acquisition Control

It is important to have a formal, appropriate and proven methodology to govern the development, acquisition, implementation, and maintenance of information systems and related technologies. Key elements in system development and acquisition control are given in following table

Control Category	Threats/Risks	Controls
System development and acquisition controls	System development projects consume excessive resources	Long-range strategic master plan, data processing schedules, assignment of each project to manage team, project development plan, project milestones, performance evaluations, system performance measurements
Change Management Controls	System development project consume excessive resources, unauthorized system changes.	Change management control policies and procedures, periodic review of all systems for needed changes, standardized format for changes, log and review change requests, assess impact of changes on system reliability.

Copyright Violations

Software programs can easily be copied or installed on multiple computers. It is necessary for organization to specifically address software piracy in training, in policy and procedures or in the application of general internal controls.

Service Level Agreements (SLA)

The SLA is a formal agreement between a customer requiring services and the organization that is responsible for providing those services. It is not a legal contract in itself, but an essential component of it. An SLA states the required performance of the system in terms of its availability to users, response times and numbers of transaction processed and any other suitable criteria meaningful to the user.

Information Classification

Information classification is the conscious decision to assign a level of sensitivity to information as it is being created, amended, enhanced, stored or transmitted. The classification of information and documents is essential if one has to differentiate between that which is of little value and that which is highly sensitive and confidential. For many organizations, simple five injury grade walls suffice as follows.

- a. Top Secret
- b. Highly confidential
- c. Proprietary
- d. Internal use only
- e. Public documents

Security Concepts and Techniques

1. **Cryptosystems:** refers to a suite of algorithms needed to implement a particular form of encryption and decryption. Typically, a cryptosystem consists of three algorithms: one for key generation, one for encryption and one for decryption. The term 'cipher' is often used to refer to a pair of algorithms, one for encryption and one for decryption.
2. **Data Encryption Standard (DES):** the DES is a cipher selected as an official federation information processing standard for the United States in 1976, and which was now used by internationally.
3. **Public Key Infrastructure (PKI):** Public key infrastructure, if properly implemented and maintained, can provide a strong means of authentication. The system is based on public key cryptography in which user has a key pair - a unique electronic value added as a public key and mathematically related private key. The public key is made available to those who need to verify user identity.

Data Security and Public Networks

Historically one large company could afford secure networks, which they created from expensive leased lines. Everyone else had to make do with the relatively unsecure internet. So for this many security feature are available and from that one common and very useful concept is firewall.

Firewalls

A firewall is a collection of components that mediate access between different security domains. All traffic between the security domains must pass through the firewall, regardless of the direction of the flow. Since the firewall serves as an access control point for traffic between security domains, they are ideally situated to inspect and block traffic and coordinate activities with network intrusion detection systems.

They are four primary firewall types from which to choose

1. **Packet filter firewall:** Packet filter firewall evaluate the headers of each incoming and outgoing packet to ensure it has a valid internal address, originates from a permitted external address, connects to an authorized protocol or service, and contains valid basic header instructions.
2. **Stateful Inspection Firewall:** Stateful inspection firewalls are packet filters that monitor the state of TCP connection.
3. **Proxy Server Firewall:** Proxy servers acts as an intermediary between internal and external IP address and block direct access to the internal network.
4. **Application Level Firewall:** Application level firewall perform application-level screening, typically including the filtering capabilities of packet filter firewalls with additional validation of the packet content based on the application.

The selection of the firewall type is dependent on many characteristics of the security zone, such as the amount of traffic, the sensitivity of the system and data, and applications. Additionally, consideration should be given to the ease of firewall administration, degree of firewall monitoring support through automated logging and log analysis, and the capability to provide alerts for abnormal activity.

Firewalls are subject to failure. When firewalls fail, they typically should fail closed, blocking all traffic, rather than failing open and allowing all traffic to pass.

Hacking

Hacking is an act of penetrating computer system to gain knowledge about the system and how it works.

Unauthorized Intrusion

Intrusion detection is the attempt to monitor and possibly prevent attempts to intrude into or otherwise compromise the system and network resources of an organization. Simply put it works like this: the computer system on an organization are attached to a network, and perhaps even to the internet. The organization would allow access to that computer system from the network, by authorized people for acceptable reasons.

Intrusion detection is the set of mechanism that should be in place to warn of attempted unauthorized access to the computer.

There are two types of intrusion detection system.

1. Network Based system
2. Host Based System

Data Privacy

Data privacy refers to the evolving relationship between technology and the legal right to, or public expectation of privacy in the collection and sharing of data. There are many data privacy policies which are as follows

1. Copyright notice
2. E-Mail Monitoring
3. Non-Business use inflammatory, unethical or illegal consent disclosure
4. Customer information sharing
5. Encryption of data backups
6. Encryption of extranet connections
7. Data Access

Controlling Against Viruses and other Destructive programs

Destructive programs such as viruses are responsible for huge amount of corporate losses annually. The losses are measured in terms of data corruption and destruction, degraded computer performance, hardware destruction, violation of privacy, and the personnel time devoted for repairing the damage.

Virus

A virus is a program that attaches itself to a legitimate program to penetrate the operating system. The virus destroys application programs, data files, and operating system in a number of ways. Virus programs usually attach themselves to the following types of files

1. An .EXE or .COM program file
2. The .OVL program file
3. The boot sector of a disk
4. A device driver program.

Anti-Virus Software

Among the counter measures against virus attacks, anti-virus software are the most widely used techniques of detect viruses, and prevent their further propagation and harm. There are three types of anti-virus software are

1. Scanner
2. Active monitor and Heuristic Scanner
3. Integrity Checkers

Logical Access Control

These controls are Software related and include procedures exercised in the IS software through access controls through system software and application software. Logical access control are implemented to ensure that access systems, data and programs restricted to authorized users so as to damage or loss.

➤ Role of an IS auditor in evaluating logical access Controls

1. Reviewing the relevant documents pertaining to logical facilities and risk assessment and evaluation techniques and understanding the security risks facing the information processing system.
2. The potential access paths into the system must be evaluated by the auditor and documented to assess their sufficiency
3. Deficiencies or redundancies must be identified and evaluated
4. By supplying appropriate audit techniques, he must be in a position to verify test controls over access paths to determine its effective functioning.
5. He has to evaluate the access control mechanism, analyze the test results and other auditing evidences and verify whether the control objectives have been achieved.
6. The auditor should compare security policies and practices of other organization with the policies of their organization and assess its adequacy.

Physical Access Control

These controls are personnel; hardware and software related and include procedures exercised on access by employees/outside to IT resources. These physical security and access controls should address not only the area containing system hardware, but also locations of wiring used to connect elements of the system, supporting services, backup media and any other elements required for the system operation.

Some of the most common access control techniques are discussed categorically as follows.

1. Lock on doors
 - a. Cipher lock: The cipher locks consist of a pushbutton panel that is mounted near the door outside of a secured area. Cipher locks are used in low security situation or when a large number of entrances and exits must be usable all the time
 - b. Bolting Door Lock
 - c. Electronic Door Locks
 - d. Biometric door Locks
2. Physical Identification Medium
3. Logging in utilities
 - a. Manual logging
 - b. Electronic Logging
4. Other measures
 - a. Video Cameras
 - b. Security Guards
 - c. Controlled visitor access
 - d. Bonded personnel
 - e. Dead man doors

- f. Non-exposure of sensitive facilities
- g. Computer terminal locks
- h. Controlled single entry point
- i. Alarm system
- j. Control of out of hours of employee-employees
- k. Secured report/Document distribution cart
- 5. Accounting Audit trail
- **Role of IS auditor in Physical access control**
 - 1. Risk assessment
 - 2. Controls assessment
 - 3. Planning for review of physical access controls
 - 4. Testing of controls

Environmental Controls

This section deals with the external factors in the information system and preventive measures to overcome these conflicts. Issues covered are

- 1. Environmental issues and exposures
- 2. Audit and evaluation techniques for environmental controls.
- **Audit and evaluation techniques for environmental control**
 - a. Water and Smoke detectors
 - b. Hand-Held fire extinguisher
 - c. Fire suppression systems
 - d. Regular inspection by fire department
 - e. Fireproof walls, Floors and Ceiling Surrounding the Computer room
 - f. Electrical surge protectors
 - g. Power leads from two substations
 - h. Fully documented and tested business continuity plan
 - i. Wiring placed in electrical panels and conduit
 - j. Documented and tested emergency evacuation plans
 - k. Humidity/temperature controls
- **Role of Auditor in Environmental Controls**
 - 1. Audit planning and assessment
 - a. The risk profile should include the different kinds of environmental risks that the organization is exposed to
 - b. The controls assessment must ascertain that controls safeguard the organization against all acceptable risks including probable once are in place
 - c. The security policy of the organization should be reviewed to determine the appropriateness of location of IPF, review of surroundings, power and cable wiring etc.
 - d. The IS auditor should interview relevant personnel to satisfy himself about employees' awareness of environmental threats and controls.
 - e. Administrative procedures such as preventive maintenance plans and their implementation, incident reporting and handling procedures, inspection and testing plan and procedures need to be reviewed.
 - 2. Audit of Technical Controls
 - a. The IPF and the construction with regard to the type of materials used for construction
 - b. The presence of water and smoke detectors
 - c. The location of fire extinguisher
 - d. Emergency procedures
 - e. Legal compliance with fire safety protection
 - f. Power sources and conduct tests to assure the quality of power
 - g. Environmental control equipment like AC, heaters, dehumidifiers etc.

- h. Complaint logs and maintenance logs to assess if MTBF and MTTR are within acceptable levels.
- i. Activities in the IPF.