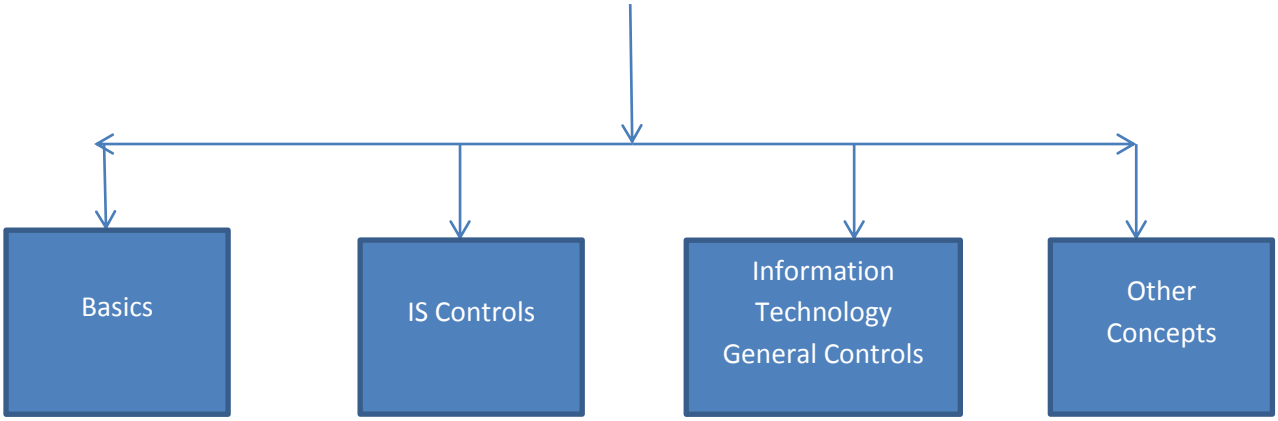
Protection of Information System



Basics

- Need for Protection of Information System
- What information is sensitive
- Information System Security and its Objectives
- Information Security Policy and related issues

Need for Protection of Information System

Information Security failure may result in both

- Financial and/or
- Intangible losses

Such as unauthorised disclosure of competitive or sensitive information

A reason why the protection of information system has become a need for the organisation

Information Security refers to the protection of the valuable assets against loss, disclosure or damage

Security includes not only the physical safeguard but also the logical safeguards

What information is sensitive?

This is the critical information that each organisation generates

- **Business Operations:-**Organisations Processes and Procedures
- **Strategic Plans**:- If Competitor learns about this, the company could end up losing money
- **Finances:-** Salaries and Wages-precise information can provide a competitive edge

Information System Security and its objectives

Information Security refers to the protection of valuable assets against loss, disclosure or damage

Objectives of Information System Security are

- Confidentiality
- Availability
- Integrity

Information Security Policy and its objectives

Information Security refers to the protection of the valuable asset against loss, disclosure or damage

Objectives of Information Security are

- Confidentiality
- Integrity
- Availability

Information Security Policy and Related issues

Information Security is the statement of intent by the management about how to protect a company's information assets.

It is a formal statement of the rules which give access to people to an organisation's technology and information assets and which they must abide by

Information Security Policy and their hierarchy

Various types of Information Security Policies are:-

- User Security Policies
    - User Security Policy:- It sets out the responsibilities and requirements of all IT System users
    - Acceptable Usage Policy:- This sets out the policy for acceptable use of e-mail, Internet Services and other IT resources
- Organisation Security Policies
    - Organisational Information Security Policy:- This sets out the Group Policy for the Security of the information assets and information technology
    - Network and System Security Policy:- This Policy sets out the detailed policy for the system and network security and applies to IT department users
    - Information Classification Policy :- This sets out the policy for the classification of information
- Conditions of Connection:- This policy sets out the Group Policy for connecting to the network

Components of the Security Policy

- Purpose and Scope of the document and the intended audience
- The Security Infrastructure
- Security Organisation Structure
- Incident response mechanism and incident reporting
- Physical and Environmental Security
- IT operations management
- IT communications

Issues to address in Information Security

- Definition of Information Security
- Reasons why information security is important to the organisation
- Brief explanation of Security Policies and Principles and compliance requirements
- Definition of all relevant information security responsibilities
- Reference to supporting documentation

IS Controls

Control is defined as policies, procedures, practices and enterprise structure that are designed to provide reasonable assurance that business objectives will be achieved and undesirable events are prevented, detected and controlled

Impact of Technology on Internal Controls

- *Competent and Trustworthy Personnel*
- *Authorisation Procedures*
- *Comparing Recorded Accountability with Assets*
- *Segregation of Duties*
- *Physical Control Over assets and records*
- *Adequate Management Supervision*
- *Independent Checks on Performance*
- *Delegation of Authority and Responsibility*

Competent and Trustworthy Personnel:- Personnel have proper and competent skills

Authorisation Procedures:- Manual Systems, auditors evaluate the adequacy of procedures and in automated systems, these are embedded within a computer program

Comparing Recorded Accountability with Assets:- Data and the assets to be compared to ensure that incompleteness or inaccuracies exist in the system. Manual System-this was work of the independent staff and in automated one, this is work of software

Segregation of Duties:-Distribution of work among employees so that they are doing only their specific work. Main purpose is to prevent errors

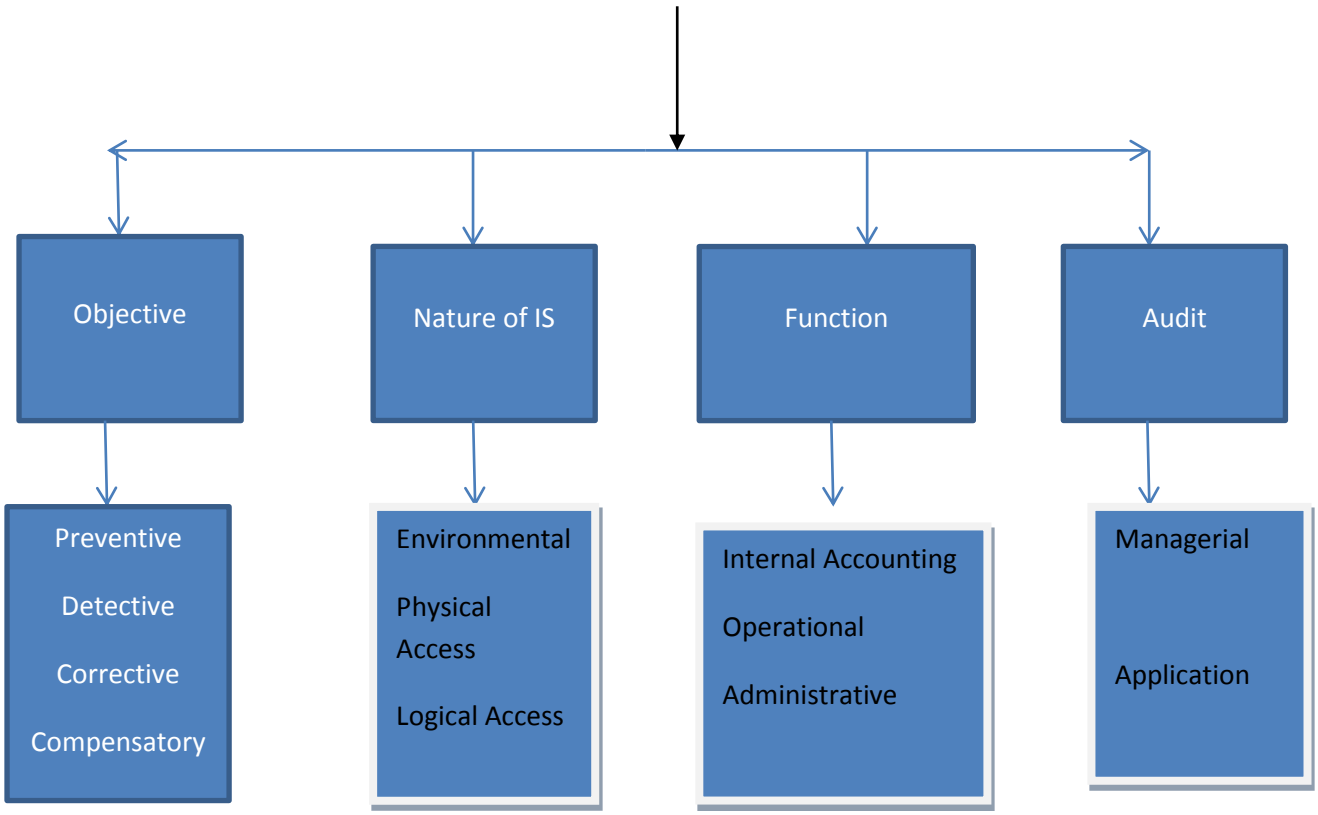
Physical Control over assets and records:-Manual systems used the locked doors and cabinets whereas automated systems use logins and passwords

Adequate Management Supervision:- Refers to review of work by a supervisor

Independent checks on performance:- Manual system-chances of deviation from the procedures are high whereas in the automated system- there are prescribed procedures which system will always follow

Delegation of Authority and Responsibility:- In Computer system, delegation in an unambiguous way might be too difficult because some resources may be shared among multiple users

Classification of Information System Controls



Preventive Controls

Preventive Controls are those inputs, which are designed to prevent an error, omission or malicious act from occurring. E.g. Password

Characteristics

- Clear cut understanding about the vulnerabilities of the asset
- Understanding probable threats
- Provision of necessary controls to prevent the probable threats from materialising

Examples

- Employ qualified personnel
- Segregation of Duties

- Access Control
- Authorisation of Transaction

Detective Controls

Detective Controls are controls designed to detect errors, omissions or malicious acts that occur and report their occurrence

Characteristics

- Clear understanding of lawful activities
- Established mechanism to report the unlawful activities
- Interaction with the preventive control
- Surprise checks by the supervisor

Examples

- Duplicate checks
- Security Camera
- Intrusion Detection Systems
- Due Accounts report

Corrective Controls

Controls designed to reduce the impact or correct an error once it has been detected

Characteristics

- Minimising the impact of the threat
- Identifying the cause of the problem
- Providing remedy to the problems discovered by detective controls
- Getting Feedback from preventive and corrective controls
- Correcting error arising from a problem

Examples

- Contingency Planning
- Investigate Budget Variations and Report Variations

Compensatory Controls

Controls designed to reduce the probability of threats, which can exploit the vulnerabilities of an asset and cause loss to that asset.

While designing the appropriate control-Keep in mind the fact that the Cost of the Lock should not be more than the cost of the asset it protects