Protection of Information Systems

[Exam importance- 16 marks; Most practical and Easy to remember topic of ISCA; LBH]

- Need for Protection of Information Systems:
  - Risks have led to a gap b/w the need to protect systems and the degree of protection applied. This gap is caused by:
    1. Widespread use of Technology
    2. Interconnectivity of systems
    3. Elimination of distance, time and space as constraints
    4. Unevenness of technological changes
    5. Devolution of management & controls
    6. External factors such as legal & regulatory requirements

- Information System Security:
  - Information Security Objectives:
    1. Confidentiality (C): prevention of unauthorized disclosure of information.
    2. Integrity (I): prevention of unauthorized modification of information.
    3. Availability (A): prevention of unauthorized withholding of information.

  - What information is sensitive? :
    1. Strategic Plans
    2. Business Operations
    3. Finances

- Information Security Policy: is a statement of intent by the mgt. about how to protect the company's information assets. Includes rules intended to:
  - Preserve and protect information's CIA.
  - Limit/ eliminate potential legal liability from employees or 3rd parties.
  - Prevent waste or inappropriate use of the resources of an org.

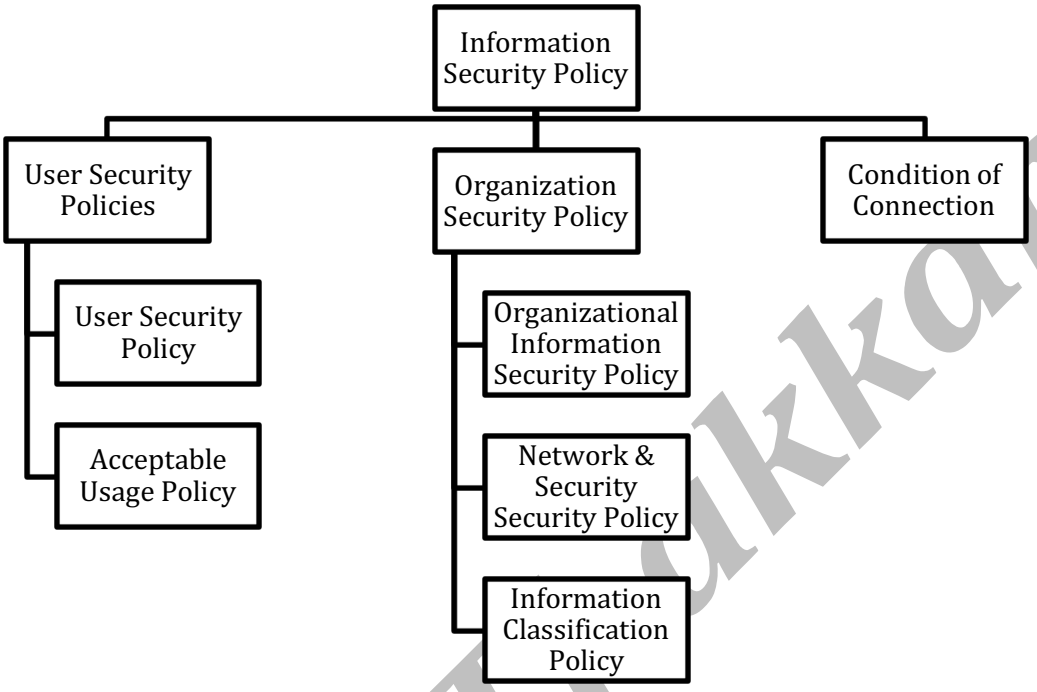
  - Tools to implement policy:
    - Standards
    - Guidelines
    - Procedures

  - Issues to addressed by Information Security Policy:
    1. Definition of information security
    2. Reasons why info. Security is important to the org., and its goals & requirements
    3. Brief explanation of the security policies, principles, standards and compliance requirements
    4. Definition of all relevant information security Responsibilities
    5. A reference to the supporting documentations

  - Members of Security Policy:

1. Management members
2. Technical group
3. Legal experts

- Information Security Policies and their hierarchy:



- Components of the Security Policy:
  1. Purpose & Scope of Document
  2. The Security Infrastructure
  3. Security Policy document maintenance and compliance requirements
  4. Physical and Environmental Security
  5. Identity management and Access Control
  6. System Development and Maintenance controls
  7. Business Continuity Planning
  8. Legal Compliances
  9. Monitoring and Auditing Requirements

➢ Information System Controls:
- Need for Controls in Information Systems:
  - A well designed IS should have controls built in for all its critical sections. IS control procedure may include:
    1. Strategy and direction
    2. Access to IT Resources
    3. System development methodologies and change control
    4. Operation procedures
    5. Quality assurance procedures
    6. Physical access controls
    7. BCP and DRP

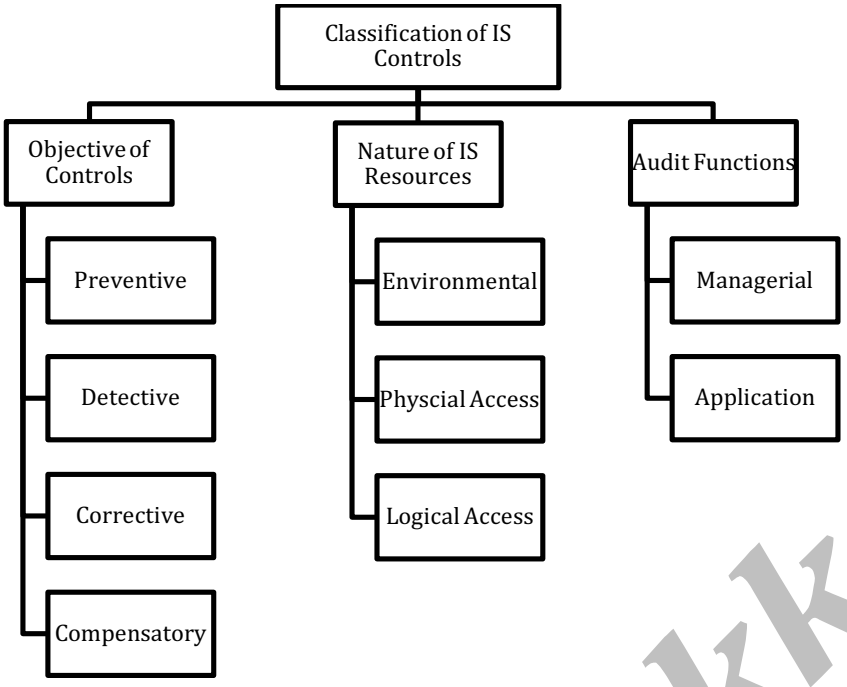
8. Protective and detective mechanisms against internal & external attacks

- Objectives of Controls: is to reduce or if possible eliminate the causes of the exposure to potential loss.
  - Some of the critical <u>control LACKING in the Computerized environment</u> are as follows:
    1. Lack of management understanding of IS risks and related controls
    2. Absence or inadequate IS Control framework
    3. Absence or weak General controls and IS controls
    4. Lack of awareness and knowledge of IS risks and controls amongst the business users and even IT staff
    5. Complexity of implementation of controls in distributed computing environments
    6. Lack of control features or their implementation in highly technological driven environments
    7. Inadequate security functionality in technologies implemented

  - Control objectives serve 2 main purposes:
    - Outline the policies of the org. as laid down by the mgt.
    - Set a benchmark for evaluating whether control objectives are met.

- Impact of Technology on Internal Controls:
  1. Competent and Trustworthy Personnel
  2. Segregation of Duties
  3. Authorization Procedures
  4. Adequate Documents and Records
  5. Physical Control over Assets and Records
  6. Adequate Management Supervision
  7. Independent Checks on Performance
  8. Comparing Recorded Accountability with Assets
  9. Delegation of Authority & Responsibility

- Classification of Information System Controls:



- Classification on the basis of "Nature of IS Resources":
  - Environmental Controls:
    - Environmental Issues and Exposures:
      - These exposures are primarily due to elements of nature.
      - Issues:
        1. Fire
        2. Power Spikes: Is Power supply properly controlled so to avoid power spike?
        3. Water damage
        4. Pollution damage: Is computer equipment kept free from dust, smoke?
        5. Natural disasters
        6. Are A/c and ventilation systems protected against the effects of electricity failure?
        7. Is consumption of food around equipment room prohibited by a policy?
        8. Are backup media protected from damage due to magnetic fields and water damage?
      - IS Resources Based On Env. Exposures & controls:
        1. Hardware & Media
        2. IS Supporting Infrastructure/Facilities
        3. Documentation
        4. Supplies
        5. People
    - CONTROLS for Environmental Exposures:
      - Fire Damage
        1. Fire Alarms
        2. Fire Extinguishers

3. Control panel which shows location of alarm triggered
4. Fire Exists
5. Staff knows the Emergency procedures
6. Regular inspection by Fire Department
7. Smoke Detectors
8. Wiring placed in Electrical Panel and Conduit

- Power Spikes (Fluctuation)
  1. Using Electrical Surge Protectors
  2. Uninterruptible Power Supply (UPS)/ Generator
  3. Emergency Power-Off switch

- Water Damage
  1. Water Detectors
  2. Strategically Locating the Computer Room
  3. Proper Drainage Exists
  4. Water Alarms
  5. Water Leakage Alarms
  6. Water proofing

- Pollution Damage and Others: (major pollutant- dust)
  1. Documented and Tested Emergency Evacuation Plans
  2. Power Leads from Two Substations
  3. Prohibition against Eating, Drinking and Smoking within Information Processing Facilities

- Physical Access Controls:
  - Are the controls relating to physical security of the tangible IS resources and intangible resources stored on tangible media, etc.
  - Physical Access Issues & Exposures: results due to accidental or intentional violation of the access paths:
    1. Abuse of data processing resources
    2. Blackmail
    3. Embezzlement
    4. Damage or theft to equipments or docs.
    5. Public disclosure of sensitive information
    6. Unauthorized entry

  - Reasons for above possible offences (Possible Perpetrators- mostly because of employees):
    1. Accidental ignorant
    2. Discontented
    3. Addicted to gambling
    4. Experiencing financial/emotional problems
    5. Notified for their termination
    6. Former Employee
    7. Threatened by disciplinary action or dismissal

- Facilities that need to be protected from auditor's perspective:
    1. Communications channels
    2. Computer Room
    3. Control units and processors
    4. Telecommunication lines
    5. Input/ Output devices
    6. Power sources
    7. Operator consoles
    8. Storage rooms and supplies

- CONTROLS for Physical Access Exposures:
    1. Locks on Doors:
        a. Cipher locks (enter codes)
        b. Bolting door locks (metal key)
        c. Biometric door locks (unique body features)
        d. Electronic door locks (advantages)
            i. Degree of duplication is reduced.
            ii. Individual access needs can be restricted through the special internal code and sensor devices.
            iii. Through the special internal code, cards can be made to identify the correct individual
            iv. Card entry can be easily deactivated in the event an employee is terminated or card is lost.
            v. The card key becomes an important item to retrieve when an employee leaves the firm.

    2. Physical Identification Medium:
        a. Personal Identification Number (PIN)
        b. Plastic Cards
        c. Identification Badges
    3. Logging Utilities:
        a. Manual logging
        b. Electronic logging
    4. Other means of controlling Physical Access:
        a. Video cameras
        b. Security guards
        c. Controlled visitor access
        d. Bond-ed personnel
        e. Dead man doors
        f. Non-exposure of sensitive facilities
        g. Computer terminal locks
        h. Alarm systems
        i. Perimeter fencing

- Logical Access Controls:
    - Are the controls relating to logical access to information resources. Are implemented to ensure that access to systems,

data and programs is restricted to authorized users so as to safeguard CIA of the information.

- Logical Access Paths (How logical access is obtained):
    1. Online Terminals; 1.1 Operator Console
    2. Dial-up ports
    3. Telecommunication Network

- Logical Access Issues & Exposures & Revelations:
    - Technical Exposures:
        1. Bombs (Time & Logic Bomb)
        2. Data diddling (changes the data before or as it is being entered into the system)
        3. Trojan Horse
        4. Worms
        5. Salami Techniques
        6. Rounding Down
        7. Trap Doors

    - Computer Crime Exposures:
        1. Financial Loss
        2. Legal Repercussions
        3. Disclosure of Confidential/Sensitive information
        4. Blackmail/Industrial Espionage
        5. Loss of Credibility/Competitive Edge
        6. Sabotage
        7. Spoofing

    - Asynchronous Attacks: (data that are waiting to be transmitted are liable to unauthorized access; hard to detect)
        1. Subversive Threats (Invasive tap & Inductive tap)
        2. Data Leakage
        3. Wire Tapping (draw diagram)
        4. Piggybacking (draw diagram)
        5. Shut down/ Denial of Service

    - Remote and Distributed Data Processing applications can be controlled in many ways:
        1. Having Terminal Locks
        2. Proper control over remotely accessible applications
        3. Proper control mechanism over system documentation and manuals
        4. Data transmissions should be well controlled
        5. Ensure that duplicated data does not exist
        6. Proper monitoring for violations

- Logical Access Violators: (require more technical & complex skills as compared to physical access violators)
    1. Hackers
    2. Employees

3. IS Personnel
4. End Users
5. Former Employees
6. Competitors, Foreigners, Criminals, Accidental Ignorant

- CONTROLS for Logical Access Exposures:
    1. User Management Control:
        i. User Registration
        ii. Privilege/Access management
        iii. User password management
        iv. Review of User Access Rights
    2. User Responsibilities Control:
        i. Password use
        ii. Unattended user equipment
    3. Network Access Control:
        i. Policy on use of network services
        ii. Enforced path (path to be used)
        iii. Segregation of Networks (public from pvt.)
        iv. Security of Network Services
        v. Firewall
        vi. Encryption
        vii. Call back devices
        viii. Recording of Access Logs
    4. Operating System Access Control:
        i. Automated Terminal identification
        ii. Terminal log-in procedures
        iii. Access Token
        iv. Access Control List
        v. Discretionary Access Control
        vi. User Identification and Authentication
        vii. Password Management System
        viii. Restricted Access to general user
        ix. Duress Alarm to safeguard users
        x. Terminal timeout
        xi. Limitation of connection time
    5. Application and Monitoring System Access Control:
        i. Information access restriction
        ii. Sensitive system isolation
        iii. Event logging
        iv. Monitoring system use
        v. Clock Synchronization
    6. Mobile Computing

- Controls over Data Integrity and Security:
  - Information Classification:
    1. Public Documents
    2. Top Secret
    3. Highly Confidential
    4. Proprietary
    5. Internal Use Info.

  - Categories of Integrity Controls:
    1. Source Data Controls
    2. Input Validation routines
    3. Online data entry Controls
    4. Data processing & storage Controls
    5. Output Controls
    6. Data Transmission Controls

  - Data Integrity POLICIES:
    1. Virus-signature updating
    2. Software testing
    3. Division of environments (into Dev./Test/Prod. Systems)
    4. Offsite Backup storage
    5. Quarter and Year end Backups
    6. Disaster recovery

- Financial CONTROLS:
    1. Authorization
    2. Budgets
    3. Cancellation of Documents
    4. Documentation
    5. Dual Control
    6. Safekeeping
    7. Sequentially numbered documents
    8. Input/ Output verification
    9. Supervisory review

- Personal Computer Risks and related CONTROLS:
    - Risks:
        1. Easy to move them for theft of information
        2. Pen drives & HDD used to steal info.
        3. Data corruption due to lack of safeguards
        4. Leakage of info. due to vast number of installations
        5. Operating staff may not be adequately trained

    - Controls:
        1. Physically locking the system
        2. Proper logging into system
        3. Centralized purchase of H/w & S/w
        4. Set Standards for developing, testing and documenting
        5. Use anti-malware S/w

- Cyber Frauds:
    - Types:
        - Pure Cyber Frauds- exist only in cyber world. E.g. Website hacking.
        - Cyber-Enabled Frauds- committed in physical world with use of technology. Egg. Stealing credit card info and transferring money.

    - Cyber Attacks:
        1. Phishing
        2. Network Scanning
        3. Virus/ Malicious Code
        4. Spam
        5. Website Compromise
        6. Others:
            i. Cracking
            ii. Eavesdropping
            iii. Email forgery
            iv. Email threats
            v. Scavenging

    - Impact of Cyber Frauds on Enterprise:
        1. Financial Loss
        2. Legal Repercussions
        3. Loss of Credibility/ Competitive Edge

4. Disclosure of Confidential/ Sensitive Info.
5. Sabotage

- Techniques to Commit Cyber Frauds:
    1. Hacking
    2. Cracking
    3. Data Diddling
    4. Data Leakage
    5. DoS Attack
    6. Internet Terrorism
    7. Logic Time Bombs
    8. Masquerading/ Impersonation
    9. Password Cracking
    10. Piggybacking
    11. Trapdoor