Chapter – 3
Protection of Information Systems

Need for Protection of Information Systems: Information security failures may result in both financial losses and/or intangible losses such as unauthorized disclosure of competitive or sensitive information. That is why protection of information systems has become a need for organizations.

Information System Security: Information security refers to the protection of valuable assets against loss, disclosure, or damage. For any organization, the security **objective comprises three universally accepted attributes:**

1. **Confidentiality:** Prevention of the unauthorized disclosure of information
2. **Integrity:** Prevention of the unauthorized modification of information; and
3. **Availability:** Prevention of the unauthorized withholding of information.

The relative priority and significance of Confidentiality, Integrity and Availability (CIA) vary according to the data within the information system and the business context in which it is used.

What Information is Sensitive?

The common aspect in each organization is the critical information that each organization generates. These are:

1. Strategic Plans,
2. Business Operational data and
3. Financial records etc.

Information Security Policy: An Information Security policy 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 govern access to people to an organization's technology and information assets, and which they must abide by.

Members of Security Policy: Security has to encompass managerial, technological aspects. Security policy broadly compromises the following three groups of management:

1. Management member who have budget and policy authority.
2. Technical group who know what can cannot be supported and
3. Legal experts who know the legal ramification of various policy charges.

Major Information Security Policies are:

1. Information Security Policy
   - A. Users security policy
   - B. Acceptable usage policy
2. Organizational Information Security Policy,
   - **a.** Network & System Security Policy and
   - **b.** Information Classification policy
3. Conditions of Connection – this policy sets out the group policy for connecting to the network.

Components of the Security Policy: - A good security Policy should clearly state the following:

I. Purpose and scope of the document and the intended audience
II. The security infrastructure
III. Security policy document maintenance and compliance requirement
IV. Incident purpose mechanism and incident reporting
V. Security organization structure

VI. Inventory and classification of Assets
VII. Physical and environmental security
VIII. IT Operation management
IX. IT Communication
X. Business continuity planning
XI. Legal compliance
XII. Monitoring and Auditing requirements

Information Systems 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 undesired events are prevented, detected and corrected. Thus, information systems auditing includes reviewing the implemented system or providing consultation and evaluating the reliability of operational effectiveness of controls.

A well designed information system should have controls built in for all its sensitive or critical sections. An information system should be properly controlled. Procedure of information system control may includes the following:

1. Strategy and direction
2. General organization and management
3. Access to IT resources
4. System development methodology and change control
5. Operation procedures
6. Physical access control
7. BCP & DRP
8. Network and Communication
9. Data base management and
10. Protective and Detective mechanism

Objectives of Controls: The objectives of control are to reduce or if possible eliminate the causes of exposure to potential loss. Exposures are potential losses due to threats materializing. All exposures have been causes. Some categories of exposures are:

1. Errors or omission in data, procedure, processing & comparison
2. Improper authorization and improper accountability with regards to procedure
3. Inefficient activity in procedure, processing and comparison

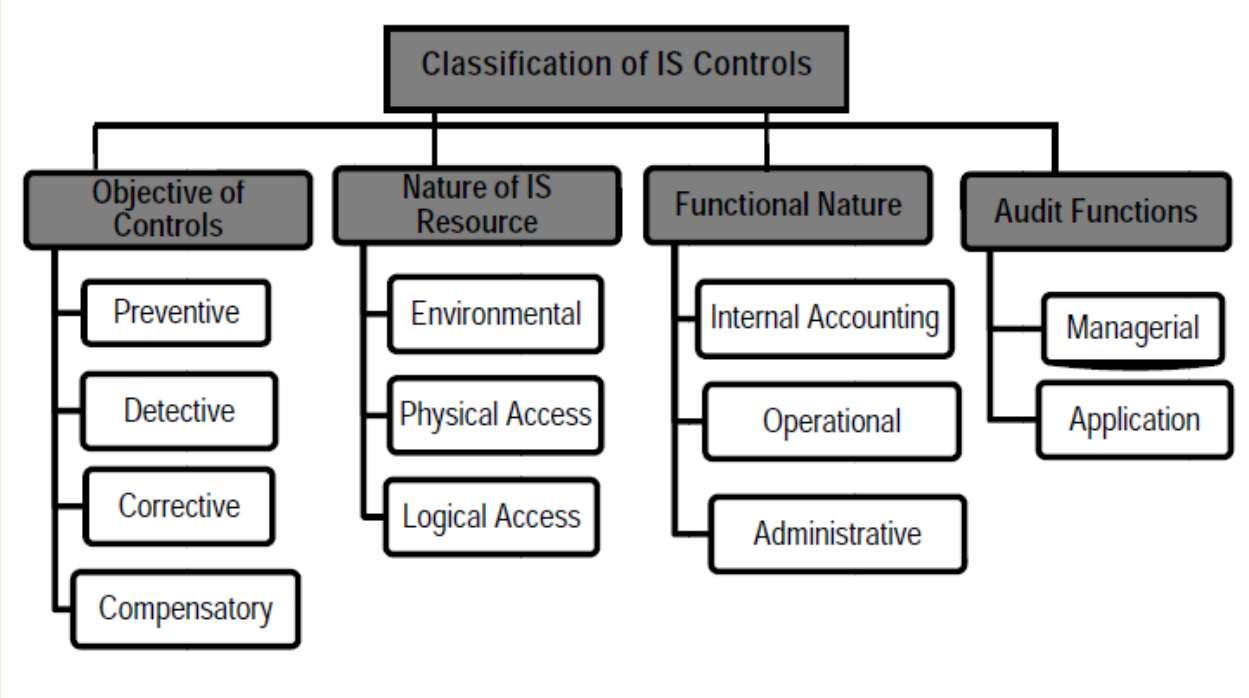
Internal controls comprise of the following five interrelated components:

1 . Control Environment,
2 . Risk Assessment,
3 . Control Activities,
4. Information and Communication,
5. Monitoring.

Impact of Technology on Internal Controls: The internal controls within an enterprise in a computerized environment encompass the goal of asset safeguarding, data integrity, system efficiency and effectiveness. These are:

1 . Personnel,
2. Segregation of duties,
3. Authorization procedures,
4. Record keeping,
5. Management supervision and review,
6. Risks due to concentration of programs and
7. Data.

Categories of Controls: The controls can be classified as under



Based on the objective of **controls**, these can be classified as under:

1. **Preventive Controls:** Preventive controls are those, 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 a financial system.
2. **Detective Controls:** These controls are designed to detect errors, omissions or malicious acts that occur and report the occurrence. An 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. Corrective controls may include the use of default dates on invoices where an operator has tried to enter the incorrect date. A Business Continuity Plan (BCP) is considered to be a corrective control.
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. While designing the appropriate control one thing should be kept in mind— "*the cost of the lock should not be more than the cost of the assets it protects.*"

Another classification of controls is based on the **nature of IS resource**. These are given as follows:

1. **Environmental Controls:** These are the controls relating to IT environment such as power, air-conditioning, UPS, smoke detection, fire-extinguishers, dehumidifiers etc. These are related to the external factors in the Information Systems and preventive measures to overcome the conflicts.

   A. **The controls over environment exposures are:** Water Detectors, Hand-Held Fire Extinguishers, Manual Fire Alarms, Smoke Detectors, Fire Suppression Systems,

Strategically Locating the Computer Room, Regular Inspection by Fire Department, Fireproof Walls, Floors and Ceilings surrounding the Computer Room, from the perspective of environmental exposure and controls and information systems resources may be categories as follows

1. Hardware and media
2. Information system supporting infrastructure
3. Documentation
4. Supplies
5. Peoples

B. Controls for environmental exposure : These are given as follows

1. Water detector
2. Hand held water extinguisher
3. Manual fire alarms
4. Fire suppressing system
5. Regular inspection by fire department
   Electrical Surge Protectors,
6. Uninterruptible Power System (UPS)/Generator,
7. Power Leads from Two Substations,
8. Emergency Power-Off Switch,
9. Wiring Placed in Electrical Panels and Conduit,
   Prohibitions against Eating,
10. Drinking and Smoking within the Information Processing Facility and
11. Fire Resistant Office

2. **Physical Access Controls:** These are the controls relating to physical security of tangible IS resources and intangible resources stored on tangible media etc. Such controls include Access control doors, Security guards, door alarms, restricted entry to secure areas, visitor logged access, CCTV monitoring etc. These controls are personnel; hardware and include procedures exercised on access to IT resources by employees/outsiders. The controls relate to establishing appropriate physical security and access control measures for IT facilities, including off-site use of information devices in conformance with the general security policy. These controls are designed to protect the organization from unauthorized access or in other words, to prevent illegal entry.

i. Physical access issues & exposure : the following points elaborate the results due to accidental or intentional violation of the access path :

Abuse of data processing resource
Blackmail
Damage or theft to equipments or documents
Unauthorized entry

ii. Controls for physical access exposure: These controls should be designed in such a way that it allows access only to authorized persons. These are as follows:

A. Locks on Doors - Cipher locks (Combination Door Locks), Bolting Door and Electronic Door Locks.

B. Physical Identification Medium - Personal Identification numbers (PIN), Plastic Cards Identification Badges.

C. Logging on Facilities - Manual Logging and Electronic Logging.

D. Other means of Controlling Physical Access - Video Cameras, Security Guards, Controlled Visitor Access, Bonded Personnel, Dead Man Doors, Non– exposure of Sensitive

Facilities, Computer Terminal Locks, Controlled Single Entry Point, Alarm System, Perimeter Fencing, Control of out of hours of employee-employees and Secured Report.

3. **Logical Access Controls:** These are the controls relating to logical access to information resources such as operating systems controls, application software boundary controls, networking controls, access to database objects, encryption controls etc. are the system-based mechanisms used to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted. Logical access controls are implemented to ensure that access to systems, data and programs is restricted to authorized users so as to safeguard information against unauthorized use, disclosure or modification, damage or loss.

   (I) **Logical Access Paths:** These are Online Terminals, Dial-up Ports and Telecommunication Network etc.

   (II) **Issues and Revelations related to Logical Access:** Compromise or absence of logical access controls in the organizations may result in potential losses due to exposures that may lead to the total shutdown of the computer functions. Intentional or accidental exposures of logical access control encourage technical exposures and computer crimes. These are as follows:

   a. **Technical Exposures:** Technical exposures include unauthorized implementation or modification of data and software. Technical exposures include:

   1. **Data Diddling** – it involves the changes of data before or after they are enter into the system.
   2. **Bombs-** it is a piece of bad code deliberately planted by an insider or suppliers of the program. It has two type – Time Bomb & Logic Bomb
   3. **Time Bomb** – a physical time bomb explodes at the time it is set for. The computer clock initiates it.
   4. **Logic Bomb** – logic Bomb are activated by combination of events. These bombs can be set to go off at a future time or event.
   5. **Trojan Horse** – xmas card is well example of Trojan.

Trojan Horse: These are malicious programs that are hidden under any authorized program. Typically, a Trojan horse is an illicit coding contained in a legitimate program, and causes an illegitimate action. The concept of Trojan is similar to bombs but a computer clock or particular circumstances do not necessarily activate it. A Trojan may:

- Change or steal the password or
- May modify records in protected files or
- May allow illicit users to use the systems.

Trojan Horses hide in a host and generally do not damage the host program. Trojans cannot copy themselves to other software in the same or other systems. The trojans may get activated only if the illicit program is called explicitly. It can be transferred to other system only if an unsuspecting user copies the Trojan program.

   6. Worms

Worm: A worm does not require a host program like a Trojan to relocate itself. Thus, a Worm program copies itself to another machine on the network. Since, worms are stand-alone programs, and they can be detected easily in comparison to Trojans and computer viruses. Examples of worms are Existential Worm, Alarm clock Worm etc. The Alarm Clock

   7. Rounding

Rounding Down: This refers to rounding of small fractions of a denomination and transferring these small fractions into an authorized account. As the amount is small, it gets rarely noticed.

8. Salami

Salami Techniques: This involves slicing of small amounts of money from a computerized transaction or account. A Salami technique is slightly different from a rounding technique in the sense a fix amount is deducted. For example, in the rounding off technique, ₹ 21,23,456.39 becomes ₹ 21,23,456.40, while in the Salami technique the transaction amount ₹ 21,23,456.39 is truncated to either ₹ 21,23,456.30 or ₹ 21,23,456.00, depending on the logic.

9. Trap Doors.

Trap Doors: Trap doors allow insertion of specific logic, such as program interrupts that permit a review of data. They also permit insertion of unauthorized logic.

b. Computer Crime Exposures: Crimes are committed by using computers and can damage the reputation, morale and even the existence of an organization. Computer crimes generally result in Loss of customers, embarrassment to management and legal actions against the organizations. These are:

i. Legal Repercussions,
ii. Loss of Credibility or Competitive Edge,
iii. Blackmail/Industrial Espionage,
iv. Disclosure of Confidential,
v. Sensitive or Embarrassing Information,
vi. Sabotage
vii. Spoofing and
viii. Financial losses

Asynchronous Attacks: They occur in many environments where data can be moved asynchronously across telecommunication lines. Numerous transmissions must wait for the clearance of the line before data can be transmitted. Data that is waiting to be transmitted are liable to unauthorized access called asynchronous attack. There are many forms of asynchronous attacks, some of them are:

(i) Data Leakage

Data Leakage: Data is a critical resource for an organization to function effectively. Data leakage involves leaking information out of the computer by means of dumping files to paper or stealing computer reports and tape.

(ii) **Wire-tapping:** this involves spying on information being transmitted over telecommunication network. We can better understand with the help of following diagram.

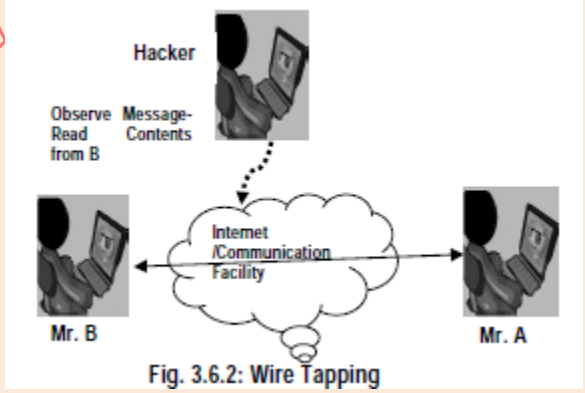


Fig. 3.6.2: Wire Tapping

(iii) Piggybacking

Piggybacking: This is the act of following an authorized person through a secured door or electronically attaching to an authorized telecommunication link that intercepts and alters transmissions. This involves intercepting communication between the operating system and the user and modifying them or substituting new messages. A special terminal is tapped into the communication for this purpose as shown in the Fig. 3.6.3.

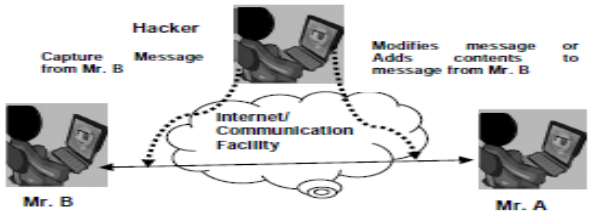


Fig. 3.6.3: Piggybacking

(iv) Shutting Down of the Computer/Denial of Service.

Logical Access Control across the System: The purpose of logical access controls is to restrict access to information assets/resources. They are expected to provide access to information resources on a need to know and need to do basis using principle of least privileges. These are:

A. User access management,
B. User responsibilities,
C. Network access control,
D. Operating system access control,
E. Application and monitoring system access control and
F. Mobile computing related controls.

Further, another **category of controls** is based on their **functional nature**. These controls are given as follows:

(i) Internal Accounting Controls: The Controls, which are intended to safeguard assets and ensure the reliability of the financial records, are called internal accounting controls.

(ii) Operational Controls: These deals with day-to-day operations, functions and activities to ensure that operational activities are contributing to business objectives.

(iii) Administrative Controls: These are concerned with ensuring efficiency and compliance with management policies.

Classification on the basis of "Audit Functions" –

1. *Managerial Controls and*
2. *Application Controls*

Managerial Controls: *These are the controls over the managerial functions that must be performed to ensure the development, implementation, operation and maintenance of information systems in a planned and controlled manner in an organization.*

Types of Management Subsystem and their description

S.No.	*Management Subsystem*	*Description of Subsystem*
1	*Top Management*	*Top management must ensure that information systems function is well managed. It is responsible primarily for long – run policy decisions on how Information Systems will be used in the organization.*
2	*Information Systems*	*IS management has overall responsibility for the planning and*

	Management	*control of all information system activities. It also provides advice to top management in relation to long-run policy decision making and translates long-run policies into short-run goals and objectives.*
3	***Systems Development Management***	*Systems Development Management is responsible for the design, implementation, and maintenance of application systems.*
4	***Programming Management***	*It is responsible for programming new system; maintain old systems and providing general systems support software.*
5	***Data Administration***	*Data administration is responsible for addressing planning and control issues in relation to use of an organization's data.*
6	***Quality Assurance Management***	*It is responsible for ensuring information systems development; implementation, operation, and maintenance conform to established quality standards.*
7	***Security Administration***	*It is responsible for access controls and physical security over the information systems function.*
8	***Operations Management***	*It is responsible for planning and control of the day-to-day operations of information systems.*

Application Controls: *Application system controls are undertaken to accomplish reliable information processing cycles that perform the processes across the enterprise. Applications represent the interface between the user and the business functions. Application Control Techniques include the programmatic routines within the application program code. The* ***objective of application controls*** *is to ensure that*

1. *Data remains complete,*
2. *Accurate and valid during its input, update and*
3. *Storage.*

Types of Application Subsystem and their description

S.No.	*Application Subsystem*	*Description of Subsystem*
1	***Boundary Controls***	*Major controls of the boundary system are the access control mechanisms. Access control mechanism links authentic users to authorized resources that they are permitted to access. Major Boundary Control techniques are Cryptography, Passwords, Personal Identification Numbers (PIN), Identification Cards and Biometric Devices.*
2	***Input Controls***	*These controls are responsible for ensuring the accuracy and completeness of data and instruction input into an application system.*

3	***Communication Controls***	*These controls discuss exposures in the communication subsystem, controls over physical components, communication line errors, flows, and links, topological controls, channel access controls, controls over subversive attacks, internetworking controls, communication architecture controls, audit trail controls, and existence controls.*
4	***Processing Controls***	*Data processing controls perform validation checks to identify errors during processing of data. They are required to ensure both the completeness and the accuracy of data being processed.*
5	***Database Controls***	*Protecting the integrity of a database when application software acts as an interface to interact between the user and the database, are called update controls and report controls. Major update controls are: Sequence Check between Transaction and Master Files, Ensure All Records on Files are processed, Process multiple transactions for a single record in the correct order and maintain a suspense account.*
6	***Output Controls***	*These controls ensure that the data delivered to users will be presented, formatted and delivered in a consistent and secure manner. Output can be in any form, it can either be a printed data report or a database file in a removable media such as a CD-ROM or it can be a Word document on the computer's hard disk.* *Major Report controls are: Standing Data, Print-Run-to Run control Totals, Print Suspense Account Entries and Existence/Recovery Controls.*

Application Controls and their Categories

Application system controls are undertaken to accomplish reliable information processing cycles that perform the processes across the enterprise. Applications represent the interface between the user and the business functions. From the point of view of users, it is the applications that drive the business logic. Different Application Controls are as follows:

1 Boundary Controls: The major controls of the boundary system are the access control mechanisms. Access controls mechanism links the authentic users to the authorized resources, they are permitted to access. The access control mechanism has **three steps:**

1 . identification,
2 . authentication and
3. authorization

Boundary Control techniques:

A. **Cryptography:** It deals with programs for transforming data into cipher text that are

meaningless to anyone, who does not possess the authentication to access the respective system resource or file.

B. **Passwords:** User identification by an authentication mechanism with personal characteristics like name, birth date, employee code,
C. **Personal Identification Numbers (PIN):** PIN is similar to a password assigned to a user by an institution a random number stored in its database independent to a user identification details, or a customer selected number.
D. **Identification Cards:** Identification cards are used to store information required in an authentication process. These cards are to be controlled through the application for a card, preparation of the card, issue, use and card return or card termination phases.
E. **Biometric Devices:** Biometric identification e.g. thumbs and/or finger impression, eye retina etc. are also used as boundary control techniques.

2 Input Controls: These controls are responsible for ensuring the accuracy and completeness of data and instruction input into an application system. Input controls are important since substantial time is spent on input of data, involve human intervention and are, therefore error and fraud prone.
Input controls are divided into the following broad classes:

1. Source Document Control,
2. Data Coding Controls
3. Batch Controls, and
4. Validation Controls.

1. **Source Document Controls:** In systems that use physical source documents to initiate transactions, careful control must be exercised over these instruments. Source document fraud can be used to remove assets from the organization.
   A. Use pre-numbered source documents
   B. Use source documents in sequence
   C. Use source documents in sequence

2. **Data Coding Controls:** Two types of errors can corrupt a data code and cause processing errors. These are transcription and transposition errors, which are :
   1. **Transcription Errors:** Addition errors occur when an extra digit or character is added to the code.
   2. **Transposition Errors:** There are two types of transposition errors.
      A. Single transposition errors occur when two adjacent digits are reversed. For instance, 12345 are recorded as 21345.
      B. Multiple transposition errors occur when nonadjacent digits are transposed. For example, 12345 are recorded as 32154.

3. **Batch Controls:** Batching is the process of grouping together transactions that bear some type of relationship to each other. Various controls can be exercises over the batch to prevent or detect errors or irregularities. Two types of batches occur:
   1. **Physical Controls:** These controls are groups of transactions that constitute a physical unit. For example – source documents might be obtained via the email.
   2. **Logical Controls:** These are group of transactions bound together on some logical basis, rather than being physically contiguous.

4. **Validation Controls:** Input validation controls are intended to detect errors in the transaction data before the data are processed. There are three levels of input validation controls:
   A. Field interrogation,
   B. Record interrogation, and

C. File interrogation

3 Communication Controls

Three major types of exposure arise in the communication subsystem:

(i) Transmission impairments can cause difference between the data sent and the data received
(ii) Data can be lost or corrupted through component failure
(iii) A hostile party could seek to subvert data that is transmitted through the subsystem

(a) **Physical Component Controls:** These controls incorporate features that mitigate the possible effects of exposures.

1. Transmission media
2. Communication line
3. Modem
4. Port protection devices

(b) **Line Error Control:** Whenever data is transmitted over a communication line, recall that it can be received in error because of attenuation distortion, or noise that occurs on the line. These errors must be detected and corrected.

(i) Error detection
(ii) Error correction

(c) **Flow Controls:** Flow controls are needed because two nodes in a network can differ in terms of the rate at which they can send, received, and process data.

(d) **Link Controls:** In WANs, line error control and flow control are important functions in the component that manages the link between two nodes in a network.

(e) **Topological Controls:** A communication network topology specifies the location of nodes within a network, the ways in which these nodes will be linked, and the data transmission capabilities of the links between the nodes.

1. Local Area Network Topologies
2. Wide Area Network Topologies

(f) **Channel Access Controls:** Two different nodes in a network can compete to use a communication channel. Whenever the possibility of contention for the channel exists. These techniques **fall into two classes:**

(i) Polling methods and
(ii) Contention methods.

(g) **Internetworking Controls:** Internetworking is the process of connecting two or more communication net-works together to allow the users of one network to communicate with the users of other networks. **Three types of devices are used to connect sub-networks**

1. Bridge
2. Gateway and
3. Router

5 Database Controls

Protecting the integrity of a database when application software acts as an interface to interact between the user and the database, are called update controls and report controls. **Major update controls are given as follows:**

1. Sequence Check between Transaction and Master Files
2. Ensure All Records on Files are processed
3. Process multiple transactions for a single record in the correct order
4. Maintain a suspense account

Major Report controls are given as follows:

1. Standing data
2. Print-Run-to Run control Totals
3. Print Suspense Account Entries
4. Existence/Recovery Controls

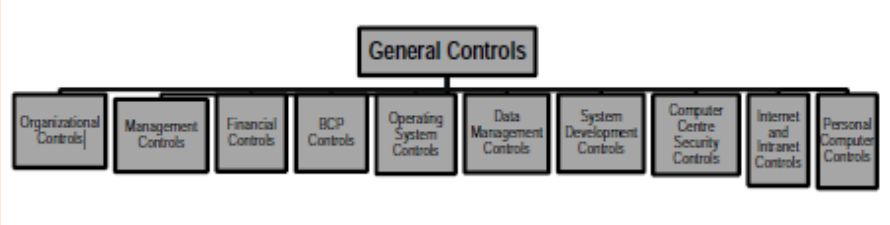
6 Output Controls

These controls ensure that the data delivered to users will be presented, formatted and delivered in a consistent and secured manner. Output controls have to be enforced both in a batch-processing environment as well as in an online environment. **Various Output Controls are given as follows:**

a. Storage and logging of sensitive, critical forms
b. Logging of output program executions
c. Spooling/queuing
d. Controls over printing
e. Report distribution and collection controls
f. Retention controls

7 General Controls

Some of the general controls that are quite commonly used are derived and shown in the following diagram:



1. **Organizational Controls:** These controls are concerned with the decision-making processes that lead to management authorization of transactions. Companies with large data processing facilities separate data processing from business units to provide control over its costly hardware, software, and human resources. **Organizational control techniques include documentation of** :
   (i) Segregating the maker / creator from checker
   (ii) Reporting responsibility and authority of each function
   (iii) Definition of responsibilities and objectives of each function
   (iv) Policies and procedures
   (v) Job descriptions, and
   (vi) Segregation of duties

2. **Management Controls:** The controls adapted by the management of an enterprise are to ensure that the information systems function correctly and meet the strategic business objectives. The scope of control here includes framing high level IT policies, procedures and standards on a holistic view and establishing a sound internal control framework within the organization. The control considerations

while reviewing management controls in **an IS system shall include:**

a. Responsibility,
b. An IT Organization Structure and
c. An IT Steering Committee.

3. **Financial Controls:** These controls are generally defined as the procedures exercised by the system user personnel over source, or transactions origination, documents before system input. These areas exercise control over transactions processing using reports generated by the computer applications to reflect un-posted items, non-monetary changes, item counts and amounts of transactions for settlement of transactions processed and reconciliation of the applications (subsystem) to general ledger. Few examples is budgets, dual control & documentation etc.

4. **Business Continuity Planning (BCP) Controls:** These controls are related to having an operational and tested IT continuity plan, which is in line with the overall business continuity plan, and its related business requirements so as to make sure IT services are available as required and to ensure a minimum impact on business in the event of a major disruption.

5. **Operating System Controls:** Operating system performs major tasks that include Scheduling Jobs, Managing Hardware and Software Resources, Maintaining System Security, Enabling Multiple User Resource Sharing, Handling Interrupts and Maintaining Usage Records. Major control objectives are: Protect itself from user; Protect user from each other; Protect user from themselves; the operating system must be protected from itself; and the operating system must be protected from its environment.

The following security components are found in

1. secure operating system:
2. Log-in Procedure,
3. Access Token,
4. Access Control List and
5. Discretionary Access Control.

6. **Data Management Controls:** These Controls fall in two categories:

(a) Access Controls: Access controls are designed to prevent unauthorized individual from viewing, retrieving, computing or destroying the entity's data. Controls are established in the following manner: *User Access Controls through passwords, tokens and biometric Controls; and Data Encryption: Keeping the data in database in encrypted form.*

(b) Back-up Controls: Backup controls ensure the availability of system in the event of data loss due to unauthorized access, equipment failure or physical disaster; the organization can retrieve its files and databases. **Various backup strategies are:**

(i) *Dual recording of data,*
(ii) *Periodic dumping of data*,
(iii) *Logging input transactions and*
(iv) *Logging changes to the data.*

7. **System Development Controls:** System development controls are targeted to ensure that proper documentations and authorizations are available for each phase of the system development process. **These includes**

a. System Authorization Activities,
b. User Specification Activities,
c. Technical Design Activities,
d. Internal Auditor's Participation,

e. Program Testing,
f. User Test and
g. Acceptance Procedures

8. **Computer Centre Security and Controls:** These are of the following types:
    1. **Physical Security:** The security required for computer system can be categorized as security from accidental breach and intentional breach. Physical security includes arrangements for
        a. *Fire Damage,*
        b. *Water Damage,*
        c. *Power Supply Variation,*
        d. *Pollution Damage and*
        e. *Unauthorized Intrusion*.
    2. **Software & Data Security:** In today's business world, trade is through networks & has spread over geographical area, so security is must, e.g. Passwords & PINs, Monitoring after office hour's activity etc.
    3. **Data Communication Security:** This is another important aspect to be covered, e.g. Audit trails of crucial network activities, Sign on user identifier etc.

9. **Internet and Intranet Controls:** There are some major exposures in the communication sub-system including Internet and Intranet, which are given as follows:
    a. **Component Failure:** Data may be lost or corrupted through component failure.
    b. **Subversive Threats:** An intruder attempts to violate the integrity of some components in the sub-system.

    The mechanisms used to control such risks are
    - *Firewalls,*
    - *Encryption,*
    - *Recording of Transaction Log and*
    - *Call Back Devices.*

10. **Personal Computer Controls:** The Security Measures that could be exercised to overcome related risks are:
    a. *Physically locking the system;*
    b. *Proper logging of equipment shifting;*
    c. *Centralized purchase of hardware and software;*
    d. *Standards set for developing, testing and documenting;*
    e. *Uses of antimalware software; and*
    f. *The use of personal computer and their peripherals must be controlled*. 9845324040

Controls over Data Integrity and Security: The primary objective of data integrity control techniques is to prevent, detect, and correct errors in transactions as they flow through various stages of a specific data processing program. **There are six categories of integrity controls:**

1. Source data control,
2. Input validation routines,
3. On-line data entry controls,
4. Data processing and storage controls,
5. Output controls and Data
6. Transmission controls.

Data integrity controls protect data from accidental or malicious alteration or destruction and provide assurance to the user that the information meets expectations about its quality and integrity.

Categories of Data integrity

(i) Source data control
(ii) Input validation routine
(iii) Online data entry controls
(iv) Output controls
(v) Data transmission control

Data Integrity Policies: Major data integrity policies are:

(i) Virus-Signature Updating,
(ii) Software Testing,
(iii) Division of Environments etc.
(iv) Off site backup storage
(v) Quarter end & year end back up
(vi) Disaster recovery

Cyber Frauds: Cyber Fraud shall mean fraud committed by use of technology. Cyber fraud refers to any type of deliberate deception for unfair or unlawful gain that occurs online. The most common form is online credit card theft. On the basis of the functionality, **these are of two types:**

1. **Pure Cyber Frauds:** Frauds, which exist only in cyber world. They are borne out of use of technology. For example: Website hacking.

2. **Cyber Enabled Frauds:** Frauds, which can be committed in physical world also but with use of technology; the size, scale and location of frauds changes. For example: Withdrawal of money from bank account by stealing PIN numbers.

Cyber Attacks: Major cyber-attacks are:

1. Phishing,
2. Network Scanning,
3. Virus/Malicious Code,
4. Spam,

Website Compromise/Malware Propagation and others like

a. Cracking,
b. Eavesdropping,
c. E-mail Forgery,
d. E-mail Threats and
e. Scavenging.

Impact of Cyber Frauds on Enterprises: The impact of cyber frauds on enterprises can be viewed under the **following dimensions**:

1. Financial Loss,
2. Legal Repercussions,
3. Loss of credibility or Competitive Edge,
4. Disclosure of Confidential,

5. Sensitive or Embarrassing Information and
6. Sabotage.

Techniques to Commit Cyber Frauds: Following are the major techniques to commit cyber frauds:

1. **Hacking:** It refers to unauthorized access and use of computer systems, usually by means of personal computer and a telecommunication network. Normally, hackers do not intend to cause any damage.
2. **Cracking:** Crackers are hackers with malicious intentions, which means, un-authorized entry. Now across the world hacking is a general term, with two nomenclatures namely: Ethical and Un-ethical hacking. Un-ethical hacking is classified as Cracking.
3. **Data Diddling:** Changing data before, during, or after it is entered into the system in order to delete, alter, or add key system data is referred as data diddling.
4. **Data Leakage**: It refers to the unauthorized copying of company data such as computer files.
5. **Denial of Service (DoS) Attack**: It refers to an action or series of actions that prevents access to a software system by its intended/authorized users; causes the delay of its time-critical operations; or prevents any part of the system from functioning.
6. **Internet Terrorism**: It refers to the using Internet to disrupt electronic commerce and to destroy company and individual communications.
7. **Logic Time Bombs:** These are the program that lies idle until some specified circumstances or a particular time triggers it. Once triggered, the bomb sabotages the system by destroying programs, data or both.
8. **Masquerading or Impersonation**: In this case, perpetrator gains access to the system by pretending to be an authorized user.
9. **Password Cracking**: Intruder penetrates a system's defense, steals the file containing valid passwords, decrypts them and then uses them to gain access to system resources such as programs, files and data.
10. **Piggybacking**: It refers to the tapping into a telecommunication line and latching on to a legitimate user before s/he logs into the system.
11. **Round Down:** Computer rounds down all interest calculations to 2 decimal places. Remaining fraction is placed in account controlled by perpetrator.
12. **Scavenging or Dumpster Diving:** It refers to the gaining access to confidential information by searching corporate records.
13. **Social Engineering Techniques:** In this case, perpetrator tricks an employee into giving out the information needed to get into the system.
14. **Super Zapping:** It refers to the unauthorized use of special system programs to bypass regular system controls and performs illegal acts.
15. **Trap Door:** In this technique, perpetrator enters in the system using a back door that bypasses normal system controls and perpetrates fraud.

In spite of having various controls as well as countermeasures in place, cyber frauds are happening and increasing on a continuous basis. To overcome these frauds, there is an urgent need to conduct research in the related areas and come up with more appropriate security mechanisms, which can make information systems more secure.