CHAPTER 3

PROTECTION OF INFORMATION SYSTEM

1. INTRODUCTION:

In this changing environment most of the business processes are automated. Organisations are relying heavily on the Information technology for information and transaction processing. But the organisations relying on such technologies are indeed vulnerable to various threats related to technology.

2. NEED FOR PROTECTION OF INFORMATION SYSTEMS:

As discussed in previous topic about the technological risks, consequences of it there exists a gap between **need to protect the system** and **degree of protection applied**:

CODE TO REMEMBER: E^2 – D.I.E.T.

1. **E**limination Of distance, time and space as constraints.
2. **E**lectronic attacks.
3. **D**evolution of management and control
4. **I**nterconnectivity of systems.
5. **E**xternal factors such as **legislature, legal and regulatory requirements or technological development.**
6. **T**echnology usage is worldwide.

Information system failure may result in both financial and intangible loss such as unauthorised access to sensitive information.

3. INFORMATION SYSTEMS SECURITY:

Information security refers to **protection of valuable assets against loss, disclosure or damage.** Security policy not only safeguard the physically **(lockers, fences etc)** but also ensures logical safeguards to be installed **(identifiers, password, firewalls etc.)**

In order to ensure protection of information system and information from unauthorised access, loss, theft etc it is indeed mandatory for the organisation to install a layered series of technological and non-technological safeguards.

INFORMATION SECURITY OBJECTIVES:

The objective of information system security is to:

1. Protect interest of those relying on information.
2. Protect the information system and communications that deliver the information from harm, resulting from **failure of confidentiality, integrity and availability.**

For any organisation, security objectives comprise 3 universally attributes:

1. **Confidentiality:** Prevention of unauthorised information disclosure.
2. **Integrity:** Prevention of unauthorised information modifications.
3. **Availability:** Prevention of unauthorised information withholding.

INTEGRITY
AVAILABILITY
INFORMATION SECURITY
CONFIDENTIALITY
101
1010
000101

4. WHAT INFORMATION IS SENSITIVE:

The following types of information can be regarded as sensitive if it relates to:

CODE TO REMEMBER: F.B.S. (Fake Balance Sheet)

A. FINANCES:

Financial information such as salaries, wages, customer position order, cash and bank position are very crucial and should not be disclosed or made public. When a competitor knows specific information about the company's wages, he may be able to price its product accordingly. As such the damage to the organisation may be significant.

B. BUSINESS OPERATIONS:

It consists of an organisation process and procedures which are related to production and technologies. It is necessary to protect or secure such type of information. Leakage of any such information led to market advantage of its competitor. Any carelessness may result in inadvertent (negligent) storage of data on **unauthorised system.**

C. STRATEGIC PLANS:

Strategic plans are very crucial for the success of the company and it is rather imperative to protect these strategic plans. These plans normally involves the decision making part of the management. For instance, a company discover new areas of launching its product, but due to weak information system the same is being exploited by its competitors.

5. INFORMATION SECURITY POLICY :

An information security policy is the **statement of intent** by the management about how to protect a company's information assets. Information security policy is:

WHY INFORNATION SECURITY POLICY NEEDED BY MANAGEMENT

A. Format rules which give access to people to the organisation's technology and information assets.
B. A document that describes information security controls and activities.
C. An essential foundation for an effective and comprehensive information security program.
D. It provides guidance to people who build, install and maintain information systems.

THINGS THAT MUST BE ENSURED BY THE INFORMATION SECURITY POLICY

A. Preserve and protect information from any unauthorised modifications, access or disclosure.
B. Limit or eliminate legal liability from employees or third party.
C. Prevent waste or inappropriate use of organisations resources.

TOOLS TO IMPLEMENT POLICY: STANDARDS, GUIDELINED AND PROCEDURES:

Policies are broad general statements for which organisation have to develop standards, guidelines and procedures that **offer users, managers** a clear approach for implementing the policies and to achieve organisational objectives.

STANDARDS: Specifies **technologies and methodologies to be used to secure the systems.** It specifies uniform use of technologies across the organisation. Standards are compulsory within an organisation.

GUIDELINES: Guidelines helps in **smooth implementation of information security policies.** It assists user, system personnel and others in effectively securing their system.

PROCEDURES: These are more detailed steps to be followed to accomplish security related tasks. Procedure normally assists in implementing **applicable information security policy.** These are detailed steps to be followed by the users.

ISSUES TO ADDRESS:

The policies must clearly state **management commitment to information security.** The policy should atleast address the following issues:

A. Definition of information security.
B. Goals and principles of information security and why it is important to organisation.
C. Explanation of **security policies, principles, standards and compliance requirements.**
D. Definition of all relevant information security responsibilities.

MEMBERS OF SECURITY POLICY:

Security has to cover **trio (Managerial, technological and legal aspects).** Security policy comprises **3** groups of management:

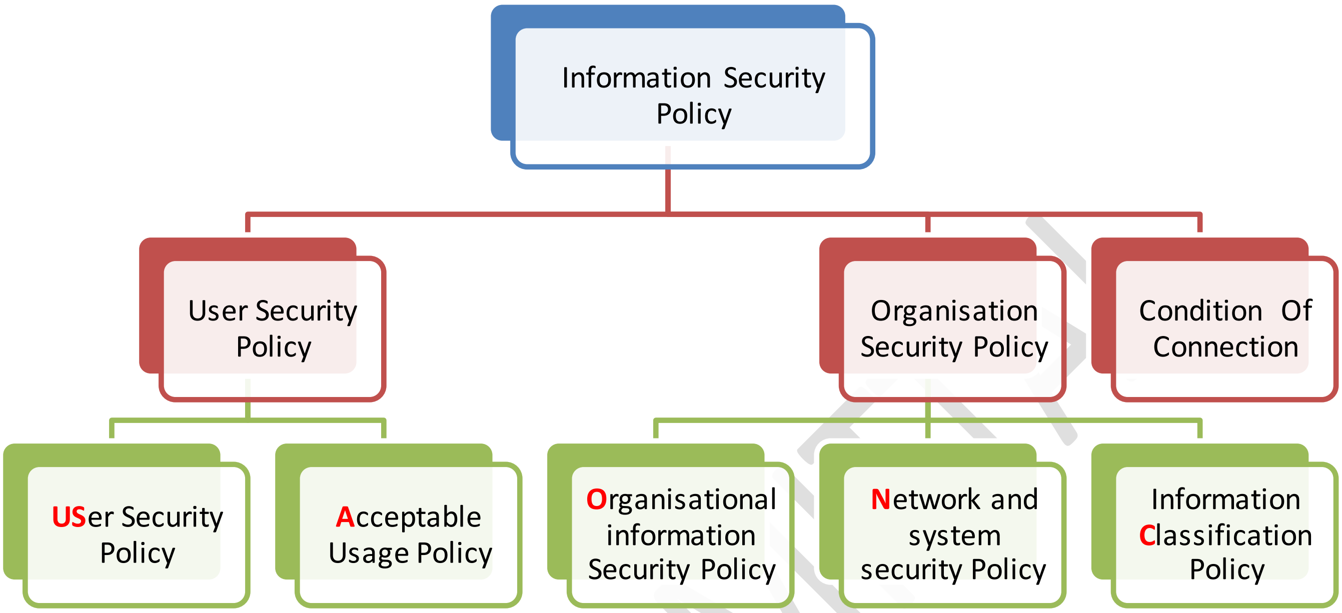
Management members who have policy making authority

Technical group who know what can be supported or not...

LEGAL EXPERTS

Who knows legal ramification (unwelcome consequence) **of various policy charges.**

INFORMATION SECURITY POLICIES AND THEIR HIERARCHY


Information Security Policy
User Security Policy
Organisation Security Policy
Condition Of Connection
USer Security Policy
Acceptable Usage Policy
Organisational information Security Policy
Network and system security Policy
Information Classification Policy

CODE TO REMEMBER: U.S.A. - O.N. - C

USER SECURITY POLICY->

1. **USer Security Policy:** This set out the responsibilities & requirements from information security.
2. **Acceptable Usage policy:** This policy defines rules for use of email and internet services.

ORGAISATION SECURITY POLICY->

3. **Organizational Information security policy:** Defines group of policies for security of information assets and IT systems.
4. **Network and system security policy:** This policy defines rules for network & data communication security.
5. **Information Classification Policy:** This policy defines rules for classification of information.

CONDITION OF CONNECTION->

This policy defines the rules for access of network and it also specifies the conditions to be satisfied for connection to network.

6. INFORMATION SYSTEM CONTROLS :

The increasing use of IT in organizations has made it imperative that appropriate information systems are implemented in an organization. IT should cover all key aspects of business processes of an enterprise and should have an impact on its strategic and competitive advantage for its success.

The enterprise strategy outlines the approach, it wishes to formulate with relevant policies and procedures to achieve business objectives. 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. An information systems auditing includes reviewing the implemented system or providing consultation and evaluating the reliability of operational effectiveness of controls.

NEED FOR CONTROLS IN INFORAMTION SYSTEM

Today's dynamic global enterprises need information integrity, reliability and validity for timely flow of accurate information throughout organisation. Safeguarding assets is to maintain data integrity to achieve system effectiveness and efficiency. IS control procedure may include:

- Strategy and direction,
- General Organization and Management,
- Access to IT resources, including data and programs,
- System development methodologies and change control,
- Operation procedures,
- System Programming and technical support functions,
- Qualify Assurance Procedures,
- Physical Access Controls,
- BCP and DRP,
- Network and Communication,
- Database Administration, and
- Protective and detective mechanisms against internal and external attacks.

OBEJCTIVES OF CONTROL

Control is defined as **policies, procedures, practices and enterprise structure** that are designed to provide reasonable assurance that business objectives are met. An information system auditing includes reviewing the **implemented system or providing consultation and evaluating the reliability** of operational effectiveness of controls.

Some categories of exposure are:

(a) Error or omission of data, procedure or process.
(b) Improper authorisation, judgements or comparison.
(c) Inefficient activity in procedure, processing and comparison.

Here are some of the critical controls lacking in the computerised environment:

(a) Lack of management understanding of IS risks and related controls.
(b) Absence of weak general control system.
(c) Absence of inadequate IS control framework.
(d) Lack of awareness and knowledge of IS risks and controls.

(e) Lack of control features.
(f) Inappropriate technology implementation or inadequate security functionality.

IMPACT OF TECHNOLOGY ON INTERNAL CONTROLS

The internal controls within enterprises in **a computerised environment** cover the **following major areas:**

A. **Personnel:**
-- Whether staff is trustworthy or not.
-- Whether the personnel knows what are their objectives & if they have requisite skill to do.

B. **Segregation of duties:**
-- Segregation means **various stages in the process of a transaction** are split among people.
-- Within a computerised environment, the staffs **know the interrelationship** between the source of data, how it is processed & distribution & use of the outputs.

C. **Authorisation procedures:**
-- To ensure that **transactions are approved.**
-- **In on-line** transaction system, **written evidences of individual** data entry authorisation

D. **Record Keeping:**
-- Controls over **protection & storage of documents, transaction details & audit trail** etc

E. **Access to assets & records:**
-- Client's financial information is more prone to **unauthorised access.** Increased use of the networking facilities **increases the risk of unauthorised access.**
-- As such proper controls are needed to protect the critical information by way **of physical & logical controls.**

F. **Management supervisions & review:**
-- Management supervisions & review helps **in detecting ERROR & FRAUD** on regularly basis.

G. **Concentration of programs & data:**
-- Transactions, programs & data files may be stored in **computer readable form.**
-- **In the absence of** appropriate controls over this programs from **unauthorised access**

Without adequate controls, anyone can access to records and make amendments, some of which could be undetected. Internal controls comprise of the following **5 INTERRELATED COMPONENTS:**

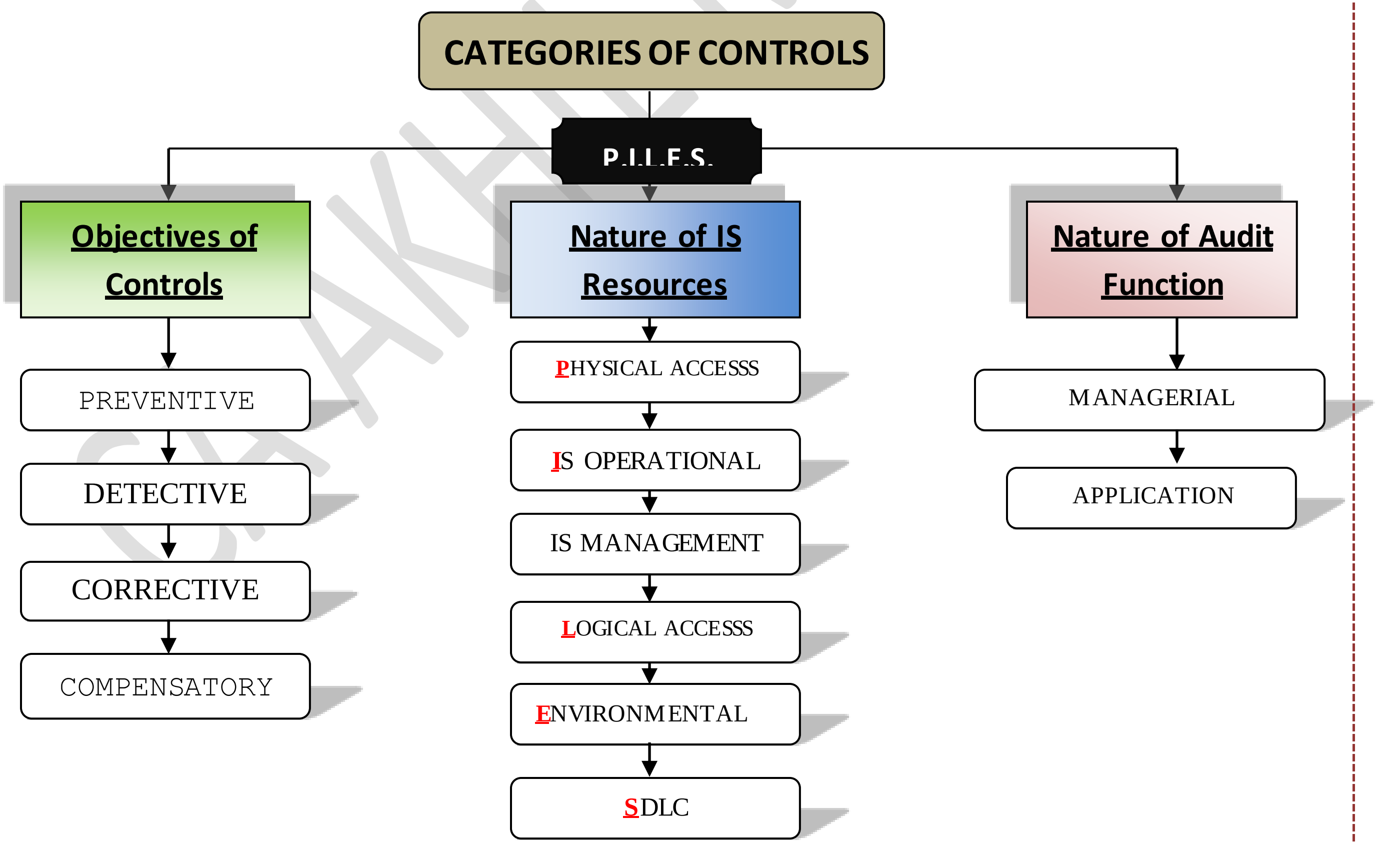
CONTROL ENVIRONMENT	Elements that establish the control context in which specific accounting system and control procedures must operate.

RISK ASSESSMENT	Elements that identify and analyse the risks faced by an organisation and the way risks can be managed.
CONTROL ACTIVITIES	Elements that operate to ensure transactions are authorised, duties are segregated, documents are maintained, assets and records are safeguarded.
INFORMATION & COMMUNICATION	Elements in which information is identified and captured and exchanged in timely manner to allow personnel to discharge their responsibilities.
MONITORING	Elements that ensure internal controls operate reliably over the time.

7. CLASSIFICATION OF IS CONTROL:

Following are the classification of controls:

CATEGORIES OF CONTROLS


CATEGORIES OF CONTROLS

P.I.I.L.E.S.

Objectives of Controls
- PREVENTIVE
- DETECTIVE
- CORRECTIVE
- COMPENSATORY

Nature of IS Resources
- PHYSICAL ACCESSS
- IS OPERATIONAL
- IS MANAGEMENT
- LOGICAL ACCESSS
- ENVIRONMENTAL
- SDLC

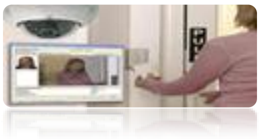
Nature of Audit Function
- MANAGERIAL
- APPLICATION

OBJECTIVES OF CONTROLS

TYPE OF CONTROL	CHARACTERISTIC	EXAMPLES
PREVENTIVE CONTROL 	-- Understanding the vulnerabilities of assets -- Understanding probable THREATS -- Provision of necessary controls	-- Segregation Of duties -- Access Control -- Firewalls, Antivirus software
DETECTIVE CONTROL 	--Detecting Errors, omissions, malicious act etc. --Clear understanding of lawful activities & report deviation --Surprise Checks by supervisor	--Error message over tape labels. --Periodic report of the performance with variance -- Internal Audit functions
CORRECTIVE CONTROL	--Minimise impact of the THREAT --Identify the CAUSE of problems --Correct error arising from a problem --Getting feedback from detective & preventive control	--Backup procedures. --Rerun procedures --Contingency Planning
COMPENSATORY CONTROL	--Designed to REDUCE probability of threats. --Implemented where organisation is not able to have appropriate CONTROLS. --Compensatory measures to be adopted to reduce probability of threats	

ANOTHER CLASSIFICATION OF CONTROLS **based on NATURE of such controls is as under:**

NATURE OF IS RESOURCES

TYPE OF CONTROL	CHARACTERISTIC	EXAMPLES
PHYSICAL ACCESS CONTROL 	--Controls relating to PHYSICAL SECURITY of the tangible IS resources & intangible resources.	-- Access control Doors -- Security Guard -- Door Alarm
IS OPERTIONAL CONTROL	--Controls relating to IS operations, administration & its management.	-- Helpdesk Operations -- IS Infrastructure mgmt.
IS MANAGEMENT CONTROL	--Controls relating IS management, policies, procedures, standards etc	-- Monitoring of IS operations -- Steering Committee
LOGICAL ACCESS CONTROL 	--Controls relating to logical access to information resources.	-- Networking Control --Application boundary controls
ENVIRONMENTAL CONTROL 	--Controls relating for HOUSING IT resources	-- Smoke Detection -- Fire extinguisher -- Power, air conditioning
SDLC CONTROL	--Controls relating to planning, design, development, testing etc	

ENVIRONMENTAL CONTROL

This section deals with **external factors** in **information system & preventive measures** to overcome these conflicts. Issues covered:

-- Environmental issues & exposures
-- Audit & evaluation techniques for environmental controls.

Following are the information system resources:

1. HARDWARE & MEDIA:

-- Includes computer & communication equipment & storage media

2. INFORMATION SYSTEMS SUPPORTING INFRASTRUCTURE:

-- Includes the following

Physical premises	Communication Closet
Cabling Ducts	Power Source

3. DOCUMENTATION:

--Physical & geographical Documentation of,

--Computing facilities with emergency plans & incident planning procedure.

4. SUPPLIES:

-- Third party maintenance procedure,

-- By the civil contractors whose entry & assess with respect to their scope of work assigned.

5. PEOPLE:

-- Employees, contractor employees, visitors, third party personnel,

-- are to be made responsible/accountable for environmental controls.

ENVIRONMENTAL ISSUES AND EXPOSURES

Environmental exposures are primarily due to elements of nature, however, with proper controls, exposure to rudiments can be reduced. **Environmental exposures are:**

- Fire Damage : the most common risk to any facility
- Water Damage / flooding – even with facilities located on upper floors of high buildings.
- Power spike
- Electrical Shock
- Natural disasters – earthquake , volcano, hurricane, tornado
- Equipment failure, air Conditioning failure, bomb threats

CONTROLS FOR ENVIRONMENTAL EXPOSURES

1.WATER & SMOKE DETECTOR:

-- Presence of water & smoke detector are to be,
-- Verified by visiting the computer rooms.

2.HAND HELD FIRE EXTINGUISHER:

-- Presence of fire extinguisher in strategic locations.
-- Throughout the facility is checked for.

3.FIRE SUSPENSION SYSTEMS:

-- Testing of **suppression systems,** & documenting that the system has been inspected **& tested.**

4.FIREPROOF WALLS, FLOORS ETC.

-- Check the fire rating of the wall surrounding the information system facilities.

5.ELECTRICAL SURGE PROTECTOR:

-- Here, **presence of** electrical surge **protectors** for **sensitive & expensive computer equipment** is observed.

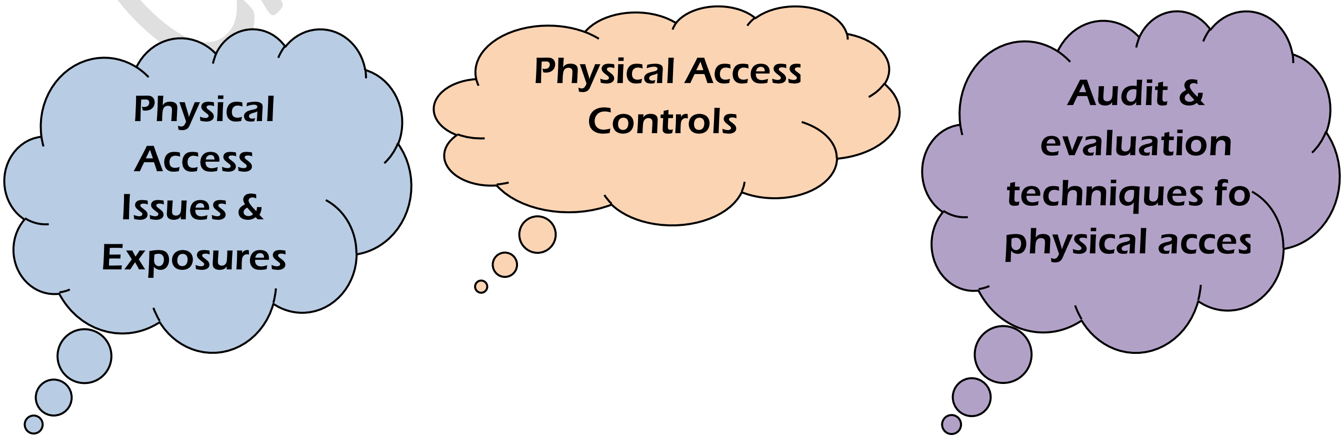
6.WIRING PLACED IN ELECRTIC PANELS:

-- Check whether **wiring in the information** facilities **is placed** in the fire resistant panel.

1. PHYSICAL ACCESS CONTROLS:

This section of my notes **deals with the losses due to accidents, intentional violation of access paths** etc.

It covers the flowing 3 areas of discussion



Physical Access Issues & Exposures

Physical Access Controls

Audit & evaluation techniques fo physical acces

Now explaining each of the above said areas in detail:

PHYSICAL ACCESS ISSUES & EXPOSURES

Following points depicts the result due to intentional violation of access paths:

Code to Remember: U.B.I. - M.A.D.E.

1. **U**nauthenticated entry.
2. **B**lackmail
3. **I**nformation disclosure publicly.
4. **M**odification of semester equipment & information.
5. **A**buse of data processing resources.
6. **D**amage or theft of documents or equipment
7. **E**mbezzlement.

POSSIBLE PERPETRATORS:

-- Perpetrators may be because of employees who are:

- Discontented
- Former Employees
- On Strike
- Terminated employee

- Interested outsider.
- Threatened for disciplinary action
- Addicted to gambling

-- Facilities to be protected from **auditor point of view:**

- Computer Room
- Local Area Network
- Power sources
- Storage rooms

- Portable equipment
- Control Units
- Input/output control room

ACCESS CONTROL MECHANISM:

-- It is associated with **identified, authorised** users & the resources they are allowed to access.
-- The **mechanism** processes **user request in 3steps:**
-- Identification
-- Authentication
-- Authorisation

Control for Physical Access Controls

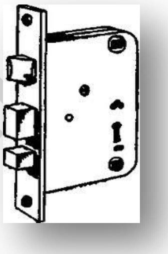
Physical access controls are designed to protect the organisation **from UNAUTHORISED ACCESS.** Some of common access controls techniques are as follows:

(a) **Locks on Doors:**

CIPHER LOCKS

-- Cipher lock consists of **pushbutton** fixed near door.
-- There are **10 numbered buttons** on the panel.
-- To enter. **A person has to punch 4 DIGIT** sequence & door unlock for **a predetermined period.**

BOLTING DOOR LOCKS



-- Special metal key is used **to gain entry,**
-- When the lock is a **bolting door lock.**

ELECTRONIC DOOR LOCKS

-- A magnetic **chip-based** plastics card key, may be
-- Entered into **a sensor reader to gain access in system.**
-- Thereafter the sensor read the code, **that is stored** within **card activates** the door locking mechanism.

BIOMETRIC DOOR LOCKS

-- These locks are extremely secure, which uses individual's unique body features such as:
-- **Retina, voice, fingerprints, signature** etc.
-- **This type of security needed to protect sensitive information.**

(b) **Physical Identification medium:**

PERSONAL IDENTIFICATION NUMBERS

-- A secret number is assigned to individual.
-- Visitor is asked to **log on** by inserting card in device & enter their PIN for authentication.
-- Example : **Cash withdrawal procedure from ATM**

PLASTIC CARDS

-- These cards used **for identification purpose**.
-- Control over this card ensures **authorised access** by the users.

IDENTIFICATION BADGES

-- Can be **issued to personnel as well to visitors.**

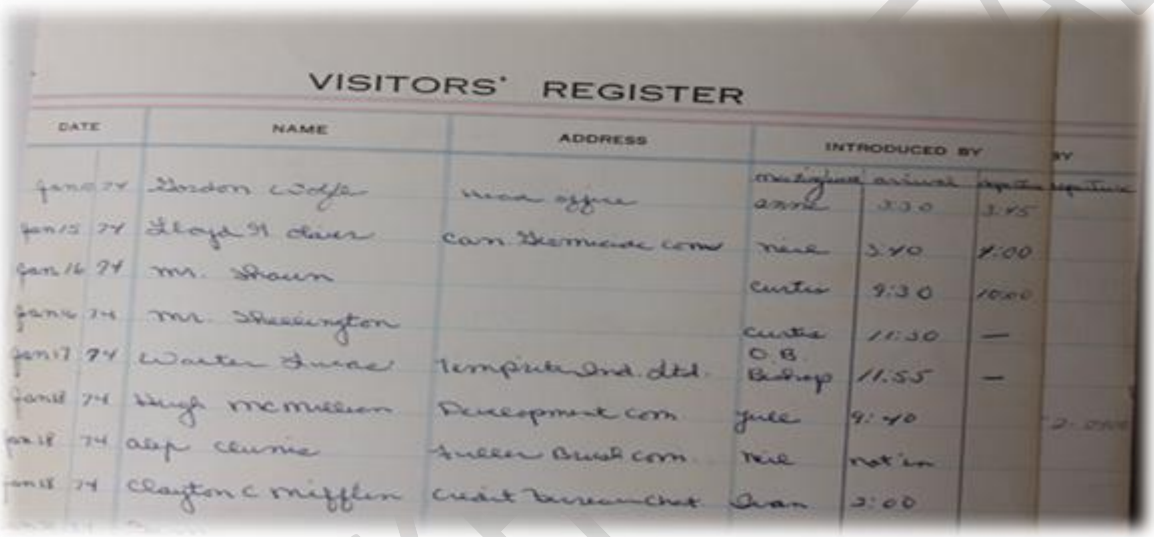
-- For easy identification, **badges** may be given different **colours.**

(c) **Logging on utilities:**

MANUAL LOGGING

-- Keeps the record of the visitors **including NAME, PURPOSE OF VISIT, and PERSON TO SEE.**

-- Any identification proof may also be asked for gaining the entry.



VISITORS' REGISTER

DATE	NAME	ADDRESS	INTRODUCED BY			BY
			meeting with	arrival	departure	departure
Jan ? 74	Gordon Wolfe	head office	Anne	3:30	3:45	
Jan 15 74	Lloyd H. Davies	Can. [illegible] com	Neil	3:40	4:00	
Jan 16 74	Mr. Shawn		Curtis	9:30	10:00	
Jan 16 74	Mr. Sheffington		Curtis	11:30	—	
Jan 17 74	Walter [illegible]	Templeton Ind. Ltd.	O.B. Bishop	11:55	—	
Jan 18 74	Hugh McMillan	Development com	Julie	9:40		2:00
Jan 18 74	Alf Clunie	Fuller Brush com.	Neil	not in		
Jan 18 74	Clayton C Mifflin	Credit Bureau Chat	Ivan	2:00		

ELECTRONIC LOGGING

-- This feature is combination of electronic and biometric security system.

-- The users logging can be monitored and unsuccessful attempts being highlighted.

(d) Other means of controlling physical access:

❖ Video Cameras	❖ Computer Terminal Locks
❖ Security Guards	❖ Alarm System
❖ Controlled Visitor Access	❖ Perimeter Fencing
❖ Bonded Personnel	❖ Secured Report
❖ Dead Man Doors	❖ Controlled single Entry Point

2. LOGICAL ACCESS CONTROLS:

It is also known as electronic or technological controls. It restricts the access of resources through programs, applications and network channels to authorized users only. These controls are designed to designate WHO or WHAT to have access to a SPECIFIC SYSTEM RESOURCES & type of transactions & functions. Assessing logical access controls involves evaluating the FOLLOWING critical procedures*:*

-- Logical access control restricts the **unauthorized access to system.**
-- There are logical controls over the **network access.**
-- Controls implemented **to protect the integrity of the application.**

Here we will discuss some of the

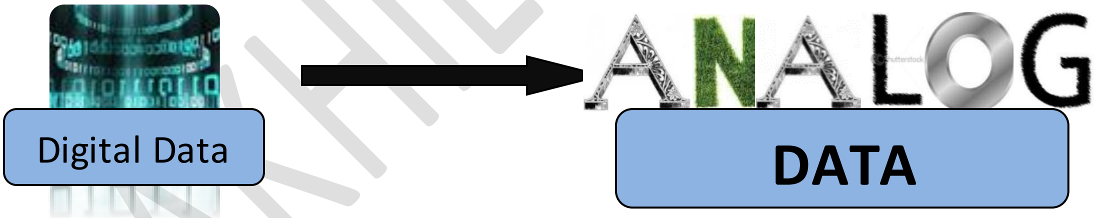
LOGICAL PATH ACCESS

1. **Online Terminals:**
   -- To access on line terminals, a user has to provide a valid LOGIN-ID & password.

   Operator Console:
   -- The operator console is the place where intruder can play havoc (नाश).
   -- Due to above reason, operator console need to be protected and access to be restricted.
   - Keeping the operator console at a place where it is visible t\o all.
   - By keeping the console in protected room accessible to selected personnel.

2. **Dial up ports:**
   -- Dial up port connects remotely to other network via communication media.
   -- MODEM = convert

INTO



-- Modem can be used to connect with other through terminal & telephone lines.

3. **Telecommunication Network:**
   -- In this network, a number of computer terminals, personal computers etc are host computers, through network or telephone lines.
   -- Each of these routes has to be protected by means of security procedures**.**

LOGICAL ACCESS ISSUES AND EXPOSURES

Control that reduces the risks of misuse of theft, alteration or destruction of information. This should be done to protect information from unauthorised and unnecessary access to computer files.

Restricting and monitoring the computer operation activities in a batch-processing environment provide this control. The opportunities of access in an online system, is more and **hence level of control for this system must be more complex.**

ISSUES AND REVELATIONS RELATED TO LOGICAL ACCESS

Logical access controls are used to increase the **organization's potential** for the losses that result due to **exposures** that may lead to shut down of the system. Some of the exposures that an entity's system is **open to:**

TECHNICAL EXPOSUERS

It includes unauthorised implementation & modification of data & software.

I. DATA DIDDLING:

-- Data diddling involves **change of data** before **or** as they entered in system.

-- **Limited** technical knowledge is required **to diddle data.**

II. BOMBS:

-- Bomb is a piece **of BAD CODE** deliberately planned by an insider.
-- This bomb explodes or cause damage when **condition of explosion** gets fulfilled.
-- Bombs are generally of 2 types:

TIME BOMB

- It causes disruption **of computer, system modification of data etc.** on a **particular DATE & TIME** for which it is developed.
- The ***COMPUTER CLOCK*** initiate it

LOGIC BOMB

- It is **combination of EVENTS.**
- For instance
  "If a file name **Akhil** is changed, then content will be **permanently deleted.**"

III.TROJAN HORSE:

-- These are **program hidden under AUTHORISED PROGRAM.**
-- It is **ILLICIT (ILLEGAL)** coding contained in **a legal program.**
-- **It doesn't copy itself to** another machine.
-- Trojan May Result In:

Change or steal The password

May modify records in protected files

May allow illicit users to use the systems

IV. WORMS:

--WORM copies itself **to another machine on the network.**

--Worms **are stand-alone programs,** & can be easily detected.

--Worms **doesn't harm or cause damage to the** system, **BUT ONLY COPIES** itself in a **computer network.**

V. ROUNDING DOWN:

-- Refers to **ROUNDING OF SMALL FRACTIONS,** of a **denomination** & **transferring fractions to AUTHORISED** account.

VI. SALAMI TECHNIQUES:

-- Involves slicing of small amounts of money from computerised transactions. For example Rs. 21,45,526.95 is being written as Rs. 21,45,526.

VII. TRAP DOORS:

-- It allows **insertion of SPECIFIC LOGICS,** such as program interrupts **that permits a review of the data.**

-- It also permits insertion of UNAUTHORISED LOGIC.

COMPUTER CRIME EXPOSUERS

Computer systems are used to steal money, goods, software or corporate information. Some of the side effects of these computer crimes are as follows:

1. FINANCIAL LOSES:

-- It covers **loss of electronic funds,**

-- Or increase in **expenditure towards repair of** damaged electronic components.

2. LEGAL REPERCUSSION:

-- An entity has to adhere to various **human rights** policies.

-- Organisation is **exposed to LAWSUITS** from investors in case of non-compliance of rules.

-- Auditor must take **legal view** before reviewing the issues related to it.

3. LOSS OF CREDIBILITY:

-- Credibility is the **ESSENCE** of any business to **maintain its competitive edge in market.**

-- This credibility will be shattered **resulting in loss to the business & prestige.**

4. BLACKMAIL:

-- The perpetrator **(One who designs)** can obtain money from the organisation by **threatening & exploiting the SECURITY VIOLATION.**

5. DISCLOSURE OF INFORMATION:

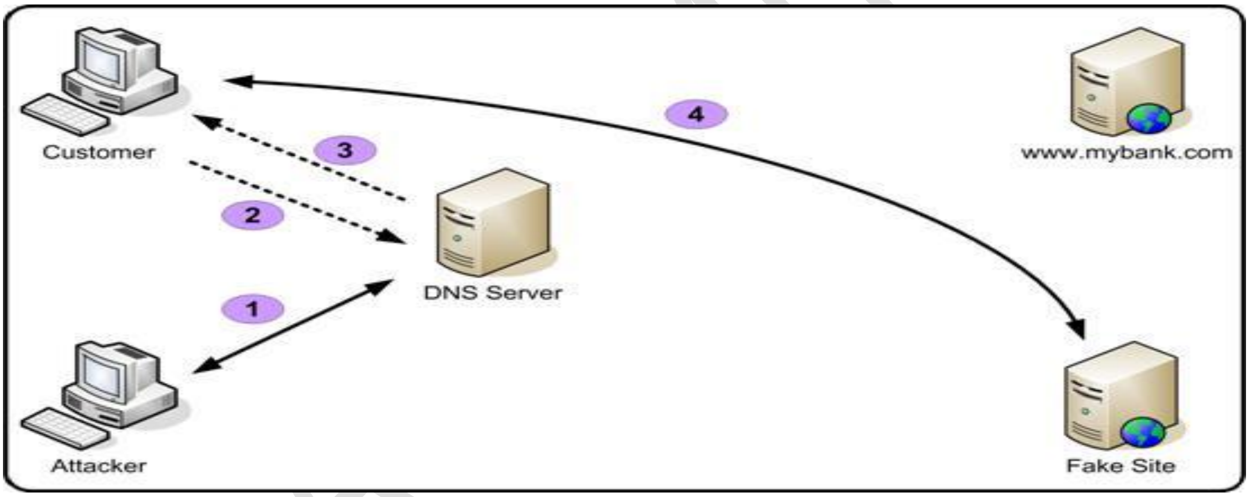
-- This event involves **disclosure of sensitive, confidential** information.
-- Such practice can **spoil the REPUTATION** of the organisation.

6. SABOTAGE:

-- People, who are not interested in **financial gain,** also want to spoil the credibility of the organisation.
-- This is due to reason of **DISLIKE** for the organisation.

7. SPOOFING:

-- It involves FORGING ONE'S SOURCE ADDRESS.
-- Spoofing is when an attacker pretends to be someone else in order gain access to restricted resources or steal information.
-- One machine is used to **IMPERSONATE** (To assume character of) the other in spoofing technique.
-- For example, **a penetrator makes the USER think that he/she is connected to operating system.**



1. The attacker targets the DNS service used by the customer

2. The customer queries the DNS server

3. The DNS responds to the customer query– not the real IP address

4. The Customer then connects to the host, expecting it to be www.mybank.com, but in fact reaching the attackers fake site.

ASYNCHRONOUS ATTACKS:

Here data can be moved asynchronously across the telecommunication lines. Data that is waiting to be transmitted are liable to be unauthorised access called asynchronous attacks. There are many forms of Asynchronous attacks:

1. **DATA LEAKAGE:**

-- Data leakage involves **dumping files to papers OR stealing computer reports & tape.**

2. **WIRE-TAPPING:**

-- This involves **SPYING INFORMATION** being transmitted over the telecommunication network.

3. **PIGGYBACKING:**

-- This is an **act of following an AUTHORISED person through**

A SECURED DOOR

OR

ATTACHING TO AUTHORISED
TELECOMMUNICATION LINK

-- This involves **intercepting communication** between OPERATING SYSTEM & USERS**.**

4. **SHUT DOWN OF COMPUTERS :**

-- This is **initiated** through **terminals or microcomputers** that are **directly or indirectly** connected to the computers.

-- These security measures will function **if appropriate access control** on the logging. In case of **overloading** some system proved to be vulnerable & **shut them.**

-- HACKERS use this technique to **SHUT DOWN** computer system over internet.

LOGICAL ACCESS CONTROL ACROSS THE SYSTEM

This access controls are expected to restrict access to information assets/resources. Such controls must be sufficient for one to perform the duties. Data can be:
-- Used by an application.
-- Stored in some medium.
-- Or it may be in transit.

LOGICAL ACCESS CONTROL

Logical access controls are implemented in order to protect the following type of assets:

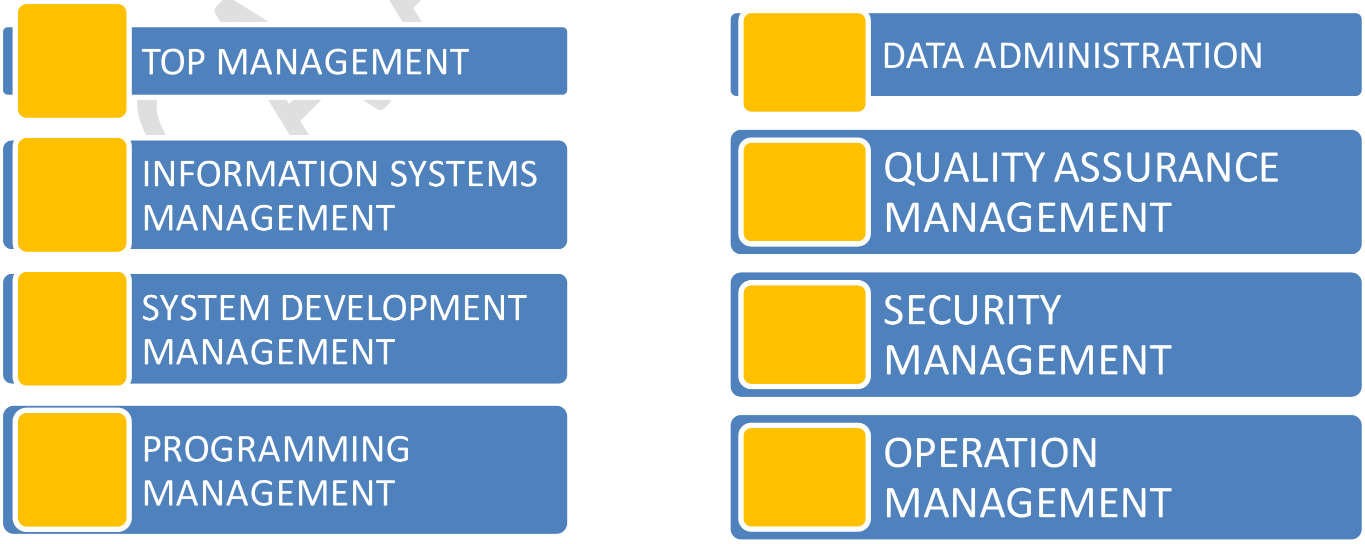
TYPES OF ASSET	SECURITY CONTROL
User Access Management	❖ Is the user registered to access the information?

USER REGISTRATION *PRIVILEGE MANAGEMENT* *USER PASSWORD MANAGEMENT* *REVIEW OF USER ACCESS RIGHT*	❖ Is de-registration process is followed? ❖ **Privilege** access i.e. **one can access that data** which he uses in fulfilling his duties. ❖ Allocation, storage, revocation & reissue of password are **password management functions.** ❖ User needs changes with time & as such **requires periodic** review of access right.
User Responsibilities *PASSWORD USE* *UNATTENDED USER EQUIPMENTS*	User awareness & responsibility is critical factor. ❖ Use of strong passwords to maintain confidentiality. ❖ User must ensure that no equipment under their responsibility is left unprotected.
Network access control *POLICY ON USE OF NETWORK SERVICES*	Internet puts an organization on stake, since one can access entity information easily: ❖ Selection of appropriate services & approval to access them is part of the policy.
ENFORCED PATH *SEGREGATION OF NETWORKS* *SECURITY OF NETWORK SERVICE*	❖ Based on risk assessment, it is necessary to specify path connecting networks. ❖ Based on sensitive information, it is necessary that some network to be isolated from the internet service. ❖ Technique of authentication & authorization policy implemented across the organization's network.
Operating system access control *AUTOMATED TERMINAL IDENTIFICATION* *TERMINAL LOG ON PROCEDURES* *USER IDENTIFICATION &*	Operating system helps application to use various IS resources & perform functions. If there is an unauthorized access, operating system is last barrier to be conquered for unlimited access. It ensures that a session could only be started from a particular location or computer terminal It doesn't provide unnecessary help to provide information which may be misused by intruder. The user must be identified & authenticated.

AUTHENTICATION *PASSWORD MANAGEMENT SYSTEM* *USE OF SYSTEM UTILITIES*	An operating system must have selection of good passwords. System utilities are the programs that help to manage critical functions of operating system.
Application & monitoring system access control *SENSITIVE SYSTEM ISOLATION* *EVENT LOGGING*	A user is allowed to access the information for which he is authorised to access. Controls are implemented on the access rights of the users. Critical constitution of the system, if necessary must be run in isolation. It is necessary to review if logging is enabled. In computer system, it is rather easy to maintain the log of all types of the events.
MOBILE COMPUTING	Theft of data on the disk drives is HIGH RISK FACTOR. To protect the data, information has to be encrypted & access identifications i.e. fingerprints, eye-iris, smart cards etc.

Type of control	Objective
MANAGERIAL CONTROLS	Here, controls over managerial control are examined that are to be performed to ensure development, implementation and maintenance of information system in a planned and controlled manner.

Following are the types of management sub-systems and their descriptions:



TOP MANAGEMENT

INFORMATION SYSTEMS MANAGEMENT

SYSTEM DEVELOPMENT MANAGEMENT

PROGRAMMING MANAGEMENT

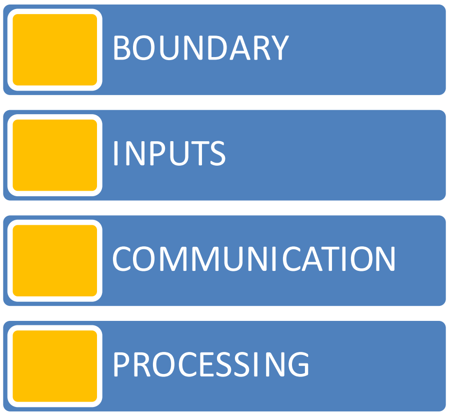
DATA ADMINISTRATION

QUALITY ASSURANCE MANAGEMENT

SECURITY MANAGEMENT

OPERATION MANAGEMENT

Type of control	Objective
APPLICATION CONTROLS	Includes programmatic routines within the application program code. It ensures that data remains complete, accurate and valid during its input, update and storage.

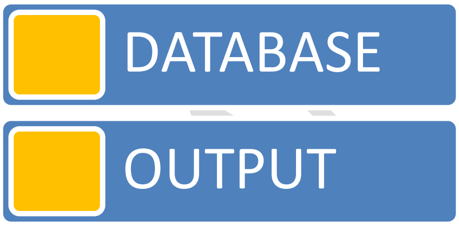


BOUNDARY

INPUTS

COMMUNICATION

PROCESSING



DATABASE

OUTPUT

TOP MANAGEMENT AND INFFORAMTION SYSTEM MGMT. CONTROLS

Top management is responsible for preparing the master plan for the information system functions. The scope of IT related functions is being decided by the top management personnel. As such, we will study the functions performed by the senior management:

PLANNING: This includes determining the goals & objectives of information system controls.

Preparing the Plan:

(1) Recognise opportunities & problems before the organisation.
(2) Identify the resources needed to provide required information and technology.
(3) Formulation of technology for acquiring the needed resources.

Types of Plan:

Strategic Plans → It is long term plan covering the next 3-5 years of operation.
Operation Plan→ It is long short term plan covering the next 1-3 years of operation.

Role of Steering Committee:

It includes representative from all areas of business, and IT personnel. The responsibility of this committee is **information technology planning.**

ORGANISING: This includes gathering, allocating and coordinating the resources needed to accomplish the goals of the organisation.

Resourcing the Information System Function:

Management should acquire the resources to accomplish the goals & objectives. Resources include **hardware, software, personnel etc.** Adequate funding should be provided to support the resources.

Staffing the Information Systems Function:

Staffing the information systems involves **application of Information system, development of information system personnel & termination of information systems personnel.**

LEADING:

This includes motivating and guiding the personnel. The main objective of leading is to achieve harmony of the objectives. The process of leading helps the manager to **motivate the subordinates**, directs them and communicate.

Motivating and leading Information systems personnel:

Strategies for motivating and leading people should be formulated & need to be changed as per the characteristic of an individual.

Communicating with IS personnel:

Effective communication is essential to create healthy environment among employees. This creates a sense of trust among work colleagues.

CONTROLLING:

Include comparison of actual performance with the standards fixed by the management. This activity is undertaken to evaluate the deviation from the standards.

Overall Control of IS function:

Top management has to decide as to how much to be spent on the information system functions.

Control of Information system Activities:

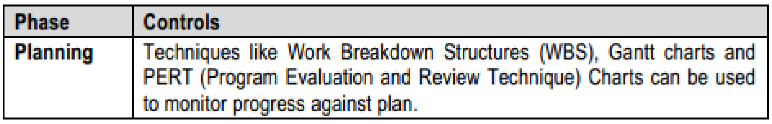
Management would like to control IS activities on the basis of policies and procedures.

Control over Information system Services:

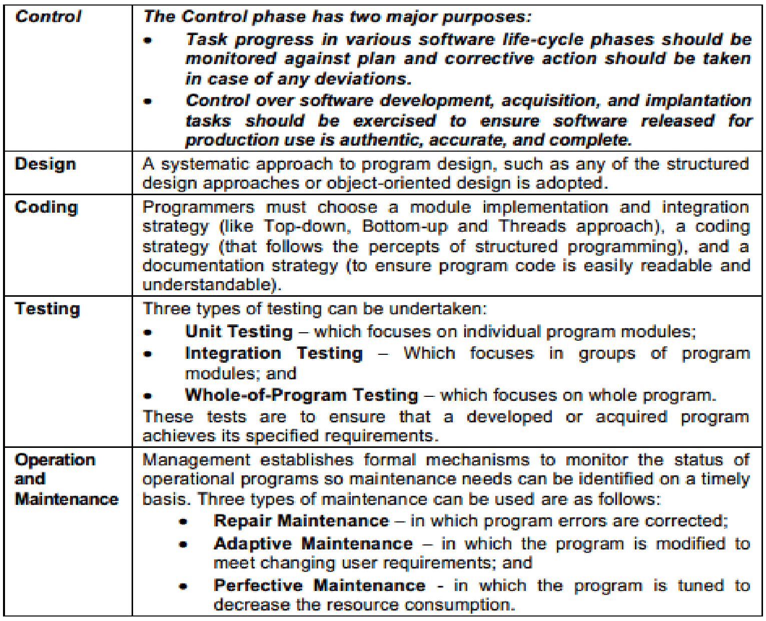
Management should make the estimates about the benefits & resource consumption.

PROGRAMMING MANAGEMENT CONTROL

Primary objective of this phase is to implement high quality programs. The purpose of control phase during the software development or acquisition is to monitor process:



Phase	Controls
Planning	Techniques like Work Breakdown Structures (WBS), Gantt charts and PERT (Program Evaluation and Review Technique) Charts can be used to monitor progress against plan.



Control	***The Control phase has two major purposes:*** • ***Task progress in various software life-cycle phases should be monitored against plan and corrective action should be taken in case of any deviations.*** • ***Control over software development, acquisition, and implantation tasks should be exercised to ensure software released for production use is authentic, accurate, and complete.***
Design	A systematic approach to program design, such as any of the structured design approaches or object-oriented design is adopted.
Coding	Programmers must choose a module implementation and integration strategy (like Top-down, Bottom-up and Threads approach), a coding strategy (that follows the percepts of structured programming), and a documentation strategy (to ensure program code is easily readable and understandable).
Testing	Three types of testing can be undertaken: • **Unit Testing** – which focuses on individual program modules; • **Integration Testing** – Which focuses in groups of program modules; and • **Whole-of-Program Testing** – which focuses on whole program. These tests are to ensure that a developed or acquired program achieves its specified requirements.
Operation and Maintenance	Management establishes formal mechanisms to monitor the status of operational programs so maintenance needs can be identified on a timely basis. Three types of maintenance can be used are as follows: • **Repair Maintenance** – in which program errors are corrected; • **Adaptive Maintenance** – in which the program is modified to meet changing user requirements; and • **Perfective Maintenance** - in which the program is tuned to decrease the resource consumption.

DATA RESOURCE MANAGEMENT CONTROL

The control activities involved in maintaining the integrity of the database is as under:

(a) Definition Controls:

These controls ensure that database always correspond & comply with the set standards.

(b) Existence/backup Controls:

These controls ensure existence of the database by establishing **backup and recovery** procedures. Back up means making copies of the data so that additional copies can be used to restore the original data. Various back up strategies are as follow:

-- **Dual recording:** 2 complete copies of database are maintained.
-- **Periodic dumping of Data:** Periodic backup of all or part database onto some storage device.
-- **Logging input Transactions:** Involves logging input data transaction.
-- **Logging changes to the data:** Involves copy of data each time it is changed by update action.

(c) Access Controls:

These controls are designed to ensure prevention of **unauthorized access from viewing retrieving the** organizational data.

(d) Update Controls:

These controls restrict the update of database to authorized users in 2 ways:
-- By permitting only addition of the data to the database.
-- Allowing users to change or delete the existing data.

(e) Concurrency Controls:

These controls provide solutions to overcome the data integrity problems.

(f) Quality Controls:

These controls ensure the accuracy, completeness and consistency of the fata maintained in the database.

QUALITY ASSURANCE MANAGEMENT CONTROL

Quality assurance management is concerned assuring that:

-- Information provided by the information system is as per goals.
-- Development, implementation & maintenance of information system as per standards.

Now, we will read the **why the quality assurance is needed** in an organization:

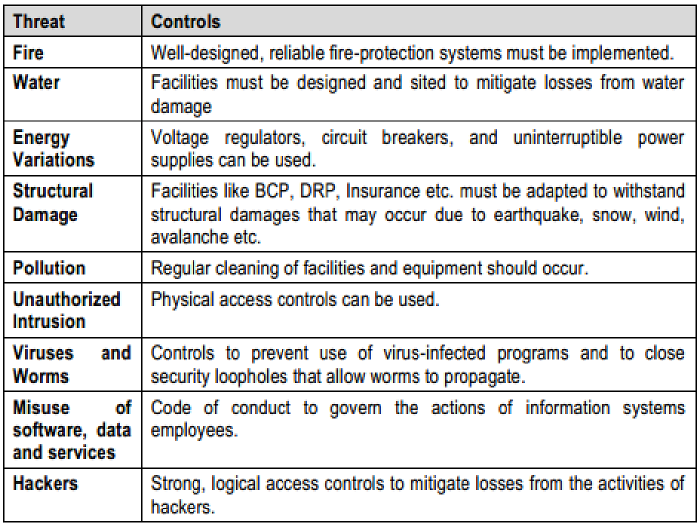
(1) Organizations are undertaking more ambitious projects as such quality is more important.
(2) If an entity has good quality, it will be able to provide good quality of services & goods to customers.
(3) All users who are deploying the software are concerned with its quality.

SECURITY MANAGEMENT CONTROLS

These controls ensure that information system assets are being protected and secured from any unauthorized intrusion. Various security measures are undertaken by the entity in order to ensure their data remains protected from possible threats.

Threat Identification:

A threat is some event that will lead to lose. During the threat identification, security administrator would like to flesh all material threats. Following are the possible threats and counter measure:



Threat	Controls
Fire	Well-designed, reliable fire-protection systems must be implemented.
Water	Facilities must be designed and sited to mitigate losses from water damage
Energy Variations	Voltage regulators, circuit breakers, and uninterruptible power supplies can be used.
Structural Damage	Facilities like BCP, DRP, Insurance etc. must be adapted to withstand structural damages that may occur due to earthquake, snow, wind, avalanche etc.
Pollution	Regular cleaning of facilities and equipment should occur.
Unauthorized Intrusion	Physical access controls can be used.
Viruses and Worms	Controls to prevent use of virus-infected programs and to close security loopholes that allow worms to propagate.
Misuse of software, data and services	Code of conduct to govern the actions of information systems employees.
Hackers	Strong, logical access controls to mitigate losses from the activities of hackers.

However, it may be possible that despite of so much counter measures threat occurs and leads to unrepairable damages to the information system.

As such, it is imperative to develop programs like **disaster recovery Plan** and **Insurance** can be the way to mitigate the damages caused by threats.

-- Disaster Recovery Plans

-- Insurance.

OPERATIONS MANAGEMENT CONTROLS

These controls ensure that hardware and software works smoothly in order to support daily functions. Some of the operational controls are as under:

Computer Operation:
Control over the computer operations that govern the activities that directly support the day-to-day execution. 3 types of controls are:

Operational Controls:
Prescribe the functions that either computer/human will perform.

Scheduling Controls:
These controls prescribe how the job to be scheduled.

Maintenance Controls:
These controls prescribes how hardware to be maintained in good working condition.

Network Operation:
Include proper functioning of network operation and monitoring performance of the network. Data may be lost due to the component failure.

Data Preparation & Entry:
Input components should be designed to promote speed and accuracy and to maintain the well-being of keyboard operator.

Production Control:
Include control of dispatch of output, job scheduling, and management of service-level agreements with the users.

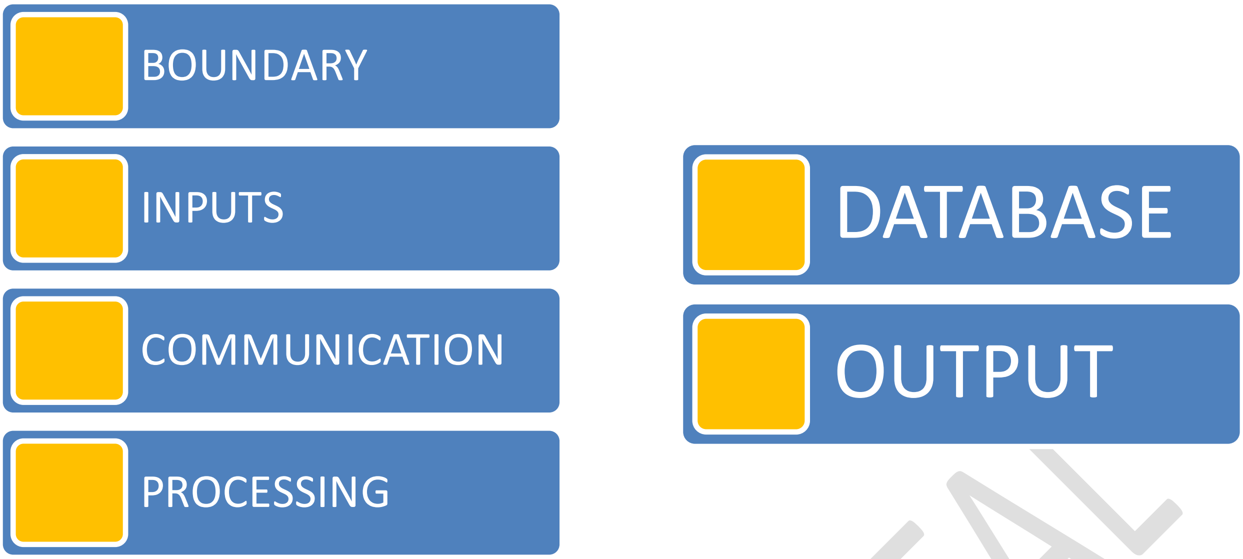
File Library:
Include management of machine-readable storage devices.

Documentation & Program Library:
Ensure that documents are stored safely. It means only authorised person are able to access the records. They will be liable to update the information as and when required. The documentation includes reporting of responsibility and authority of each function.

Help desk/Support:
This assists end-user to employ end-user hardware & software and provide technical support for production systems by assisting with problem resolution.

3. APPLICATION CONTROLS AND THEIR CATEGORIES

Type of control	Objective
APPLICATION CONTROLS	Includes programmatic routines within the application program code. It ensures that data remains complete, accurate and valid during its input, update and storage.



BOUNDARY

INPUTS

COMMUNICATION

PROCESSING

DATABASE

OUTPUT

CONTROLS	SCOPE
BOUNDARY CONTROLS	□ Establishes interface between the user of the system and the system itself. □ The system must ensure that it has an authentic user. □ Users allowed using resource`s in restricted ways.
INPUT CONTROLS	□ Responsible for the data and instructions in to the information system. □ Input Controls are validation and error detection of data input into the system.
COMMUNICATION CONTROLS	□ These controls discusses exposures in the communication systems, control over physical components, communication error lines, flows and links, topographic controls etc.
PROCESSING CONTROLS	□ Responsible for computing, sorting, classifying and summarizing data.
OUTPUT CONTROLS	□ To provide functions that determine the data content available to users, data format, timeliness of data and how data is prepare and routed to users.
DATABASE CONTROLS	□ Responsible to provide functions to define, create, modify, delete and read data in an information system. □ It maintains procedural data-set of rules to perform operations on the data to help a manager to take decisions.

Now explaining each of the controls in detail:

BOUNDARY CONTROLS

-- Major controls of boundary system are **access control mechanism.**

-- The access control **mechanism** involves **3 steps:**

-- Identification

-- Authentication

-- Authorisation

-- User can provide **3 classes of input** information for authentication process & gain access control to his required resources.

Class of information	Types of inputs
Personal Information	Name, birth, account number, PIN
Personal Characteristic	Fingerprint, hand size, signature
Personal Objects	Identification cards, key, badge

CYRPTOGRAPHY

-- Deals with the **programs** for **transforming DATA into CODES.**
-- CYRPTOGRAPHIC TECHNIQUE:
Encrypts

a. **Data {Clear Text}** into **cryptograms {Cipher Text}**

b. **Factors:** Time & cost involved in **DECIPHER** the cipher text by **CRYPT-ANLAYST.**

PASSWORD

-- Passwords **can be used as** BOUNDRAY ACCESS CONTROLS.
-- User can easily protect their information by using passwords.
-- Following things to be kept in mind: **frequent changes in password, minimum password length**

PERSONAL IDENTIFICATION NUMBER [PIN]

--Passwords **can also be used as** BOUNDRAY ACCESS CONTROLS.
--This number is provided to a user **by an institution based on USER CHARECTERISTICS.**
--However PIN is exposed to certain vulnerabilities while **issuance, delivery, transmission, storage** etc.

IDENTIFICATION CARDS

-- Identification cards are **used to store information** required in an authentication process.

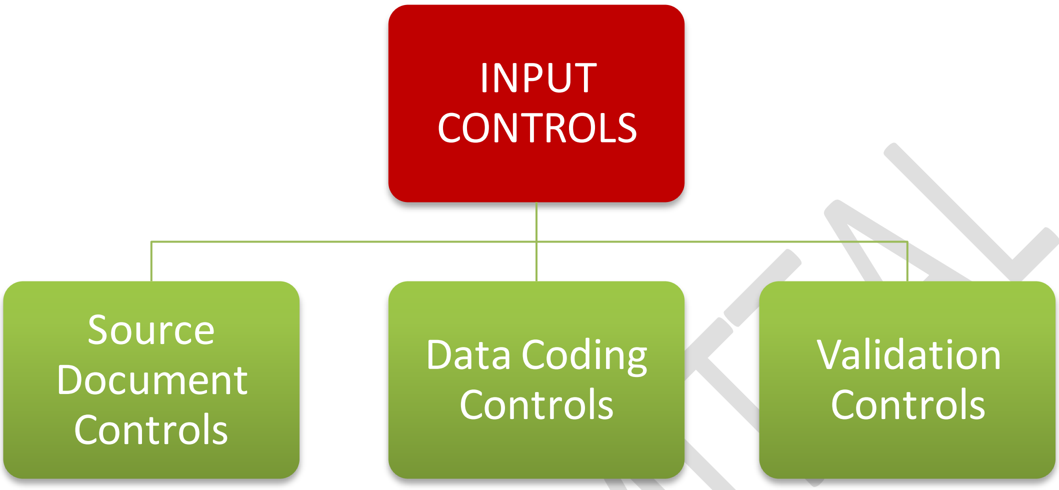
INPUT CONTROLS

Inputs controls are responsible for **ensuring & completeness of the data & instructions** input into an **application system.** Controls are being implemented on **input** since **human intervention** is required involving **considerable time, as such prone to error & frauds.** Data codes are used to **give unique identity.** Auditor must verify **the quality of coding system** & analysing the impact on **integrity & accurateness of data.**

Following are the broad classes of the inputs controls:

-- Source document Controls
-- Data Coding Controls
-- Validation Controls

Now explaining each control in detail:



Source Document Controls:

At place, where transaction is being initiated on the basis of physical source document there is need of careful control.

For example, **an individual who have access to purchase orders and receiving reports** may fabricate a fake purchase transaction. As a result, this fake transaction is being entered in to the system with all source documents as if it is a genuine transaction.

In absence of any controls to detect such type of error, it is very much possible that this **fake entry** would result in financial loss to the company. This can be explained as below:

Purchase entry is entered from नकली source दस्तावेज़…. As such system ने creditor बना दिया.

And against this creditor भुगतान किया गया… That's why financial loss to the company

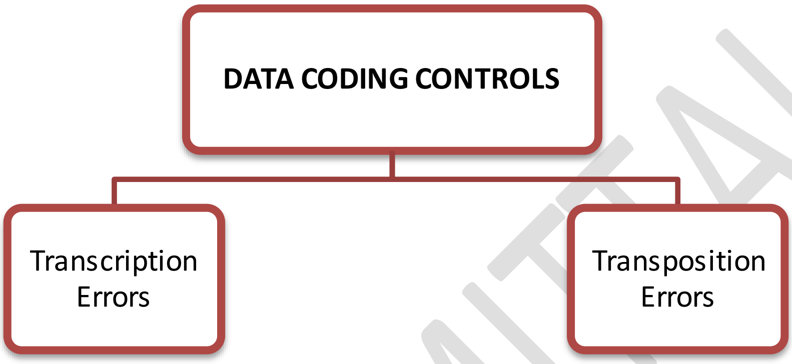
So in order to control such type of risks it is imperative to implement the control procedures over the source document. Some of the control procedures are:

USE PRE-PRINTED SOURCE DOCUMENTS **(Purchase bill पर pre-printed number होना चाहिए)**	Source documents must be pre-numbered from the printer with a unique serial number on each such document. Such practice enables accurate accounting and provide easy audit trail.
USE SOURCE DOCUMENT IN SEQUENCE **(Purchase bill sequence vice issue होना चाहिए)**	Source document should be distributed in number and used in sequence. When the source documents are not in use, then it must be kept in the lockers and access of which must be limited and to authorized person(s) only.

PERIODICALLY AUDIT SOURCE DOCUMENT **(Timely audit होनी चाहिए of missing documents)**	Missing documents should be identified by way reconciliation of the sequence numbers. **All documents = Used + In inventory + Voided** Any missing document must be reported to the management.

Data Coding Controls:

There are errors which may corrupt a data coda and as a consequence cause processing errors. Following are 2 types of errors;



TRANSCRIPTION ERRORS

- Addition errors: e.g., inventory item number 83276 recorded as 832766
- Truncation errors: e.g., the inventory item above recorded as 8327
- Substitution errors: e.g., the inventory item above recorded as 83266

TRANSPOSITION ERRORS

- Single transposition errors: occur when two adjacent digits are reversed. For example, 12345 is recorded as 21345.
- Multiple transposition errors: occur when nonadjacent digits are transposed. For example, 83276 is recorded as 87236.

Batch Controls:

Batching is the process of grouping together transactions that have some type of relationship to each other. 2 types of batch occur:

(a) Physical control :

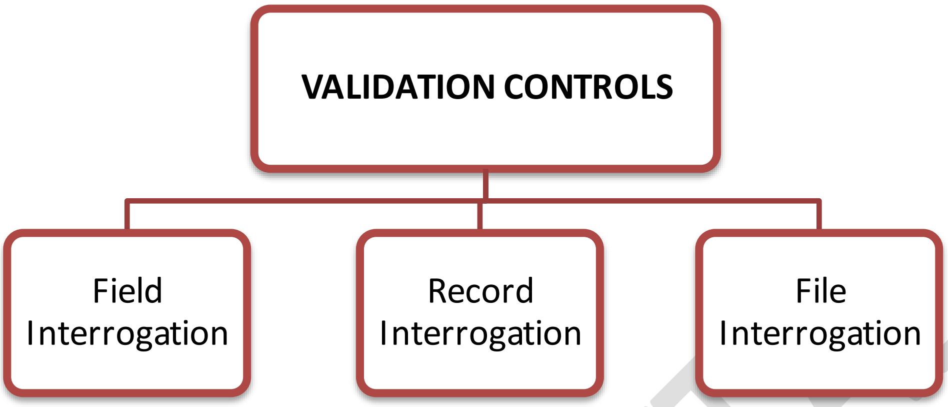
These controls are group of transactions that constitute a physical unit. E.g. source document can be obtained via mail, assembled into batch and tied together and then given to a data-entry clerk to be entered into application system at a terminal.

(b) Logical control:

Group of transactions bound together on some logical reasoning.

Validation Controls:

These controls are being implemented to detect errors in the **transaction data** before the data are processed. Following are the 3 levels of input validation:



FIELD INTERROGATION

It involves programmed decisions that **examine characters** of the data in the field. Following are different field interrogation:

CODE TO REMEMBER: C^{3}- L.A.P

1. **Cross Check:**
   -- To verify fields appearing in different files to see that the result tally.

2. **Check Digits:**
   -- Method to detect data coding errors in a check digit. It is digit **added to code when it is originally assigned** that allows the integrity of code during subsequent processing. It can be located at any place i.e. as a suffix, prefix, in middle etc.

3. **Code Checks:**
   -- Checks are made against pre-determined transaction codes to ensure input data are valid.

4. **Limit Checks :**
   -- This check ensures data processing accuracy and applied to both input & output data.
   -- The field is checked against **predefined** limits to ensure **no input/output error.**

5. **Arithmetic Check :**
   -- Emergency procedures, evacuation plans and making of fire exits. There should be half-yearly fire drill to test the preparedness.

6. **Picture Check :**
   -- This check is against entry into processing of **incorrect or invalid characters.**

RECORD INTERROGATION

1. **Reasonableness Check:**
   -- To verify whether value specified in the field is **reasonable** for that particular field?

2. **Valid Sign:**
   -- The contents of one field may determine which sign is valid for a **numeric field.**

3. **Sequence Checks:**
   -- If physical records follow a **required order** matching with **logical records**.

FILE INTERROGATION

CODE TO REMEMBER: V- P.U.L.S.E.

1. **Version Usage:**
   -- Proper version of a file should be used for data processing. It should be ensured that only most current file is processed.

2. **Parity Check:**
   -- These check is required when program or data are transmitted. These transmission errors are controlled primarily by detecting **errors or correcting codes.**

3. **Updation and maintenance authorization:**
   -- Sufficient controls should exist for file up-dation and maintenance to ensure that stored data is protected.

4. **Labeling:**
   -- It is important to label the files loaded for the process. Where there is manual process for loading files, **external labeling** is important to ensure that correct file is processed.

5. **Security of data files:**
   -- Unauthorized access to be prevented to maintain **confidentiality, integrity & availability** of data.

6. **Entry imaging and Logging:**
   -- System must provide reporting of before & after images of transactions. These images are then combined with **logging of events** to re-construct the data files to its last state of integrity.

COMMUNICATION CONTROLS

Inputs controls are responsible for **ensuring & completeness of the data & instructions** input into an **application system.** Controls are being implemented to ensure that none of the below exposure/risk occurs in communication sub-system:

(a) Transmission impairment
(b) Data loss due to component failure.
(c) A hostile party seek to subvert data that is transmitted through sub-system.

PHYSICAL COMPONENT CONTROLS

These controls incorporate features that mitigate the possible effect of the exposure. Following are the physical components affecting reliability of communication sub-system:

Transmission Media	It is physical path along which a signal can be transmitted between a sender and receiver.
Communication Lines	The reliability of data transmission can be improved by choosing a private communication.
Modem	Increase the speed with which data can be transmitted over communication lines.
Port Protection Devices	Used to mitigate exposures Associated with dial-up access to a computer system. The port-protection devices performs various security functions to authenticate users.
Multiplexes and concentrators	This allows the band width or capacity of a communication lines to be used more effectively.

LINE ERROR CONTROLS

It normally happens that data being sent is not received due to attenuation distortion, or noise that occurs on the line. These errors must be detected and corrected.

FLOW CONTROLS

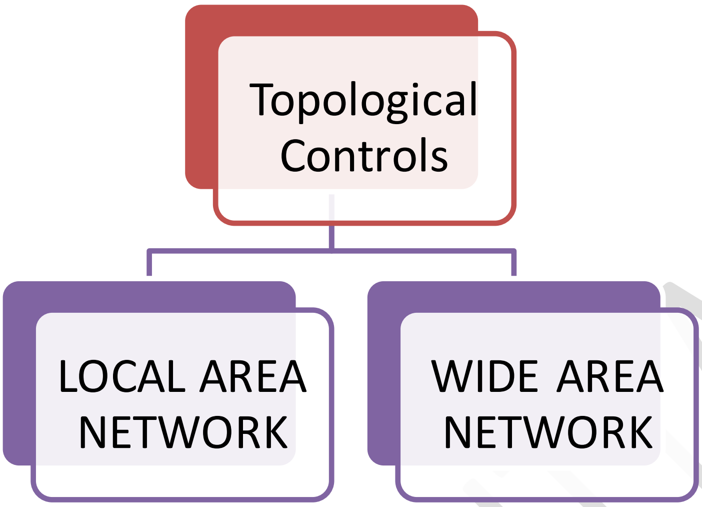
This control is needed because 2 nodes in the network can differ in terms of rate at which they can be send, received and process data.

LINK CONTROLS

In WANs, line error control and flow controls are important functions in the component that manages link between 2 nodes in a network.

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 links between the nodes.



LOCAL AREA NETWORK:
The following are 3 characteristics->

1. They are privately owned networks.
2. They provide high speed communication between the nodes.
3. Confined to limited geographic areas.

WIDE AREA NETWORK:
The following are 3 characteristics->

4. They encompass components that are owned by other parties.
5. Provide low speed communication between the nodes.
6. Covers large geographic areas.

CHANNEL ACCESS CONTROLS

1. Two different nodes in a network can complete to use a communication channel. Below are the two access control techniques that must be used:
   -- Polling. -- Contention Method.

INTERNETWORING CONTROLS

It is the process of connecting two or more communication net-works together to allow users to communicate with each other. Following are 3 types of devices that are used to connect sub-networks in an internet:

BRIDGE	Connects similar local area networks.
ROUTER	Performs all function of a bridge. It can connect heterogeneous locals are networks and direct network traffic over the fastest channel between two modes.
GATEWAY	Primary function is to perform protocol conversion to allow different types of communication.

CONTROL TECHNIQUES

ORGANISATIONAL CONTROL:

-- Enterprise control **concerned with DECISION MAKING** processes.

-- Companies with **large data processing facilities at SEPERATE LOCATION** & combining it as **A SINGLE BUSINESS UNIT** is difficult process.

-- **Organisational Control** technique includes **documentation of:**

-- Reporting responsibilities & authority of each function
-- Definition of responsibilities & objective of each function
-- Policies & Procedures
-- Job description
-- Segregation of duties

(i) **Responsibilities & objectives**:

a. Each IS function must be **clearly defined & documented.**

b. This includes **system software/development, application programming etc.**

c. Managers of each group is responsible for optimum utilisation of IS resources. These responsibilities includes:
-- Providing information to senior management on IS resources.
-- Planning for **expansion of IS resources.**
-- Controlling the **use of IS resources.**
-- Implementing activities & functions that support **accomplishment of the company's strategic plan.**

(ii) **Policies, standards, procedure & practices:**

a. These are **standards & instructions** that all **IS personnel** must follow **while performing their duties.**

b. Documented instructions **for filling out a standard changes request, justification of the cost of the changes** etc.

c. Documented policies should exist in **IS** for:
-- Use of IS resources.
-- Physical Security
-- Data Security
-- On-line security etc.

(iii) **Job description:**

a. These communicate management's specific expectation for job performance.

b. All jobs must have **a current, documented JOB DESCRIPTION** readily available to the employees.

c. Job description **establishes responsibilities & accountability** of the employee's actions.

(iv) **Segregation of duty:**

a. Common control technique **aimed at separating conflicting job duties.**

b. By such separation **work of one is checked** by the person.

MANAGEMENT CONTROL:

-- Controls adopted by the management of an enterprise **are to ensure that information system function correctly.**

-- Scope of control here includes **framing high level policies, procedures.**

-- The control shall include:

Responsibility: Senior management people responsible for IS within organisational structure.

Official IT structure: There should be prescribed organisational structure with all knowing their responsibilities.

IT steering committee: Comprise of user representative areas of the business & IT personnel.

FINANCIAL CONTROL TECHNIQUES:

CODE TO REMEMBER: A.B.C^{2}D.^{2} – S.N.O.R.

1. **A**uthorization:

   -- This entails **obtaining the AUTHORITY** to perform some act.

2. **B**udget:

   -- This shows **THE AMOUNT OF TIME/MONEY** expected to be **SPENT** during a period.

   -- The budget has to be **COMPARED** with the actual performance to ascertain **deviation.**

3. **C**ancellation of documents:

   -- This makes a documents **NOT READY FOR REUSE.`**

   -- Example: **Marks of "PAID OR OROCESSED"** on the invoices.

4. **C**ontrol (DUAL):

   -- This entails having **2 people** simultaneously access **ASSETS.**

   -- Example: **ATM** machines are emptied/filled with money **in presence of 2 people.**

5. **D**ocumentation:

   -- This includes **WRITTEN OR TYPED** explanation of actions taken on **SPECIFIC TRANSACTIONS.**

6. Duties segregation:

   -- This entails **assigning SIMIALR FUNCTIONS** to separate people to provide reasonable **ASSURANCE** against **FRAUD.**

7. Safekeeping:

   -- This entails **PHYSICALLY ASSETS,** such as **computer disks, desk drawer, file cabinet storeroom etc.-**

8. Numbering documents:

   -- These are **working documents** with the **PRE-PRINTED** sequential numbers, **which helps in detection of MISSING DOCUMENTS.**

9. Output/input verification:

   -- This entails comparing **INFORMATION** provided by a **COMPUTER SYSTEM** to input documents.

10. Review:

    -- This refers to **REVIEW OF SEPCIFIC WORK BY A SUPERVISOR.**

    -- It requires a **MARK ON THE DOCUMENTS** depicting that supervisor has handled the documents at least once.

I am briefing other controls which are as follows:

DATA PROCESSING ENVIRONMENT CONTROLS:

-- These controls are **hardware & software** related.

PHYSICAL ACCESS CONTROL:

-- These controls are personnel; hardware & software related.

LOGICAL ACCESS CONTROL:

-- These controls are **software related** & includes procedures exercised in IS software.

SDLC CONTROLS:

-- Controls in SDLC involves **specifying activities that should occur in each system of SDLC**

BUSINESS CONTINUITY PLAN CONTROLS:

-- These controls relate to have an **OPERATIONAL & TESTED IT** continuity plan.

-- These controls includes: **alternative procedures, backup, recovery plans etc.**

APPLICATION CONTROL TECHNIQUES:

-- These include **programmatic routines within the APPLICATION PROGRAM CODE.**

4. USER CONTROLS:

Application system controls are undertaken to accomplish reliable information processing cycles that perform process across the entity. Following are the controls that are to be exercised for system efficiency and effectiveness:

PROCESSING CONTROLS

Data processing control **perform validation check** to identify errors during **processing of data.** It ensures **completeness & accuracy** of the data being processed. Processing controls are enforced **through database management system.**

(i) Processor Control:
Processer has 3 components: Control Unit, ALU and Registers.

(ii) Real Memory Control:
This comprises the fixed amount of primary storage in which program/data to be stored. It protects areas of memory assigned to a program from illegal access by another program.

(iii) Virtual Memory Control:
When addressable memory is larger than the available real memory space, virtual memory is used.

ACCESS CONTROL MECHANISM:

-- It is associated with **identified, authorised** users & the resources they are allowed to access.
-- The **mechanism** processes **user request in 3steps:**
-- Identification
-- Authentication
-- Authorisation

AUTHORISATION:

-- There are 2 approaches to implement the authorisation module:

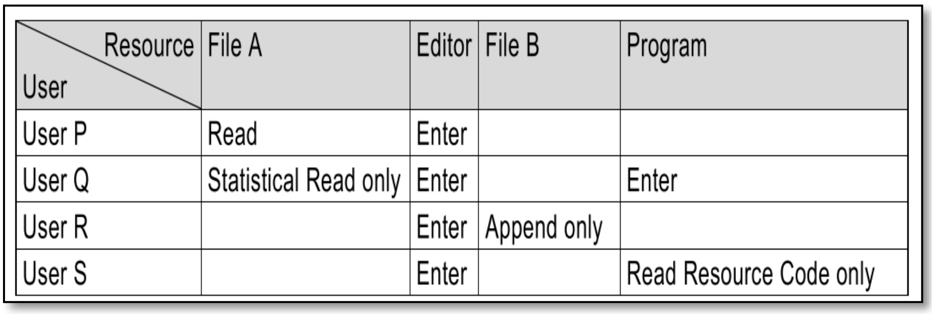
TICKET ORIENTED APPROACH

In this approach, **access control mechanism** assigns

USERS

Users are assigned **a TICKET** for each resources & element represents the **user privilege on the resources**

LIST ORIENTED APPROACH



Resource / User	File A	Editor	File B	Program
User P	Read	Enter		
User Q	Statistical Read only	Enter		Enter
User R		Enter	Append only	
User S		Enter		Read Resource Code only

DATA PROCESSING CONTROLS

These perform validation checks to identify the errors during the processing of the data Various processing controls are as follow:

1. Print Run-to-Run control totals:
-- Run-to –run control helps in **identi**fying errors or irregularities.

2. Edit Checks:

-- It is similar to data validation controls that can also be used at the time of processing data.

3. Exception reports:

--These reports are generated to identify the errors in the data processed.

--These type of reports provide reason for non-completion of transactions.

4. Reasonable Verification:

-- 2 or more field can be compared & cross verified to ensure their correctness.

-- **E.g.:** Statutory %age of provident fund can be calculated on gross pay to verify calculation.

DATABASE CONTROLS

Protecting the **integrity of a database,** when application software act as an **interface** between **the users & database** are called:

Following are the **UPDATE CONTROL:**

CODE TO REMEMBER: P.M. - C.P.
Prime Minister in Connaught Place

1. Processing of records:

While processing TRANSACTION file records mapped to respective MASTER FILES, end-of-file of transaction files with respect to end-of-file master file **IS TO ENSURED.** It simply means that all files are processed.

2. Maintain a suspense Account:

When there is mismatch between the MASTER RECORD & TRANSACTION RECORDS due to **failure in the corresponding RECORD ENTRY,** then these **transactions** are **MAINTAINED** in a suspense account.

3. Checking of transactions & master files:

-- To maintain integrity, insertion or deletion **of records in the master file, as such** there must be synchronization of processing between master and transaction files.

4. Process multiple transactions for single record:

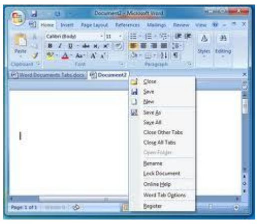
-- Multiple transactions can **occur based on SINGLE MASTER RECORD issues**

-- For instance, **DISPATCH REPORT** of product to **VARIOUS CENTRES.**

OUTPUT CONTROLS

Output controls ensure that the data delivered to users will be presented, formatted and delivered in a consistent and secured manner. Output can be in any form:

PRINTED DATA REPORT



WORD DOCUMENT

FLOPPY DISK OR CD-ROM

5. INFORMATION TECHNOLOGY GENERAL CONTROLS:

These are basic policies and procedures that ensure that an organisation's information systems are properly safeguarded. IT general controls are the foundation for overall IT control environment as they provide assurance that systems operate as desired.

Following are the example of primary objectives for general control:

(a) Safeguard Data.
(b) Protect application program.
(c) Ensure continued Computer Operations in case of unwanted environment.

Following are the common ITGCs are as follow:

(a) Logical access control over infrastructure.
(b) System development life cycle.
(c) Program change management Controls.
(d) System and data backup and recovery controls.

6. CONTROL OVER DATA INTEGRITY & SECURITY

Classification of information has been already mentioned in chapter-5. I am hereby just giving a glimpse of the names:

- **Top secret**
- **Highly confidential**
- **Proprietary**
- **Internal use**
- **Public documents.**

DATA INTEGRITY

Data integrity control techniques **aim to PREVENT, DETECT & CORRECT ERRORS** in transactions as they flow through **various stages of data processing program. Analysing d**ata integrity involves evaluating the critical procedures:

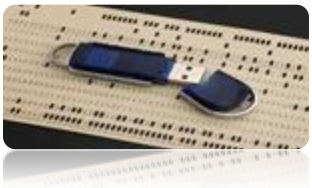
1.VIRUS detection & elimination.
2.Data integrity controls ensures that information has not been altered.

DATA INTEGRITY

Reflects **accuracy, correctness, validity & currency of the data.**

There are 6 categories of data integrity controls:

Control category	Threats/ risks	Controls
Source data control 	-- Invalid Data -- Incomplete data input	**D-VAN** -- Forms **D**esign. -- Check digit **V**erification -- **A**uthorisation Review -- Sequentially **N**umbered document
Input validation routines 	--Invalid or inaccurate data in computer – processed transaction files	-- Identifying the errors & correcting them. -- Such checking on timely basis. -- Prepare SUMMARY ERROR REPORT.

 On-line data entry controls	--Invalid or inaccurate transaction input entered through ONLINE terminals	-- User ID's & passwords -- Compatibility tests -- Transaction Log maintained by the system
 Data processing & storage controls	--Incomplete or inaccurate data in computer – processed master files	--Policies & procedures in respect of D-aus -- Data security -- Audit Trails -- Use of file labels -- Storage personnel
Output control	-- Incomplete/ inaccurate computer output	--Procedures to ensure: -- That system outputs conform to business's integrity. -- Proper distribution of the output. -- Protection of confidential information.
Data transmission control	-- Unauthorised access to data transmitted	--Monitor network to: ❖ Detect week points. ❖ Backup components. ❖ Multiple communication paths between networks

DATA INTEGRITY POLICIES

CODE TO REMEMBER: **V.D. - B.O.S.E.**

Major data integrity policies are given as under:

1. **VIRUS SIGNATURE SOFTWARE:**
   -- It must be updated immediately,
   -- When they are available from the vendor.

2. **DISASTER RECOVERY:**
   -- Comprehensive **disaster recovery plan** must be,
   -- Used to ensure **continuity of business.**

3. **BACKUP:**
   -- Quarter or year-end backup must be done separately,
   -- From the normal schedule for **accounting purpose.**

4. **OFFSITE BACKUP:**
   -- Backup Older than **1 month** must be sent **offsite** for permanent storage.

5. **SOFTWARE TESTING:**
   -- All software must be tested in a,
   -- **Suitable environment** before **installation** on production system.

6. **ENVIRONMENT DIVISION:**
   -- Division of **environment into development, test & production** is required for critical systems.

DATA SECURITY

Data security encompasses protection of data against accidental or intentional disclosure to unauthorized persons as well as the prevention of unauthorized modification and deletion of the data. Multiple levels of data security are necessary in an information system environment. They include:
-- Database protection,
-- Data integrity,
-- Security of the hardware and software controls,
-- Physical security over the user
-- Organizational policies.
An IS auditor is responsible to evaluate the following while reviewing the adequacy of data security controls:

-- Who is responsible for the accuracy of the data?
-- Who is permitted to update data?
-- Who is permitted to read and use the data?
-- Who controls the security of the data?
-- Who is responsible for determining who can read and update the data?

7. FINANCIAL ACCESS CONTROLS:

These controls are generally defined as procedure exercised by the system user over the sources, transactions origin. There are various financial control techniques, some of the, are explained below:

(a) Authorisation:
-- This means obtaining the authority to perform some act.
-- Accessing to such assets as accounting or application entries.

(b) Budgets:
-- These estimates the amount of time or money expected to spent during a particular period.
-- Budgets thereafter must be compared with the actual performance.

(c) Input/output Verification:

-- This encompasses comparing the result provided by the system with the input document.

-- It is an expensive control that tends to be over-recommended by auditors.

(d) Safekeeping:

-- It means physical securing assets under lock, key, in desk drawer, vault etc.

8. CYBER FRAUD:

With the advancement in the technology, cyber frauds are increasing day-by-day. One of the major reasons behind the rise of such frauds:

-- Failure of internal control system.

-- Failure of the organisation to be ready for new set of risks.

-- Smart fraudsters get the way in penetrating the internal system of the organisation.

"Means any type of deliberate deception for unfair or unlawful gain that occurs online"

On the basis of functionality, cyber frauds are of two types:

PURE CYBER FRAUD: This fraud exists only in cyber world. For example **website hacking.**

CYBER ENABLED FRAUD: These frauds can be committed in physical world but with the help of the technology. For example **withdrawal of money from ATM by stealing PIN.**

CYBER ATTACKS

Following are the cyber-attacks:

1. **PHISHING:**
   Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication.

2. **NETWORK SCANNING:**
   Network scanning is a procedure for identifying active hosts on a network, either for the purpose of attacking them or for network security assessment.

3. **VIRUS/MALICIOUS CODE:**
   Computer virus means any computer instruction, information, data or program **that destroys, damage, degrades & adversely affect performance of computer** or which attach itself with other computer resources & operates when a program is executed.

4. **SPAM:**
   E-mailing the same message to everyone on one or more Usenet group is termed as SPAM.

5. **WEBSITE COMPROMISE:**
   It includes website defacements. Hosting malware on websites in an unauthorised manner.

6. **OTHERS:**

Cracking:	Crackers are hackers with malicious intention.
Eavesdropping:	Refers to listening of private voice or data transmission using wiretap.
E-mail forgery:	Sending email message that looks as if it is sent by someone else.
E-mail threats:	Sending threatening message to try and get recipients to do something.
Scavenging:	This is gaining access to confidential information by searching all records.

IMPACT OF CYBER FRAUDS ON ENTERPRISES

1. FINANCIAL LOSES:

-- It covers **loss of electronic funds,**
-- Or increase in **expenditure towards repair of** damaged electronic components.

2. LEGAL REPERCUSSION:

-- An entity has to adhere to various **human rights** policies.
-- Organisation is **exposed to LAWSUITS** from investors in case of non-compliance of rules.
-- Auditor must take **legal view** before reviewing the issues related to it.

3. LOSS OF CREDIBILITY:

-- Credibility is the **ESSENCE** of any business to **maintain its competitive edge in market.**
-- This credibility will be shattered **resulting in loss to the business & prestige.**

4. DISCLOSURE OF INFORMATION:

-- This event involves **disclosure of sensitive, confidential** information.
-- Such practice can **spoil the REPUTATION** of the organisation.

5. SABOTAGE:

-- People, who are not interested in **financial gain,** also want to spoil the credibility of the organisation. This is due to reason of **DISLIKE** for the organisation.

TECHNIQUES TO COMMIT CYBER FRAUD

HACKING: It is an act of penetrating computer systems gain KNOWLEDGE about the system & how it works.

CRACKING: Crackers are hackers with malicious intentions, which means, unauthorised entry.

DATA DIDDLING: Data diddling involves **change of data** before **or** as they entered in system. **Limited** technical knowledge is required **to diddle data.**

DATA LEAKAGE: It refers to unauthorised copying of company data such as computer files.

DoS ATTACK: It refers to series of action that prevents access to software system by its authorised users, cause delay of its time critical operations.

INTERNET TERRORISM: Refers to using internet to disrupt electronic commerce & destroy organisations communication.

LOGIC TIME BOMB: These are the program that lies idle until some specified event triggers it. Once triggered it results in destruction of programs or data or both.

MASQUERADING/IMPERSONATION: Perpetrator gains access to system as an authorised user.

PASSWORD CRACKING: Intruder penetrates a system defense, steals file containing valid passwords, decrypts them and use them to access the system.

PIGGYBACKING: Refers to tapping into telecommunication line.

ROUND DOWN: Computer round down all interest calculation up to 2 decimal places. Fraction is placed in account controlled by the perpetrator.