CH-3 Protection of Information Systems

Need for Protection of Information Systems

Q. Risks have led to a gap between the need to protect systems and the degree of protection applied. This gap is caused by: (WIDE-UAE)

-**W**idespread use of technology
-**I**nterconnectivity of systems
-**D**evolution of management and control
-**E**limination of distance, time, and space as constraints
-**U**nevenness of technological changes
-**A**ttractiveness of conducting unconventional electronic attacks **over** more conventional physical attacks against organizations.
-**E**xternal factors such as legislative, legal, and regulatory requirements or technological developments.

Q. common aspect in each case is the critical information that each organization generates

Strategic Plans: Most of the organizations readily acknowledge that strategic plans are crucial to the success of a company.

But many of them fail to really make an effort to protect these plans.

In today's global environment, the search for competitive advantage has never been greater.

The advantages of achieving insight into a competitor's intentions can be substantial. Industry studies bear witness to this fact.

Business Operations: Business operations consist of an organization's process and procedures, most of which are deemed to be proprietary.

As such, they may provide a market advantage to the organization.

This is the case when one company can provide a service profitably at a lower price than the competitor.

A company's client lists and the prices charged for various products and services can also be damaging in the hands of a competitor.

Finances: Financial information, such as salaries and wages, are very sensitive and should not be made public.

While general salary ranges are known within industry, precise salary information can provide a competitive edge.

This information if available can help competitive enterprises to understand and re-configure their salary structure accordingly.

When competitors' costs are lower, they can either underprice the market or increase prices. In either case, the damage to an organization may be significant.

Information Security Policy

Q. Issues to address

This policy does not need to be extremely extensive, **but clearly state**

senior management's
commitment to information security,
be under change,
version control and

be signed by the appropriate senior manager.

The policy should at least address the following issues:

-definition of information security & all relevant information security responsibilities
-reasons why information security is important to the organization, and its goals and principles
-brief explanation of the security policies, principles, standards and compliance requirements
-reference to security policy manual.

Q. Members of Security Policy

3 groups of management:

Management members **who** have budget and policy authority,
Technical group **who** know what can and cannot be supported, and
Legal experts **who** know the legal ramifications of various policy charges.

Q. Information Security Policies and their Hierarchy

Information Security Policy - USP+AUP	Organization Security Policies OISP+NSSP+ICP	Conditions of Connection
User Security Policy – This policy sets out the responsibilities and requirements for all IT system users. It provides security terms of reference for Users, Line Managers and System Owners. **Acceptable Usage Policy –** This sets out the policy for acceptable use of email, Internet services and other IT resources.	**Organizational Information Security Policy:** This policy sets out the Group policy for the security of its information assets and the IT systems processing this information. Though it is positioned at the bottom of the hierarchy, it is the main IT security policy document. **Network & System Security Policy** – This policy sets out detailed policy for system and network security and applies to IT department users. **Information Classification Policy –** This policy sets out the policy for the classification of information.	This policy sets out the Group policy for connecting to the network. It applies to all organizations connecting to the Group, and relates to the conditions that apply to different suppliers' systems.

Q. Components of the Security Policy – IPS-TDP-IBM-SISIIL

- Incident response and reporting mechanism
- Purpose and Scope of the Document and the intended audience
- Security policy document maintenance and compliance requirements
- The Security Infrastructure
- Description of technologies and computing structure
- Physical and Environmental Security. (PES)
- Inventory and Classification of assets
- Business Continuity Planning(BCP)
- Monitoring and Auditing Requirements (MAR)
- System Development and Maintenance Controls (SDMC)
- IT Communications (IT-C)
- Security Organization Structure (SOS)
- IT Operations management
- Identity Management and access control
- Legal Compliances.

Q. Impact of Technology on Internal Controls (A-CS-PA-A-CD-I)

Authorization Procedures:

In **manual systems**, auditors evaluate the adequacy of procedures for authorization of examining the work of employees.	In **computer systems**, authorization procedures often are embedded within a computer program.

For example: In some on-line transaction systems, written evidence of individual data entry authorization, e.g. a supervisor's signature, may be replaced by computerized authorization controls such as automated controls written into the computer programs (e.g. programmed credit limit approvals).

Competent and Trustworthy Personnel:

Personnel should have proper skill and knowledge to discharge their duties.

Substantial power is often vested in the errors responsible for the CBIS
maintained
operated,
developed, and
implemented, within organizations.

Unfortunately, ensuring that an organization has competent and trustworthy information systems personnel is a difficult task.

Segregation of Duties:

Segregation of duties refers to the concept of distribution of work responsibilities such that individual employees are performing only the duties stipulated for their respective jobs and positions.

The main purpose is to prevent or detect errors or irregularities by applying suitable controls.

The irregularities are frauds due to various facts like

Theft of assets like funds, IT equipment, the data and programs;
Modification of the data leading to misstated and inaccurate financial statements; and
Modification of programs in order to carry out irregularities like rounding down, salami etc.

From a **functional perspective**, segregation of duties should be maintained between the

Information systems use;
Data entry;
Computer operation;
Network management;
System administration;
Systems development and maintenance;
Change management;
Security administration, and
Security audit.

Physical Control over Assets and Records:

Physical control over access and records is critical in both manual systems and computer systems.

In the manual systems, protection from unauthorised access was through the use of locked doors and filing cabinets.

A client's financial data and computer programs can all be maintained at a single site – namely the site where the computer is located.

This concentration of information systems assets and records also increases the losses that can arise from computer abuse or a disaster.

The nature and types of control available have changed to address these new risks.

Adequate Documents and Records:

This includes written or typed explanations of actions taken on specific transactions;

it also refers to written or typed instructions, which explain the performance of tasks.

In a manual system, adequate documents and records are needed to provide an audit trail of activities within the system.	In computer systems, documents might not be used to support the initiation, execution, and recording of some transactions.

Thus, no visible audit or management trail would be available to trance the transactions in a computerized system.

Adequate Management Supervision:

This refers to review of specific work by a supervisor but this control requires a sign-off on the documents by the supervisor, in order to provide evidence that the supervisor at least handled them.

This is an extremely difficult control to test after the fact because the auditor cannot judge the quality of the review unless he or she witnesses it, and, even then, the auditor cannot attest to what the supervisor did when the auditor was not watching.

In a manual system, management supervision of employee activities is relatively straightforward as the managers and the employees are often at the same physical location.	In computer system, however, data communication facilities can be used to enable employees to be closer to the customers they service.

The Management's supervision and review helps to deter and detect both errors and fraud.

Comparing Recorded Accountability with Assets:

Data and the assets that the data purports to represent should periodically be compared to determine whether incompleteness or inaccuracies in the data exist or whether shortages or excesses in the assets have occurred.

In a manual system, independent staff prepares the basic data used for comparison purposes.	In a computer system, however, software is used to prepare this data. Again, internal controls must be implemented to ensure the veracity of program code, because traditional separation of duties no longer applies to the data being prepared for comparison purposes.

Delegation of Authority and Responsibility:

A clear line of authority and responsibility is an essential control in both manual and computer systems.

In a computer system, however, delegating authority and responsibility in an unambiguous way might be difficult because some resources are shared among multiple users.

Further, more users are developing, modifying, operating, and maintaining their own application systems instead of having this work performed by IS professionals.

Independent Checks on Performance:

In manual systems, independent checks are carried out because employees are likely to forget procedures, make genuine mistakes, become careless, or intentionally fail to follow prescribed procedures.	If the program code in a computer system is authorized, accurate, and complete, the system will always follow the designated procedures in the absence of some other type of failure like hardware or systems software failure.

Objective of Controls	Nature of IS Resource	Audit Functions
- Preventive Controls - Detective Controls - Corrective Controls - Compensatory Controls	**(A) Environmental** -Environmental Issues and Exposures -Controls for Environmental Exposures **(B) Physical Access** -Physical Access Issues and Exposures -Controls for Physical Access Exposures **(C) Logical Access** -Logical Access Paths -Logical Access Issues and Exposures -Issues and Revelations related to Logical Access -Logical Access Control across the System	**- Managerial** 1. Top Management and Information Systems Management Controls 2. Systems Development Management Controls 3. Programming Management Controls 4. Data Resource Management Controls 5. Quality Assurance Management Controls 6. Security Management Controls 7. Operations Management Controls **- Application** 1. Boundary Controls 2. Input Controls 3. Communication Controls 4. Processing Controls 5. Database Controls 6. Output Controls

Classification on the basis of Objective of Controls

Preventive Controls: Preventive Controls are those inputs, which are designed to prevent an error, omission or malicious act occurring.

An example of a preventive control is the use of passwords to gain access to a financial system.

The broad **characteristics** of preventive controls are as follows:

A clear-cut understanding about the vulnerabilities of the asset	Understanding probable threats	Provision of necessary controls for probable threats from materializing.

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.

The main **characteristics** of such controls are given as follows:

Clear understanding of lawful activities so that anything which deviates from these is reported as unlawful, malicious, etc.	An established mechanism to refer the reported unlawful activities to the appropriate person or group.	Interaction with the preventive control to prevent such acts from occurring	Surprise checks by supervisor

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.

The main **characteristics** of the corrective controls are:

-Minimizing the impact of the threat.
-Identifying the cause of the problem.
-Providing Remedy to the problems discovered by detective controls.
-Getting feedback from preventive and detective controls.
-Correcting error arising from a problem.
-Modifying the processing systems to minimize future occurrences of the incidents.

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."

Sometimes, while designing and implementing controls, organizations because of different constraints like financial, administrative or operational, may not be able to implement appropriate controls.

In such a scenario, there should be adequate compensatory measures, which may although not be as efficient as the appropriate control, but reduce the probability of loss to the assets.

Classification on the basis of "Nature of Information System Resources"

(A) Environmental Controls: These are the controls relating to IT environment such as power, air-conditioning, Un-interrupted Power Supply (UPS), smoke detection, fire- extinguishers, dehumidifiers etc.

This section deals with the **external factors** in the Information System and **preventive measures** to overcome these conflicts.

(i) Environmental Issues and Exposures: Environmental exposures are primarily due to elements of nature. However, with proper controls, exposures can be reduced.

Common occurrences are Fire, Natural calamities, Power spike, Air conditioning failure, Electrical shock, Equipment failure, Water damage/flooding-even with facilities located on upper floors of high buildings.

Water damage is a risk, usually from broken water pipes, and Bomb threat/attack.

From the perspective of environmental exposures and controls, Information systems resources may be categorized as follows (with the primarily focus on facilities): (HI-DSP)

Hardware and Media: This includes Computing Equipment, Communication equipment, and Storage Media.

Information Systems Supporting Infrastructure or Facilities: This typically includes Physical Premises like

Computer Rooms, Cabins, Server Rooms, Data Centre premises, Printer Rooms, Remote facilities;	Staging Room, and Storage Areas; Communication Closets; Cabling ducts; Power Source, and Heating, Ventilation and Air Conditioning (HVAC).

Documentation: Physical and geographical documentation of computing facilities with emergency excavation plans and incident planning procedures.

Supplies: The 3rd party maintenance procedures viz. air-conditioning, fire safety, and civil contractors whose entry and assess with respect to their scope of work assigned are to be monitored and logged.

People: employees, contract employees, visitors, supervisors and third party maintenance personnel are to be made responsible and accountable for environmental controls in their respective Information Processing Facility (IPF).

(B) Physical Access Controls

controls relating to physical security of the 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 software related and include procedures exercised on access to IT resources by employees/outsiders.

Controls for Physical Access Exposures

Physical access controls are designed to protect the organization from unauthorized access or in other words, to prevent illegal entry. The authorization given by the management should be explicit.

Some of the more common access control techniques are discussed categorically as follows:

(a) Locks on Doors	(b) Physical Identification medium	(c) Logging on Facilities	(d) Others
-Cipher Locks -Bolting door locks -Electronic door locks -Biometric door locks	-PIN -Plastic Cards - Identification Badges	-manual -electronic	

Cipher locks (Combination Door Locks) - Cipher locks are used in low security situations or when a large number of entrances and exits must be usable all the time.

To enter, a person presses a 4-digit number, and the door will unlock for a predetermined period of time, usually 10 to 30 seconds.

Bolting Door Locks – A special metal key is used to gain entry when the lock is a bolting door lock. To avoid illegal entry, the keys should be not being duplicated.

Electronic Door Locks – A magnetic or embedded chip-based plastics card key or token may be entered into a reader to gain access in these systems.

Advantages of electronic door locks

- Through the special internal code, cards can be made to identity the correct individual.

- Restrictions can be assigned to particular doors or to particular hours of the day.

- Degree of duplication is reduced.

- Card entry can be easily deactivated in the event an employee is terminated or a card is lost or stolen.

- An administrative process, which may deal with Issuing, accounting for and retrieving the card keys, are also parts of security.

Biometric Door Locks: These locks are extremely secure where an individual's unique body features, such as voice, retina, fingerprint or signature, activate these locks.

This system is used in instances when extremely sensitive facilities must be protected, such as in the military.

Personal Identification numbers (PIN): A secret number will be assigned to the individual, in conjunction with some means of identifying the individual, serves to verify the authenticity of the individual.

The visitor will be asked to log on by inserting a card in some device and then enter their PIN via a PIN keypad for authentication.

His entry will be matched with the PIN number available in the security database.

Plastic Cards: These cards are used for identification purposes. Customers should safeguard their card so that it does not fall into unauthorized hands.

Identification Badges-Special identification badges can be issued to personnel as well as visitors. For easy identification purposes, their colour of the badge can be changed.

Sophisticated photo IDs can also be utilized as electronic card keys.

Manual Logging: All visitors should be prompted to sign a visitor's log indicating their name, company represented, their purpose of visit, and person to see.

Logging may happen at both fronts - reception and entrance to the computer room.

A valid and acceptable identification such as a driver's license, business card or vendor identification tag may also be asked for before allowing entry inside the company.

Electronic Logging: This feature is a combination of electronic and biometric security systems.

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

Dead Man Doors: These systems encompass a pair of doors that are typically found in entries to facilities such as computer rooms and document stations. The first entry door must close and lock, for the second door to operate, with the only one person permitted in the holding area.

Non–exposure of Sensitive Facilities: There should be no explicit indication such as presence of windows of directional signs hinting the presence of facilities such as computer rooms. Only the general location of the information processing facility should be identifiable.

Controlled Single Entry Point: All incoming personnel can use controlled Single Entry Point. A controlled entry point is monitored by a receptionist. Multiple entry points increase the chances of unauthorized entry. Unnecessary or unused entry points should be eliminated or deadlocked.

Control of out of hours of employee-employees: Employees who are out of office for a longer duration during the office hours should be monitored carefully. Their movements must be noted and reported to the concerned officials frequently.

(C) Logical Access Controls

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.

(i) Logical Access Paths

(a) Online Terminals	(b) Dial-up ports	(c) Telecommunication Networks

(a) Online Terminals: To access an online terminal, a user has to provide a valid login-ID and password.

If additional authentication mechanisms are added along with the password, it will strengthen the security.

Operator Console – The operator console is one of the crucial places where any intruders can play havoc. Hence, access to operator console must be restricted.

This can be done by:

Keeping the operator console at a place, which is visible, to all?

By keeping the operator console in a protected room accessible to selected personnel.

(b) Dial-up Ports: Using a dial up port, user at one location can connect remotely to another computer present at an unknown location via a telecommunication media.

A modem is a device, which can convert the digital data transmitted to analog data (the one that the telecommunication device uses).

Thus, the modem can act as an interface between remote terminal and the telephone line.

Security is achieved by providing a means of identifying the remote user to determine authorization to access. A dial back line ensures security by confirming the presence and exactness of the data sent.

(c) Telecommunication Network: In a Telecommunication network, a number of computer terminals, Personal Computers etc. are linked to the host computer through network or telecommunication lines.

Whether the telecommunication lines could be private (i.e., dedicated to one user) or public, security is provided in the same manner as it is applied to online terminals.

(iii) Issues and Revelations related to Logical Access

Intentional or accidental exposures of logical access control encourage technical exposures, computer crimes and Asynchronous attacks. These are given as follows:

(a) Technical Exposures (7 in number)	(b) Computer Crime Exposures (7 in number)	(c) Asynchronous Attacks (5 in number)
1. Data Diddling	1. Financial Loss	1. Data Leakage
2. Bomb	2. Legal Repercussions	2. Subversive Threats
3. Trojan Horse	3. Loss of Credibility or Competitive Edge	- Invasive tap
4. Worm	4. Blackmail/Industrial Espionage	- Inductive tap
5. Rounding Down	5. Disclosure of Confidential Information	3. Wire-tapping
6. Salami Techniques	6. Sabotage	4. Piggybacking
7. Trap Doors	7. Spoofing	5. Denial of Service

Data Diddling: Data diddling involves the change of data before or after they are entered into the system.

A limited technical knowledge is required to data diddle and the worst part with this is that it occurs before computer security can protect the data.

Bomb: Bomb is a piece of bad code deliberately planted by an insider or supplier of a program.

An event, which is logical, triggers a bomb or time based.

The bombs explode when the conditions of explosion get fulfilled causing the damage immediately.

Since, these programs do not circulate by infecting other programs; chances of a widespread epidemic are relatively low.

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	May modify records in protected files	May allow illicit users to use the systems

Christmas Card is a well-known example of Trojan.

It was detected on internal E-mail of IBM system.

On typing the word 'Christmas', it will draw the Christmas tree as expected, but in addition, it will send copies of similar output to all other users connected to the network.

Because of this message on other terminals, other users cannot save their half finished work.

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: Existential Worm, Alarm clock Worm etc.

The **Alarm Clock worm** places wake-up calls on a list of users. It passes through the network to an outgoing terminal while the sole purpose of existential worm is to remain alive.	**Existential worm** does not cause damage to the system, but only copies itself to several places in a computer network.

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.

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, Rs. 21,23,456.39 becomes Rs.21,23,456.40, while in the Salami technique the transaction amount Rs.21,23,456.39 is truncated to either Rs.21,23,456.30 or Rs.21,23,456.00, depending on the logic.

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.

Financial Loss: Financial losses may be direct like loss of electronic funds or indirect like expenditure towards repair of damaged electronic components.

Legal Repercussions: An organization has to adhere to many laws while developing security policies and procedures.

These laws protect both the perpetrator and organization from trial.

The organizations will be exposed to lawsuits from investors and insurers if there have no proper security measures.

The IS auditor should take legal counsel while reviewing the issues associated with computer security.

Loss of Credibility or Competitive Edge: In order to maintain competitive edge, many companies, especially service firms such as banks and investment firms, needs credibility and public trust.

This credibility will be shattered resulting in loss of business and prestige if security violation occurs.

Blackmail/Industrial Espionage: By knowing the confidential information, the perpetrator can obtain money from the organization by threatening and exploiting the security violation.

Disclosure of Confidential, Sensitive or Embarrassing Information: These events can spoil the reputation of the organization.

Legal or regulatory actions against the company may be also a result of disclosure.

Sabotage: People, who may not be interested in financial gain but who want to spoil the credibility of the company or to will involve in such activities.

They do it because of their dislike towards the organization or for their intemperance.

Spoofing: A spoofing attack involves forging one's source address.

One machine is used to impersonate the other in spoofing technique.

Spoofing occurs only after a particular machine has been identified as vulnerable.

A penetrator makes the user think that he is interacting with the operating system.

For example, a penetrator duplicates the login procedure, captures the user's password, attempts for a system crash and makes the user login again.

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.

Subversive Threats: An intruder attempts to violate the integrity of some components in the sub-system.

Subversive attacks can provide intruders with important information about messages being transmitted and the intruder can manipulate these messages in many ways.

An intruder attempts to violate the integrity of some components in the sub-system by:

Invasive tap: By installing it on communication line, he may read and modify data.	**Inductive tap:** It monitors electromagnetic transmissions and allows the data to be read only.

Wire-tapping: This involves spying on information being transmitted over telecommunication network

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 he user and modifying them or substituting new messages.

A special terminal is tapped into the communication for this purpose.

Shutting Down of the Computer/Denial of Service: This is initiated through terminals or microcomputers that are directly or indirectly connected to the computer.

When a user establishes a connection on the Internet through TCP/IP, a **three-way** handshake takes place between

Synchronize (SYN) packets,
SYN ACK (Acknowledgement) packets and
ACK packets.

Computer hacker transmits hundreds of SYN packets to the receiver but never responds with an ACK to complete the connection.

As a result, the ports of the receiver's server are clogged with incomplete communication requests and legitimate requests are prevented from access.

This is known as Connection Flooding.

Remote and distributed data processing applications can be controlled in many ways. Some of these are given as follows:

- Remote access to computer and data files through the network should be implemented.

- Having a terminal lock can assure physical security to some extent.

- Applications that can be remotely accessed via modems and other devices should be controlled appropriately.

- Terminal and computer operations at remote locations should be monitored carefully and frequently for violations.

- In order to prevent the unauthorized user's access to the system, there should be proper control mechanisms over system documentation and manuals.

- Data transmission over remote locations should be controlled.

- The location which sends data should attach needed control information that helps the receiving location to verify the genuineness and integrity.

- When replicated copies of files exist at multiple locations it must be ensured that all are identical copies contain the same information and checks are also done to ensure that duplicate data does not exist.

Note: Logical Access Violators &
(iv) Logical Access Control across the System – both study from study material if time permits not so important.

Classification on the basis of "Audit Functions"

(A) Managerial Controls: In this part, we shall examine controls over the managerial controls that must be performed to ensure the development, implementation, operation and maintenance of information systems in a planned and controlled manner in an organization.

The controls at this level provide a stable infrastructure in which information systems can be built, operated, and maintained on a day-to-day basis.

1. Top Management and Information Systems Management Controls

The scope of control here includes framing high level IT policies, procedures and standards on a holistic view and in establishing a sound internal controls framework within the organization.

The controls flow from the top of an organization to down; the responsibility still lies with the senior management.

Top management is responsible for preparing a master plan for the information systems function.

The senior managers who take responsibility for IS function in an organization face many challenges.

The **major functions** that a senior manager must perform are as follows:

(a) Planning	(b) Organizing	(c) Leading	(d) Controlling
- Preparing the plan - Types of Plans - Role of a Steering Committee	- Resourcing the Information Systems Function - Staffing the Information Systems Function	- Motivating and Leading Information Systems Personnel - Communicating with IS Personnel	- Overall Control of IS function - Control of Information System Activities - Control over Information System Services

(a) Planning – This includes determining the goals of the information systems function and the means of achieving these goals.

Preparing the plan: This involves the following tasks:

1. Recognizing opportunities and problems that come face to face with the organization in which Information technology and Information systems can be applied cost effectively.

2. Identifying the resources needed to provide the required information technology and information systems. and

3. Formulating strategies and tactics for acquiring the needed resources.

Types of Plans:

Top management must prepare 2 types of information systems plans for the information systems function: A Strategic plan and an Operational plan.

Strategic Plan: The Strategic Plan is the long-run plan covering, say, the next 3 to 5 years of operations;	**Operation Plan:** It is the short-plan covering, say, next 1 to 3 years of operations.

Role of a Steering Committee: The steering committee shall comprise of representatives from all areas of the business, and IT personnel.

The committee would be responsible for the overall direction of IT.

The ultimate responsibility for information systems planning should be vested in an information systems steering committee.

The steering committee should assume overall responsibility for the activities of the information systems function.

Here the responsibility lies beyond just the accounting and financial systems.

(b) Organizing - There should be a prescribed IT organizational structure with documented roles and responsibilities and agreed job descriptions.

This includes gathering, allocating, and coordinating the resources needed to accomplish the goals that are established during Planning function.

Resourcing the Information Systems Function: A major responsibility of top management is to acquire the resources needed to accomplish the goals and objectives set out in the information systems plan.

These resources include hardware, software, personnel, finances and facilities.

Adequate funding should be provided to support the acquisition and development of resources when and where they are needed.

Further, Auditors should question whether top managers have a good understanding of the role the information systems function should play in their organization.

Staffing the Information Systems Function: Staffing the Information systems function involves 3 major activities –

Acquisition of information systems personnel,
Development of information systems personnel; and
Termination of information systems personnel.

(c) Leading – This includes motivating, guiding, and communicating with personnel.

The purpose of leading is to achieve the harmony of objectives; i.e. a person's or group's objectives must not conflict with the organization's objectives.

The process of leading requires managers to motivate subordinates, direct them and communicate with them.

Motivating and Leading Information Systems Personnel: Though many theories exist, however there is no one best way of motivating and guiding all people and thus the strategies for motivating/leading people need to change depending upon particular characteristics of an individual person and his/her environment.

Communicating with IS Personnel: Effective communications are also essential to promoting good relationships and a sense of trust among work colleagues.

For example - Due to failure in understanding the directions given by the top management, a serious error is made in the system design; the effect of which is for long-term.

(d) Controlling – This includes comparing actual performance with planned performance as a basis for taking any corrective actions that are needed.

This involves determining when the actual activities of the information system's functions deviate from the planned activities.

Overall Control of IS function: When top managers seek to exercise overall control of the information systems function, 2 questions arise:

How much the organization should be spending on the information systems function?	Is the organization getting value for the money from its information systems function?

Control of Information System Activities: Top managers should seek to control the activities on the basis of Policies and Procedures; where Policies provide broad, general guidelines for behavior whereas Standards provide specific guidelines for behavior.

New and existing staff must be made aware of the policies and procedures that govern their work.

Control over Information System Services: For each service level, estimates must be made of the expected benefits and resource consumption and finally the review committee must establish priorities.

2. Systems Development Management Controls

System development controls are targeted to ensure that proper documentations and authorizations are available for each phase of the system development process.

It includes controls at controlling new system development activities.

The **6 activities** discussed below deal with system development controls in IT setup. **(U-SIT-UP)**

User Specification Activities: Users must be actively involved in the systems development process.

User involvement should not be ignored because of a high degree of technical complexity in the system.

Regardless of the technology involved, the user can create a detailed written description of the logical needs that must be satisfied by the system.

The creation of a user specification document often involves the joint efforts of the user and systems professionals.

However, it is most important that this document remains a statement of user needs.

System Authorization Activities: All systems must be properly authorized to ensure their economic justification and feasibility.

As with any transaction, system's authorization should be formal.

This requires that each new system request be submitted in written form by users to systems professionals who have both the expertise and authority to evaluate and approve or reject the request.

Internal Auditor's Participation: The internal auditor plays an important role in the control of systems development activities, particularly in organizations whose users lack technical expertise.

The auditor should become involved at the inception of the SDLC process to make conceptual suggestions regarding system requirements and controls. A

uditor's involvement should be continued throughout all phases of the development process and into the maintenance phase.

Technical Design Activities: The technical design activities in the SDLC translate the user specifications into a set of detailed technical specifications of a system that meets the user's needs.

The scope of these activities includes systems analysis, general systems design, feasibility analysis, and detailed systems design.

The adequacy of these activities is measured by the quality of the documentation that emerges from each phase.

Documentation is both a control and evidence of control and is critical to the system's long term success.

User Test and Acceptance Procedures: Just before implementation, the individual modules of the system must be tested as a unified whole.

A test team comprising user personnel, systems professionals, and internal audit personnel subjects the system to rigorous testing.

Once the test team is satisfied that the system meets its stated requirements, the system is formally accepted by the user department(s).

The formal test and acceptance of the system should consider being the most important control over the SDLC. It is imperative that user acceptance be documented.

Before implementation, this is the last point at which the user can determine the system's adequacy and acceptability.

Although discovering a major flaw at this juncture is costly, discovering the flaw during the production operations may be devastating.

Program Testing: All program modules must be thoroughly tested before they are implemented.

The results of the tests are then compared against predetermined results to identify programming and logic errors.

Program testing is time-consuming, the principal task being the creation of meaningful test data.

To facilitate the efficient implementation of audit objectives, test data prepared during the implementation phase must be preserved for future use.

This will give the auditor a frame of reference for designing and evaluating future audit tests.

Having a basis for comparison, the auditor can thus quickly verify the integrity of the program code.

On the other hand, if changes have occurred, the original test data can provide evidence regarding these changes. The auditor can thus focus attention upon those areas.

3. Programming Management Controls

The purpose of the control phase during software development or acquisition is to monitor progress against plan and to ensure software released for production use is authentic, accurate, and complete.

The program development life cycle comprises **6 major phases** –

Planning; Design; Control; Coding; Testing; and Operation and Maintenance with Control phase running in parallel for all other phases. **(PC-TO-DC)**

<table>
<tr><th>Phase</th><th>Controls</th></tr>
<tr><td>Planning</td><td>Techniques like Work Breakdown Structures (WBS), Gantt charts and PERT (Program Evaluation and Review Technique) Charts can be used to monitor progress against plan.</td></tr>
<tr><td>Control</td><td>The Control phase has 2 major purposes:
<table>
<tr><td>Task progress in various software life-cycle phases should be monitored against plan and corrective action should be taken in case of any deviations.</td><td>Control over software development, acquisition, and implantation tasks should be exercised to ensure software released for production use is authentic, accurate, and complete.</td></tr>
</table></td></tr>
<tr><td>Testing</td><td>3 types of testing can be undertaken:
<table>
<tr><td>Unit Testing – which focuses on individual program modules;</td><td>Integration Testing – Which focuses in groups of program modules; and</td><td>Whole-of-Program Testing – which focuses on whole program. These tests are to ensure that a developed or acquired program achieves its specified requirements.</td></tr>
</table></td></tr>
<tr><td>Operation and Maintenance</td><td>3 types of maintenance can be used are as follows:
<table>
<tr><td>Repair Maintenance – in which program errors are corrected;</td><td>Adaptive Maintenance – in which the program is modified to meet changing user requirements;</td><td>Perfective Maintenance - in which the program is tuned to decrease the resource consumption.</td></tr>
</table></td></tr>
<tr><td>Design</td><td>A systematic approach to program design, such as any of the structured design approaches or object-oriented design is adopted.</td></tr>
<tr><td>Coding</td><td>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).</td></tr>
</table>

4. Data Resource Management Controls

Many organizations now recognize that data is a critical resource that must be managed properly and therefore, accordingly, centralized planning and control are implemented.

Careful control should be exercised over the roles by appointing senior, trustworthy persons, separating duties to the extent possible and maintaining and monitoring logs of the data administrator's and database administrator's activities.

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

1. Definition Controls: These controls are placed to ensure that the database always corresponds and comply with its definition standards.

2. Existence/Backup Controls: These ensure the existence of the database by establishing backup and recovery procedures.

Backup refers to making copies of the data so that these additional copies may be used to restore the original data after a data loss.

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 given as follows

Dual recording of data	Under this strategy, two complete copies of the database are maintained. The databases are concurrently updated.
Periodic dumping of data	This strategy involves taking a periodic dump of all or part of the database onto some backup storage medium – magnetic tape, removable disk, Optical disk etc. The dump may be scheduled.
Logging input transactions	This involves logging the input data transactions which cause changes to the database. Normally, this works in conjunction with a periodic dump.
Logging changes to the data	This involves copying a record each time it is changed by an update action.

3. 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.

4. Update Controls: These controls restrict update of the database to authorized users in two ways:

-By permitting only addition of data to the database; and

-Allowing users to change or delete existing data.

5. Concurrency Controls: These controls provide solutions, agreed-upon schedules and strategies to overcome the data integrity problems that may arise when two update processes access the same data item at the same time.

6. Quality Controls: These controls ensure the accuracy, completeness, and consistency of data maintained in the database.

This may include traditional measures such as program validation of input data and batch controls over data in transit through the organization.

5. Quality Assurance Management Controls

Quality Assurance management is concerned with ensuring that the –

- Information systems produced by the information systems function achieve certain quality goals; and

- Development, implementation, operation and maintenance of Information systems comply with a set of quality standards.

The reasons for the emergence of Quality assurance in many organizations are as follows:

Organizations are	- increasingly producing safety-critical systems and users are becoming more demanding in terms of the quality of the software they employ to undertake their work. - undertaking more ambitious projects when they build software. - becoming more concerned about their liabilities if they produce and sell defective software.
- Users are becoming more demanding in terms of their expectations about the quality of software they employ to undertake their work, - Poor quality control over the production, implementation, operation, and maintenance of software can be costly in terms of missed deadlines, dissatisfied users and customer, lower morale among IS staff, higher maintenance and strategic projects that must be abandoned.	

- Improving the quality of Information Systems is a part of a worldwide trend among organizations to improve the quality of the goods and services they sell.

6. Security Management Controls

Information security administrators are responsible for ensuring that information systems assets categorized under Personnel, Hardware, Facilities, Documentation, Supplies Data, Application Software and System Software are secure.

Assets are secure when the expected losses that will occur over some time, are at an acceptable level.

Major Security threats and their control measures

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	Code of conduct to govern the actions of information systems employees.

However, in spite of the controls on place, there could be a possibility that a control might fail. When disaster strikes, it still must be possible to recover operations and mitigate losses using the last resort controls –

A Disaster Recovery Plan (DRP) and Insurance.

DRP: A comprehensive DRP comprise four parts – an Emergency Plan, a Backup Plan, a Recovery Plan and a Test Plan. The plan lays down the policies, guidelines, and procedures for all Information System personnel.

Insurance: Adequate insurance must be able to replace Information Systems assets and to cover the extra costs associated with restoring normal operations. Policies usually can be obtained to cover the resources like – Equipment, Facilities, Storage Media, Valuable Papers and Records etc.

7. Operations Management Controls (DND-MPC-FC-H)

1. Computer Operations: The controls over computer operations govern the activities that directly support the day-to-day execution of either test or production systems on the hardware/software platform available. 3 types of controls fall under this category:

Operation controls: These controls prescribe the functions that either human operators or automated operations facilities must perform.

Scheduling controls: These controls prescribe how jobs are to be scheduled on a hardware/software platform.

Maintenance controls: These controls prescribe how hardware is to be maintained in good operating order.

2. Network Operations: This includes the proper functioning of network operations and monitoring the performance of network communication channels, network devices, and network programs and files.

Data may be lost or corrupted through component failure.

The **primary components** in the communication sub-systems are given as follows:

- Communication lines viz. twisted pair, coaxial cables, fiber optics, microwave and satellite etc.

- Hardware – ports, modems, multiplexers, switches and concentrators etc.

- Software – Packet switching software, polling software, data compression software

- Due to component failure, transmission between sender and receiver may be disrupted, destroyed or corrupted in the communication system.

3. Data Preparation and Entry: Irrespective of whether the data is obtained indirectly from source documents or directly from, say, customers, keyboard environments and facilities should be designed to promote speed and accuracy and to maintain the wellbeing of keyboard operators.

4. Production Control: This includes the major functions like- receipt and dispatch of input and output; job scheduling; management of service-level agreements with users; transfer pricing/charge-out control; and acquisition of computer consumables.

5. File Library: This includes the management of an organization's machine-readable storage media like magnetic tapes, cartridges, and optical disks.

6. Documentation and Program Library: This involves that documentation librarians **ensure**

that documentation is stored securely;
that only authorized personnel gain access to documentation;
that documentation is kept up-to-date and

that adequate backup exists for documentation.

The documentation may **include**

reporting of responsibility and authority of each function;
Definition of responsibilities and objectives of each functions;
Reporting responsibility and authority of each function;
Policies and procedures;
Job descriptions and Segregation of duties.

-Each IS function must be clearly defined and documented including system software, application software, database administration etc.

-Policies establish the rules or boundaries of authority delegated to individuals in the enterprise. Procedures establish the instructions that individuals must follow to compete their daily assigned tasks.

-Documented policies should exist in IS for use of IS resource; Physical security; Data security; On-line security; Use of Information systems; Reviewing, evaluating, and purchasing hardware and software; system development methodology; and Application program changes

-Job descriptions communicate management's specific expectations for job performance. Job procedures establish instructions on how to do the job and policies define the authority of the employee.

-Segregation of duties refers to the concept of distribution of work responsibilities such that individual employees are performing only the duties stipulated for their respective jobs and positions.

7. Help Desk/Technical support: This assists end-users to employ end-user hardware and software such as micro-computers, spreadsheet packages, database management packages etc. and also provides the technical support for production systems by assisting with problem resolution.

8. Capacity Planning and Performance Monitoring: Regular performance monitoring facilitates the capacity planning wherein the resource deficiencies must be identified well in time so that they can be made available when they are needed.

9. Management of Outsourced Operations: This has the responsibility for carrying out day-to-day monitoring of the outsourcing contract.

Application Controls and their Categories

1.Boundary Controls

The major controls of the boundary system are the access control mechanism. (ACM)

ACM links the authentic users to the authorized resources, they are permitted to access.

The ACM has 3 steps of identification, authentication and authorization with respect to the access control policy implemented.

Major Boundary Control techniques are given as follows:

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.

A cryptographic technique encrypts data (clear text) into cryptograms (cipher text) and its strength depends on the time and cost to decipher the cipher text by a cryptanalyst.

Three techniques of cryptography are

transposition (permute the order of characters within a set of data),
substitution (replace text with a key-text) and
product cipher (combination of transposition and substitution).

Passwords: User identification by an authentication mechanism with personal characteristics like name, birth date, employee code, function, designation or a combination of two or more of these can be used as a password boundary access control.

A few best practices followed to avoid failures in this control system are; minimum password length, avoid usage of common dictionary words, periodic change of passwords, hashing of passwords and number of entry attempts.

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.

Hence, a PIN may be exposed to vulnerabilities while issuance or delivery, validation, transmission and storage.

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.

Biometric Devices: Biometric identification e.g. thumb and/or finger impression, eye retina etc. are also used as boundary control techniques.

2. Input Controls

Source Document Controls	Data Coding Controls	Batch controls	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.

For example, an individual with access to purchase orders and receiving reports could fabricate a purchase transaction to a non-existent supplier.

If these documents were entered into the data processing stream along with a fictitious vendor's invoice, the system could process these documents as if a legitimate transaction had taken place.

To control against this type of exposure, the organization must implement control procedures over source documents to account for each document, as described below:

Use pre-numbered source documents: Source documents should come pre-numbered from the printer with a unique sequential number on each document.

Source document numbers enable accurate accounting of document usage and provide an audit trail for tracing transactions through accounting records.

Use source documents in sequence: Source documents should be distributed to the users and used in sequence.

This requires the adequate physical security be maintained over the source document inventory at the user site.

When not in use, lock and key and access to source documents should be limited to authorized persons.

Periodically audit source documents: Missing source documents should be identified by reconciling document sequence numbers.

Periodically, the auditor should compare the numbers of documents used to date with those remaining in inventory plus those voided due to errors.

Documents not accounted for should be reported to management.

2. Data Coding Controls: Two types of errors can corrupt a data code and cause processing errors.

Transcription Errors (3 Classes)	Transposition Errors (2 types)
-**Addition errors** occur when an extra digit or character is added to the code. For example, inventory item number 83276 is recorded as 832766. -**Truncation errors** occur when a digit or character is removed from the end of a code. In this type of error, the inventory item above would be recorded as 8327. -**Substitution errors** are the replacement of one digit in a code with another. For example, code number 83276 is recorded as 83266.	-**Single transposition errors** occur when two adjacent digits are reversed. For instance, **12**345 are recorded as **21**345. -**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:

Physical Controls: These controls are groups of transactions that constitute a physical unit. For example – source documents might be obtained via the email, assembled into batches, spiked and tied together, and then given to a data-entry clerk to be entered into an application system at a terminal.	**Logical Controls:** These are group of transactions bound together on some logical basis, rather than being physically contiguous. For example - different clerks might use the same terminal to enter transaction into an application system. Clerks keep control totals of the transactions into an application system.

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:

Level-1: Field Interrogation: It involves programmed procedures that examine the characters of the data in the field.

Various field checks used to ensure data integrity have been described below: **(AP-VLCC)**

Arithmetic Checks	Simple Arithmetic is performed in different ways to validate the result of other computations of the values of selected data fields.
Picture Checks	These check against entry into processing of incorrect/invalid characters.
Valid Code Checks	Checks are made against predetermined transactions codes, tables or order data to ensure that input data are valid. The predetermined codes or tables may either be embedded in the programs or stored in (direct access) files.

Limit Check	This is a basic test for data processing accuracy and may be applied to both the input and output data. The field is checked by the program against predefined limits to ensure that no input/output error has occurred or at least no input error exceeding certain pre-established limits has occurred.
Check Digit	One method for detecting data coding errors is a check digit. A check digit is a control digit (or digits) added to the code when it is originally assigned that allows the integrity of the code to be established during subsequent processing. The check digit can be located anywhere in the code, as a prefix, a suffix, or embedded someplace in the middle.
Cross Checks	may be employed to verify fields appearing in different files to see that the result tally.

Level-2: Record Interrogation:

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

2. **Reasonableness Check:** Whether the value specified in a field is reasonable for that particular field?

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

Level-3: File Interrogation: (VIP-DB-F)

Version usage	Proper version of a file should be used for processing the data correctly. In this regard it should be ensured that only the most current file be processed.
Internal and External Labeling	Labeling of storage media is important to ensure that the proper files are loaded for process. Where there is a manual process for loading files, external labeling is important to ensure that the correct file is being processed. Where there is an automated tape loader system, internal labeling is more important.
Parity Check	When programs or data are transmitted, additional controls are needed. Transmission errors are controlled primarily by detecting errors or correcting codes.
Data File Security	Unauthorized access to data file should be prevented, to ensure its confidentiality, integrity and availability. These controls ensure that the correct file is used for processing.
Before and after Image and Logging	The application may provide for reporting of before and after images of transactions. These images combined with the logging of events enable re-constructing the data file back to its last state of integrity, after which the application can ensure that the incremental transactions/events are rolled back or forward.
File Updating and Maintenance Authorization	Sufficient controls should exist for file updating and maintenance to ensure that stored data are protected. The access restrictions may either be part of the application program or of the overall system access restrictions.

3. Communication Controls

Physical Component Controls	Line Error Control	Flow Controls	Link Controls
Topological Controls	Channel Access Controls	Internetworking Controls	

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

Physical Components affecting reliability of Communication subsystem – **(TMC-PM)**

Transmission Media	It is a physical path along which a signal can be transmitted between a sender and a receiver. It is of two types:	
	Guided/Bound Media in which the signals are transported along an enclosed physical path like – Twisted pair, coaxial cable, and optical fiber.	In **Unguided Media**, the signals transmit via free-space emission like – satellite microwave, radio frequency and infrared.

Modem	-Increases the speed with which data can be transmitted over a communication line. -Reduces the number of line errors that arise through distortion if they use a process called equalization & also through noise.
Communication Lines	The reliability of data transmission can be improved by choosing a private (leased) communication line rather than a public communication line.
Port Protection Devices	Used to mitigate exposures associated with dial-up access to a computer system. The port-protection device performs various security functions to authenticate users.
Multiplexers and Concentrators	- These allow the band width or capacity of a communication line to be used more effectively. -These share the use of a high-cost transmission line among many messages that arrive at the multiplexer or concentration point from multiple low cost source lines.

(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.

Error Detection: The errors can be detected by either using a loop (echo) check or building some form of redundancy into the message transmitted.	**Error Correction:** When line errors have been detected, they must then be corrected using either forward error correcting codes or backward error correcting codes.

(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.

For example, a main frame can transmit data to a microcomputer terminal.

The microcomputer cannot display data on its screen at the same rate the data arrives from the main frame.

Moreover, the microcomputer will have limited buffer space.

Thus, it cannot continue to receive data from the mainframe and to store the data in its buffer pending display of the data on its screen.

Flow controls will be used, therefore, to prevent the mainframe swamping the microcomputer and, as a result, data is lost.

(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.

The link management components mainly use 2 common protocols

HDLC (Higher Level Data Link control) and SDLC (Synchronous Data Link Control).

(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. Specifying the optimum topology for a network can be a problem of immense complexity.

Local Area Network Topologies: Local Area Networks tend to **have 3 characteristics**: (1) they are privately owned networks; (2) they provide high -speed communication among nodes; and (3) they are confined to limited geographic areas (for example, a single floor or building or locations within a few kilometers of each other). They are implemented using **4 basic types of topologies**: (1) bus topology,	**Wide Area Network Topologies:** Wide Area Networks have the following characteristics: 1. they often encompass components that are owned by other parties (e.g. a telephone company). 2. they provide relatively low-speed communication among nodes; and 3. they span large geographic areas With the exception of the bus topology, all other topologies that are used to implement LANs can also be used to implement WANs.

(2) Tree topology, (3) Ring topology, and (4) Star topology. Hybrid topologies like the star-ring topology and the star-bus topology are also used.	

(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, some type of channel access control technique must be used.

These techniques fall into two classes: Polling methods and Contention methods.

Polling: Polling (non contention) techniques establish an order in which a node can gain access to channel capacity.	**Contention Methods:** Using contention methods, nodes in a network must compete with each other to gain access to a channel. Each node is given immediate right of access to the channel. Whether the node can use the channel successfully, however, depends on the actions of other nodes connected to the channel.

(g) Internetworking Controls: Internetworking is the process of connecting two or more communication networks together to allow the users of one network to communicate with the users of other networks.

The networks connected to each other might or might not employ the same underlying hardware-software platform.

Three types of devices are used to connect sub- networks in an internet.

Device	Functions
Bridge	A bridge connects similar local area networks (e.g. one token ring network to another token ring network).
Router	A router performs all the functions of a bridge. In addition, it can connect heterogeneous Local Area Networks (e.g. a bus network to a token ring network) and direct network traffic over the fastest channel between two nodes that reside in different sub-networks (e.g. by examining traffic patterns within a network and between different networks to determine channel availability.)
Gateway	Gateway is the most complex of the three network connection devices. The primary function is to perform protocol conversion to allow different types of communication architectures to communicate with one another. The gateway maps the functions performed in an application on one computer to the functions performed by a different application with similar functions on another computer.

4. Processing Controls

These 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. **(REFER)**

1. Run-to-run Totals: These help in verifying data that is subject to process through different stages. A specific record probably the last record can be used to maintain the control total.

2. Edit Checks: Edit checks similar to the data validation controls can also be used at the processing stage to verify accuracy and completeness of data.

3. Field Initialization: Data overflow can occur, if records are constantly added to a table or if fields are added to a record without initializing it, i.e. setting all values to zero/blank before inserting the field or record.

4. Exception Reports: Exception reports are generated to identify errors in the data processed. Such exception reports give the transaction code and why a particular transaction was not processed or what is the error in processing the transaction.

5. Reasonableness Verification: Two or more fields can be compared and cross verified to ensure their correctness. For example, the statutory percentage of provident fund can be calculated on the gross pay amount to verify if the provident fund contribution deducted is accurate.

5. Database Controls

Major update controls (M-EPS)	Major Report controls (P-EPS)

Major update controls are given as follows: (M-EPS)

1. Maintain a suspense account: When mapping between the master record to transaction record results in a mismatch due to failure in the corresponding record entry in the master record; then these transactions are maintained in a suspense account.

A non- zero balance of the suspense accounts reflects the errors to be corrected.

2. Ensure All Records on Files are processed: While processing, the transaction file records mapped to the respective master file, and

the end-of-file of the transaction file with respect to the end-of-file of the master file is to be ensured.

3. Process multiple transactions for a single record in the correct order: Multiple transactions can occur based on a single master record (e.g. dispatch of a product to different distribution centers).

Here, the order in which transactions are processed against the product master record must be done based on a sorted transaction codes.

4. Sequence Check between Transaction and Master Files: Synchronization and the correct sequence of processing between the master file and transaction file is critical to maintain the integrity of updating, insertion or deletion of records in the master file with respect to the transaction records.

Major Report controls are given as follows: (P-EPS)

1. Print-Run-to Run Control Totals: Run-to-Run control totals help in identifying errors or irregularities like record dropped erroneously from a transaction file, wrong sequence of updating or the application software processing errors.

2. Existence/Recovery Controls: The back-up and recovery strategies together encompass the controls required to restore failure in a database.

Backup strategies are implemented using prior version and logs of transactions or changes to the database.

3. Print Suspense Account Entries: Similar to the update controls, the suspense account entries are to be periodically monitors with the respective error file and action taken on time.

4. Standing Data: Application programs use many internal tables to perform various functions like gross pay calculation, billing calculation based on a price table, bank interest calculation etc.

Maintaining integrity of the pay rate table, price table and interest table is critical within an organization. Any changes or errors in these tables would have an adverse effect on the organizations basic functions.

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 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.

Whatever the type of output, it should be ensured that the confidentiality and integrity of the output is maintained and that the output is consistent.

Various Output Controls are given as follows: **(SLR-CSR)**

1. Storage and logging of sensitive, critical forms:

Pre-printed stationery should be stored securely to prevent unauthorized destruction or removal and usage.

Only authorized persons should be allowed access to stationery supplies such as security forms, negotiable instruments, etc.

2. Logging of output program executions:

When programs used for output of data are executed, these should be logged and monitored; otherwise confidentiality/integrity of the data may be compromised.

3. Report distribution and collection controls:

Distribution of reports should be made in a secure way to prevent unauthorized disclosure of data.

It should be made immediately after printing to ensure that the time gap between generation and distribution is reduced.

A log should be maintained for reports that were generated and to whom these were distributed.

Where users have to collect reports the user should be responsible for timely collection of the report, especially if it is printed in a public area.

Uncollected reports should be stored securely.

4. Controls over printing:

Outputs should be made on the correct printer and it should be ensured that unauthorized disclosure of information printed does not take place.

Users must be trained to select the correct printer and access restrictions may be placed on the workstations that can be used for printing.

5. Spooling:

"Spool" is an acronym for **"Simultaneous Peripherals Operations Online".**

This is a process used to ensure that the user is able to continue working, while the print operation is getting completed.

When a file is to be printed, the operating system stores the data stream to be sent to the printer in a temporary file on the hard disk.

This file is then **"spooled"** to the printer as soon as the printer is ready to accept the data.

6. Retention controls:

Retention controls consider the duration for which outputs should be retained before being destroyed. Consideration should be given to the type of medium on which the output is stored.

Retention control requires that a date should be determined for each output item produced.

Controls over Data Integrity and Security

For many organizations, a simple 5 scale grade will suffice as follows: **(THP-IP)**

1.Top Secret:

Highly sensitive internal information

e.g. pending mergers or acquisitions;
investment strategies;
plans or designs; that could seriously damage the organization if such information were lost or made public.

Information classified as Top Secret information has very restricted distribution and must be protected at all times. Security at this level should be the highest possible.

2. Highly Confidential:

Information that, if made public or even shared around the organization, could seriously impede the organization's operations and is considered critical to its ongoing operations.

Information would include accounting information, business plans, sensitive customer information of banks, solicitors and accountants etc., patient's medical records and similar highly sensitive data.

Such information should not be copied or removed from the organization's operational control without specific authority. Security at this level should be very high.

3. Proprietary:

Information of a proprietary nature; procedures, operational work routines, project plans, designs and specifications that define the way in which the organization operates.

Such information is normally for proprietary use to authorized personnel only. Security at this level should be high.

4. Internal Use only:

Information not approved for general circulation outside the organization where its loss would inconvenience the organization or management but where disclosure is unlikely to result in financial loss or serious damage to credibility.

Examples would include, internal memos, minutes of meetings, internal project reports. Security at this level should controlled but normal.

5.Public Documents:

Information in the public domain;
annual reports, press statements etc.; which has been approved for public use.

Security at this level should minimal.

Data Integrity Policies

Major data integrity policies are given as under:

Virus-Signature Updating	Virus signatures must be updated automatically when they are made available from the vendor through enabling of automatic updates.
Software Testing	All software must be tested in a suitable test environment before installation on production systems.
Division of Environments	The division of environments into Development, Test, and Production is required for critical systems.
Offsite Backup Storage	Backups older than one month must be sent offsite for permanent storage.
Quarter & Year-End Backups	Quarter-end and year-end backups must be done separately from the normal schedule, for accounting purposes
Disaster Recovery	A comprehensive disaster-recovery plan must be used to ensure continuity of the corporate business in the event of an outage.

The financial control techniques are numerous. **(ABCD-SSI)**

Authorization: This entails obtaining the authority to perform some act typically accessing to such assets as accounting or application entries.

Budgets: These estimates of the amount of time or money expected to be spent during a particular period, project, or event. The budget alone is not an effective control.

Budgets must be compared with the actual performance, including isolating differences and researching them for a cause and possible resolution.

Cancellation of documents: This marks a document in such a way to prevent its reuse. This is a typical control over invoices marking them with a “paid” or “processed” stamp or punching a hole in the document.

Dual control: This entails having two people simultaneously access an asset.

Safekeeping: This entails physically securing assets, such as computer disks, under lock and key, in a desk drawer, file cabinet storeroom, or vault.

Sequentially numbered documents: These are working documents with preprinted sequential numbers, which enables the detection of missing documents.

Input/ output verification: This entails comparing the information provided by a computer system to the input documents.

This is an expensive control that tends to be over-recommended by auditors. It is usually aimed at such non-monetary by dollar totals and item counts.

Cyber Attacks

Some of the major cyber attacks are as follows:

Phishing: It is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication.

Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public.

Network Scanning: It is a process to identify active hosts of a system, for purpose of getting information about IP addresses etc.

Virus/Malicious Code: As per Section 43 of the Information Technology Act, 2000, "Computer Virus" means any computer instruction, information, data or program that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a program, data or instruction is executed or some other event takes place in that computer resource;

Spam: E-mailing the same message to everyone on one or more Usenet News Group or LISTSERV lists is termed as spam.

Website Compromise/Malware Propagation: It includes website defacements. Hosting malware on websites in an unauthorized manner.

The impact of cyber frauds on enterprises can be viewed under the following dimensions:

Financial Loss: Cyber frauds lead to actual cash loss to target company/organization. For example, wrongfully withdrawal of money from bank accounts.

Legal Repercussions: Entities hit by cyber frauds are caught in legal liabilities to their customers. Section 43A of the Information Technology Act, 2000, fixes liability for companies/organizations having secured data of customers.

Loss of credibility or Competitive Edge: News that an organizations database has been hit by fraudsters, leads to loss of competitive advantage. This also leads to lose credibility.

Disclosure of Confidential, Sensitive or Embarrassing Information: Cyber-attack may expose critical information in public domain. For example, the instances of individuals leaking information about governments secret programs.

Sabotage: The above situation may lead to misuse of such information by enemy country.

Following are the major techniques to commit cyber frauds:

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.

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.

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.

Data Leakage: It refers to the unauthorized copying of company data such as computer files.

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.

Internet Terrorism: It refers to the using Internet to disrupt electronic commerce and to destroy company and individual communications.

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.

Masquerading or Impersonation: In this case, perpetrator gains access to the system by pretending to be an authorized user.

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.

Piggybacking: It refers to the tapping into a telecommunication line and latching on to a legitimate user before s/he logs into the system.

Round Down: Computer rounds down all interest calculations to 2 decimal places. Remaining fraction is placed in account controlled by perpetrator.

Scavenging or Dumpster Diving: It refers to the gaining access to confidential information by searching corporate records.

Social Engineering Techniques: In this case, perpetrator tricks an employee into giving out the information needed to get into the system.

Super Zapping: It refers to the unauthorized use of special system programs to bypass regular system controls and performs illegal acts.

Trap Door: In this technique, perpetrator enters in the system using a back door that bypasses normal system controls and perpetrates fraud.