CHAPTER-3
PROTECTION OF SYSTEM

3.1. Need for Protection of Information Systems

In a global information society, Organizations depend on timely, accurate, complete, valid, consistent, relevant, and reliable information. Accordingly, executive management has a responsibility to ensure that the organization provides all users with a secure information processing environment. It is clear that there are not only many direct and indirect benefits from the use of information systems, there are also many direct and indirect risks relating to the information systems. These risks have led to a gap between the need to protect systems and the degree of protection applied. This gap is caused by:

1) Widespread use of technology;
2) Interconnectivity of systems;
3) Elimination of distance, time, and space as constraints;
4) Unevenness of technological changes;
5) Devolution of management and control;
6) Attractiveness of conducting unconventional electronic attacks over more conventional physical attacks against organizations; and
7) External factors such as legislative, legal, and regulatory requirements or technological developments.

Information security failures may result in both financial losses and/or intangible losses such as unauthorized disclosure of competitive or sensitive information.

Threats to information systems may arise from intentional or unintentional acts and may come from internal or external sources. The threats may emanate from, among others, technical conditions (program bugs, disk crashes), natural disasters (fire, flood), environmental conditions (electrical surges), human factors (lack of training, errors, and omissions), unauthorized access (hacking), or viruses. In addition to these, other threats, such as business dependencies (reliance on third party communications carriers, outsourced operations, etc.) can potentially result in a loss of management control and oversight. Adequate measures for information security help to ensure the smooth functioning of information systems and protect the organization from loss or embarrassment caused by security failures.

3.2. Information System Security

Information security refers to the protection of valuable assets against loss, disclosure, or damage. Securing valuable assets from threats, sabotage, or natural disaster with physical safeguards such as locks, perimeter fences, and insurance is commonly understood and implemented by most of the organizations. However, security must be expanded to include logical and other technical safeguards such as user identifiers, passwords, firewalls, etc., which is not understood well by many organizations.

This concept of information security applies to all information. In this context, the valuable assets are the data or information recorded, processed, stored, shared, transmitted, or retrieved from an electronic medium.

1) **Information Security Objective:** The objective of information system security is “the protection of the interests of those relying on information, and protect the information systems and communications that deliver the information from harm resulting from failures of confidentiality, integrity, and availability”.

2) For any organization, the security objective comprises three universally accepted attributes:
   a) **Confidentiality:** Prevention of the unauthorized disclosure of information;
   b) **Integrity:** Prevention of the unauthorized modification of information; and
   c) **Availability:** Prevention of the unauthorized withholding of information.
   d) The relative priority and significance of Confidentiality, Integrity and Availability (CIA) vary according to the data within the information system and the business context in which it is used.

CHAPTER-3
PROTECTION OF SYSTEM

3.3. What Information is Sensitive?

The following examples highlight some of the factors, necessary for an organization to succeed. The common aspect in each case is the critical information that each organization generates.

1) **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. For example: a competitor learns that a company is testing a new product line in a specific geographic location. The competitor removes its product from that location, creating an illusionary demand for the product. When the positive results of the test marketing are provided to the company's executives, they decide to roll the product out nationwide. Only then did the company discover that in all other geographic regions the competition for their product was intense. The result is that the company lost several million, rupees as its product sales faltered.

2) **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. While many organizations prohibit the sharing of such data, carelessness often results in its compromise. Such activity includes inadvertent storage of data on unauthorized systems, unprotected laptops, and failure to secure magnetic media.

3) **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. Similarly, availability of information about product pricing may also be used by competitive enterprises to price its products, competitively. When competitors' costs are lower, they can either under- price the market or increase prices. In either case, the damage to an organization may be significant.

3.4. Information Security Policy

In its basic form, a information security policy is a document that describes an organization's information security controls and activities. The policy does not specify technologies or specific solutions; it defines a specific set of intentions and conditions that help protect a company's information assets and its ability to conduct business.

1) **Information Security policy invariably includes rules intended to:**
   - **a)** Preserve and protect information from any unauthorized modification, access or disclosure;
   - **b)** Limit or eliminate potential legal liability from employees or third parties; and
   - **c)** Prevent waste or inappropriate use of the resources of an organization.
   - **d)** An information security policy should be in written form. It provides instructions to employees about 'what kinds of behavior or resource usage are required and acceptable', and about 'what is unacceptable'. An information security policy also provides direction to all employees about how to protect organization's information assets, and instructions regarding acceptable (and unacceptable) practices and behavior.

2) **Tools to Implement Policy: Standards, Guidelines, and Procedures:** Standards specify technologies and methodologies to be used to secure systems. Guidelines help in smooth implementation of information security policy.

   Procedures are more detailed steps to be followed to accomplish particular security related tasks. Procedures normally assist in implementing applicable information security Policy. These are detailed steps to be followed by users, system operations personnel, and others to accomplish a particular task.

3) Issues to be address in Information Security Policy:

The policy should at least address the following issues:

a) a **definition** of information security,
b) **reasons for important** to the organization, and its goals and principles,
c) a brief explanation of the security policies, principles, standards and compliance requirements,
d) definition of all relevant information security responsibilities; and
e) Reference to supporting documentation.

The auditor should ensure that the policy is readily accessible to all employees and that all employees are aware of its existence and understand its contents. The policy may be a stand-alone statement or part of more extensive documentation. In general, most of the employees have some responsibilities for information security, and auditors should review any declarations to the contrary with care. The auditor should also ensure that the policy has an owner who is responsible for its maintenance and that it is updated responding to any changes affecting the basis of the original risk assessment.

4) Members of Security Policy: Security has to encompass managerial, technological and legal aspects.

Security policy broadly comprises the following three groups of management:

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

Information security policies must always take into account business requirements. Business requirements are the principles and objectives adopted by an 6organization to support its operations and information processing. E-commerce security is an example of such business requirements. Furthermore, policies must consistently take into account the legal, statutory, regulatory and contractual requirements

5) Information Security Policies and their Hierarchy:

Major Information Security Policies are given as follows:

a) **Information Security Policy**: This policy provides a definition of Information Security, its overall objective and the importance applies to all users.

b) **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.

c) **Acceptable Usage Policy:** This sets out the policy for acceptable use of email and Internet services.

d) **Organizational Information Security Policy:** This policy sets out the Group policy for the security of its information assets and the Information Technology (IT) systems processing this information. (Although it is positioned at the bottom of the above hierarchy diagram, it is the main IT security policy document.)

e) **Network & System Security Policy:** This policy sets out detailed policy for system and network security and applies to IT department users.

f) **Information Classification Policy :** This policy sets out the policy for the classification of information

6) Components of the Security Policy:

A good security policy should clearly state the following:

a) Purpose and Scope of the Document and the intended audience;
b) The Security Infrastructure;
c) Security policy document maintenance and compliance requirements;
d) Incident response mechanism and incident reporting;
e) Security organization Structure;
f) Inventory and Classification of assets;
g) Description of technologies and computing structure;
h) Physical and Environmental Security;
i) Identity Management and access control;
j) IT Operations management;
k) IT Communications;
l) System Development and Maintenance Controls;
m) Business Continuity Planning;
n) Legal Compliances; and
o) Monitoring and Auditing Requirements.

3.5. Information Systems Controls

Control is defined as Policies, procedures, practices and enterprise structure that are designed to provide reasonable assurance that business objectives will be achieved and undesired events are prevented, detected and corrected. Thus, an information systems auditing includes reviewing the implemented system or providing consultation and evaluating the reliability of operational effectiveness of controls.

1) Need for Controls in Information Systems:

Today's dynamic global enterprises need information integrity, reliability and validity for timely flow of accurate information throughout the organization. Safeguarding assets to maintain data integrity to achieve system effectiveness and efficiency is a significant control process.

a) IS control procedure may include:
b) Strategy and direction,
c) General Organization and Management
d) Access to IT resources, including data and programs,
e) System development methodologies and change control,
f) Operation procedures,
g) System Programming and technical support functions,
h) Quality Assurance Procedures,
i) Physical Access Control
j) BCP and DRP,
k) Network and Communication,
l) Database Administration, and
m) Protective and detective mechanisms against internal and external attacks.

2) Impact of Technology on Internal Controls:

The internal controls within an enterprise in a computerised environment, encompasses the goal of asset safeguarding, data integrity, system efficiency and effectiveness. These are discussed as follows:

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

b) Segregation of duties: A key control in an information system is segregation of duties. Basically means that in the processing of a transaction, there are split between different people, such that one person cannot process a transaction right from start to finish. Various stages in the transaction cycle are spread between two or more individuals. However, in a computerised system, the auditor should also be concerned with the segregation of duties within the IT department. Within an IT environment, the staff in the IT department of an enterprise will have a detailed knowledge of the interrelationship between the source of data,

how it is processed and distribution and use of output. IT staff may also be in a position to alter transaction data or even the financial applications which process the transactions.

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

d) Record keeping: There are various controls over the protection and storage of documents, transaction details, and audit trails etc.

e) Access to assets and records: In the manual systems, protection from unauthorised access was through the use of locked doors and filing cabinets. Computerised financial systems have not changed the need to protect the data. A client's financial data and computer programs are vulnerable to unauthorised amendment in the computer or from remote locations. The use of wide area networks, including the Internet, has increased the risk of unauthorised access. The nature and types of control available have changed to address these new risks.

f) Management supervision and review: Management's supervision and review helps to deter and detect both errors and fraud.

g) Concentration of programs and data: Transaction and master file data (e.g. pay rates, approved suppliers lists etc.) may be stored in a computer readable form on one computer installation or on a number of distributed installations. Computer programs such as file editors are likely to be stored in the same location as the data. Therefore, in the absence of appropriate controls over these programs and utilities, there is an increased risk of unauthorised access and alteration of financial data.

3) Internal controls comprise of the following five interrelated components:

a) Control Environment: Elements that establish the control context in which specific accounting systems and control procedures must operate. The control environment is manifested in management's operating style, the ways authority and responsibility are assigned, the functional method of the audit committee, the methods used to plan and monitor performance and so on.

b) Risk Assessment: Elements that identify and analyze the risks faced by an organisation and the way the risk can be managed. Both external and internal auditors are concerned with errors or irregularities that cause material losses to an organisation.

c) Control Activities: Elements that operate to ensure transactions are authorized, duties are segregated, adequate documents and records are maintained, assets and records are safeguarded, and independent checks on performance and valuation of records.

d) Information and Communication: Elements, in which information is identified, captured and exchanged in a timely and appropriate form to allow personnel to discharge their responsibilities.

e) Monitoring: Elements that ensure internal controls operate reliably over time.

CHAPTER-3
PROTECTION OF SYSTEM

3.6. Objective of Controls

The objective of controls is to reduce or if possible eliminate the causes of the exposure to potential loss. Exposures are potential losses due to threats materializing.

Some categories of exposures are:

1) Errors or omissions in data, procedure, processing, judgment and comparison;
2) Improper authorizations and improper accountability with regards to procedures, processing, judgment and comparison; and
3) Inefficient activity in procedures, processing and comparison. Some of the critical control lacking in a computerized environment are:
4) Lack of management understanding of IS risks and related controls;
5) Absence or inadequate IS control framework.
6) Absence of weak general controls and IS controls;
7) Lack of awareness and knowledge of IS risks and controls amongst the business users and even IT staff;
8) Complexity of implementation of controls in extended enterprises; distributed computing environments and
9) Lack of control features or their implementation in highly technology driven environments; and
10) Inappropriate technology implementations or inadequate security functionality in technologies implemented.

3.7. Categories of Controls

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

1) **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 characteristics of preventive controls are:
   a) A clear-cut understanding about the vulnerabilities of the asset;
   b) Understanding probable threats; and
   c) Provision of necessary controls for probable threats from materializing.

   Examples of preventive controls are given as follows:
   Employ qualified personnel, Segregation of duties, Access control, Vaccination against diseases, Documentation, Prescribing appropriate books for a course, Training and retraining of staff Authorization of transaction, Validation, edit checks in the application, Firewalls, Anti-virus software (sometimes this acts like a corrective control also), etc., and Passwords.

2) **Detective Controls:** These controls are designed to detect errors, omissions or malicious acts that occur and report the occurrence. The characteristics of such controls are given as follows:
   a) Clear understanding of lawful activities so that anything which deviates from these is reported as unlawful, malicious, etc;
   b) An established mechanism to refer the reported unlawful activities to the appropriate person or group;
   c) Interaction with the preventive control to prevent such acts from occurring; and
   d) Surprise checks by supervisor.

   Examples of detective controls include:
   Hash totals, Check points in production jobs, Echo control in telecommunications, Error message over tape labels, Duplicate checking of calculations, Periodic performance reporting with variances, Past-due accounts report, The internal audit functions, Intrusion detection system, Cash counts and bank reconciliation, and Monitoring expenditures against budgeted amount.

3) **Corrective Controls:** Corrective controls are designed to reduce the impact or correct an error once it has been detected. A Business Continuity Plan (BCP) is considered to be a corrective control. The main characteristics of the corrective controls are:
   a) Minimizing the impact of the threat;

b) Identifying the cause of the problem.
c) Providing Remedy to the problems discovered by detective controls;
d) Getting feedback from preventive and detective controls;
e) Correcting error arising from a problem; and
f) Modifying the processing systems to minimize future occurrences of the incidents.

Examples of Corrective Controls are given as follows
Contingency planning, Backup procedure, Rerun procedures, Change input value to an application system, and Investigate budget variance and report violations.

4) Compensatory Controls: Controls are basically designed to reduce the probability of threats, which can exploit the vulnerabilities of an asset and cause a loss to that asset. While designing the appropriate control one thing should be kept in mind— the cost of the lock should not be more than the cost of the assets it protects. 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. Such measures are called compensatory controls.

5) Another classification of controls is based on the nature of IS resources. These are as under:

a) Environmental controls: These are the controls relating to IT environment such as power, air-conditioning, UPS, smoke detection, fire-extinguishers, dehumidifiers etc.

b) Physical Access Controls: These are the 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.

c) Logical Access Controls: These are the controls relating to logical access to information resources such as operating systems controls, application software boundary controls, networking controls, access to database objects, encryption controls etc.

d) IS Operational Controls: These are the controls relating to IS operation, administration and its management such as day begin and day end controls, IS infrastructure management, Helpdesk operations etc.

e) IS Management Controls: These are the controls relating to IS management, administration, policies, procedures, standards' and practices, monitoring of IS operations, Steering committee etc.

f) SDLC Controls: These are the controls relating to planning, design, development, testing, implementation and post implementation, change management of changes to application, other software and operations.

6) Further, another category of controls is based on their functional nature. When reviewing a client's control systems, the auditor will be able to identify three components of internal control. Each component is aimed at achieving different objectives. These controls are given as follows:

a) Internal Accounting Controls: The Controls which are intended to safeguard the client's assets and ensure the reliability of the financial records are called internal accounting controls.

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

c) Administrative Controls: These are concerned with ensuring efficiency and compliance with management policies, including the operational controls.

3.8. Organizational Controls

These controls are concerned with the decision-making processes that lead to management authorization of transactions. Organizational control techniques include documentation of:

1) Reporting responsibility and authority of each function,
2) Definition of responsibilities and objectives of each functions,
3) Policies and procedures,
4) Job descriptions, and
5) Segregation of duties.

These are discussed as follows:

1) Responsibilities and objectives: Each IS function must be clearly defined and documented, including systems software, application programming and systems development, database administration, and operations. Their responsibilities include:

a) Providing information to senior management on the IS resources, to enable senior management to meet strategic objectives;
b) Planning for expansion of IS resources;
c) Controlling the use of IS resources; and
d) Implementing activities and functions that support accomplishment of strategic plan.

2) Policies, standards, procedures and practices: Policies establish the rules or boundaries of authority delegated to individuals in the enterprise. These are the standards and instructions that all IS personnel must follow when completing their assigned duties. Procedures establish the instructions that individuals must follow to compete their daily assigned tasks. Documented policies should exist in IS for:

a) Use of IS resources,
b) Physical security,
c) Data security
d) On-line security,
e) Use of Information systems,
f) Reviewing, evaluating, and purchasing hardware and software,
g) System development methodology, and Application program changes
h) Documented procedures should exist for all data processing activities.

3) Job descriptions: These communicate management's specific expectations for job performance. All jobs must have a current documented job description readily available to the employee. Job descriptions establish responsibility and the accountability of the employee's actions.

4) Segregation of duties:

There are various general guidelines, with reference to 'Segregation of Duties', which may be followed in addition with concepts like, the maker should not be the checker:

a) Separate those, who can run live programs e.g. operations department, from those who can change programs e.g. programmers. This is required in order to ensure that unauthorized programs are prevented from running.

b) Separate those, who can access the data e.g. data entry and the DBA, from those who can run programs e.g. computer operators. This is required in order to ensure that unauthorized data entry cannot take place.

c) Separate those, who can input data e.g. data entry, from those, who can reconcile or approve data e.g. data authorization persons. This is required in order to ensure that unauthorized data entry cannot take place.

d) Separate those, who can test programs e.g. users, quality assurance and security, from those, who can develop programs e.g. application programmers. This is required in order to ensure that unauthorized programs cannot be allowed to run.

e) Separate those, who can enter errors in a log e.g. data entry operator, who transfer the data to an error log, from those who can correct the errors like the end user departments. This is required in order to ensure that unauthorized data entry cannot take place.

f) Separate those, who can enter data e.g. data entry personnel, from those who can access the database e.g. the DBA. This is required in order to ensure that unauthorized data entry or data modification cannot take place.

3.9. Management Control

The management has the responsibility to determine whether the controls that the enterprise system has put in place are sufficient to ensure that the IT activities are adequately controlled. 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 high level policies establish a framework on which the controls for lower hierarchy of the enterprise. The controls flow from the top of an organization to down; the responsibility still lies with the senior management.

The controls considerations while reviewing management controls in an IS system shall include

1) **Responsibility:** The strategy to have a senior management personnel responsible for the IS within the overall organizational structure.

2) **An IT Organization Structure:** There should be a prescribed IT organizational structure with documented roles and responsibilities and agreed job descriptions.

3) **An IT 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. Here the responsibility lies beyond just the accounting and financial systems; for example, the telecommunications system (phone lines, video- conferencing) office automation, and manufacturing processing systems

3.10. Financial Controls

These controls are generally defined as the procedures exercised by the system user personnel over source, or transactions origination, documents before system input. These areas exercise control over transactions processing using reports generated by the computer applications to reflect un-posted items, non-monetary changes, item counts and amounts of transactions for settlement of transactions processed and reconciliation of the applications (subsystem) to general ledger. The financial control techniques are numerous. A few examples are highlighted here:

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

2) **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

3) **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.

4) **Documentation:** This includes written or typed explanations of actions taken on specific transactions;

5) **Dual control:** This entails having two people simultaneously access an asset. For example, the depositories of banks' 24-hour teller machines should be accessed and emptied with two people present, many people confuse dual control with dual access, but these are distinct and different. Dual access divides the access function between two.

6) **People:** once access is achieved, only one person handles the asset. With teller- machines, for example, two tellers would open the depository vault door together, but only one would retrieve the deposit envelopes.

7) **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.

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

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

10) **Supervisory review:** 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.

3.11. Physical Access Control

These controls are personnel; hardware and software related and include procedures exercised on access to IT resources by employees/outsiders. The controls relate to establishing appropriate physical security and access control measures for IT facilities, including off-site use of information devices in conformance with the general security policy

3.12. Logical Access Controls

Logical access controls are implemented to ensure that access to systems, data and programs is restricted to authorized users so as to safeguard information against unauthorized use, disclosure or modification, damage or loss. The key factors considered in designing logical access controls include confidentiality and privacy requirements, authorization, authentication and incident handling, reporting and follow-up, virus prevention and detection, firewalls, centralized security administration, user training and tools for monitoring compliance, intrusion testing and reporting.

3.13. SDLC (System Development Life Cycle) Controls

These are functions and activities generally performed manually that control the development of application systems, either through in-house design and programming or package purchase. The first control requirement is system development standards.

3.14. Business Continuity Planning (BCP) Controls

These controls are related to having an operational and tested IT continuity plan, which is in line with the overall business continuity plan, and its related business requirements so as to make sure IT services are available as required and to ensure a minimum impact on business in the event of a major disruption. The controls include criticality classification, alternative procedures, back-up and recovery

3.15. Application Control Techniques

These include the programmatic routines within the application program code. The objective of application controls is to ensure that data remains complete, accurate and valid during its input, update and storage. The specific controls could include form design, source document controls, input, processing and output controls, media identification, movement and library management, data back-up and recovery, authentication and integrity, legal and regulatory requirements.

3.16. User Controls: The following Table lists the user controls that are to be exercised for system effectiveness and efficiency. **User Controls and Audit Trail**

Scope	**Audit Trail**	
	Accounting	**Operations**
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 resources in restricted ways.	➢ Authentication of the users of the system(identity) ➢ Resources and Action privileges requested/ provided/ denied. ➢ Number of sign-on attempts ➢ In case of digital signatures for authentication audit trail includes- Registration of public keys, Notification of key compromises.	➢ Resource usage from log-on to log-out time.
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.	➢ Originator of the data/instruction, ➢ time and date the data/instruction entered, ➢ physical device used by the user, ➢ type of data/instruction and output processed.	➢ Number of read errors, ➢ Number of keying errors, ➢ Frequency of instruction usage and time-taken to process an instruction.
Processing Controls		
➢ Responsible for computing, sorting, classifying and summarizing data. ➢ It maintains the chronology of events from the time data is received from input or communication.	➢ To trace and replicate the processing performed on a data item. ➢ Triggered transactions to monitor input data entry, ➢ Intermediate results and output data values.	➢ A comprehensive log on resource consumption data with respect to hardware(processor time, peripherals, memory, communication Software
Output Controls		
➢ To provide functions that determine the data content available to users, ➢ Data format, timeliness of data and how data is prepared and routed to users.	➢ It shows what output was presented to users, who received the output, when the output was received and what action were taken with the output.	➢ Maintains the record of resources consumed graphs, images, report pages, printing time and display rate.

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.	➢ A unique time stamp to all transactions, before and after images of the data item on which a transaction is applied and any modifications or corrections to audit trail transactions accommodating the changes that occur within an application system.	➢ To maintain a chronology of events that consumes resources of the data base. The response time on the queries made on the data base.

These aforementioned Controls are discussed as follows:

1) **Boundary Controls:** The major controls of the boundary system are the access control mechanisms. Access controls mechanism links the authentic users to the authorized resources, they are permitted to access. The access control mechanism has three steps of identification, authentication and authorization with respect to the access control policy implemented
   Major Boundary Control techniques are given as follows:
   a) **Cryptography:** It deals with programs for transforming data into cipher text that are meaningless to anyone, who does not possess the authentication to access the respective system resource or file. 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, substitution and product cipher.

   b) **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.

   c) **Personal Identification Numbers (PIN):** PIN is similar to a password assigned to a user by an institution a random number stored in its database independent to a user identification details, or a customer selected number. Hence, a PIN may be exposed to vulnerabilities while issuance or delivery, validation, transmission and storage.

   d) **Identification Cards:** Identification cards are used to store information required in an authentication process. These cards are to be controlled through the application for a card, preparation of the card, issue, use and card return or card termination phases.

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

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

3) **Processing Controls:** Data processing controls perform validation checks to identify errors during processing of data. They are required to ensure both the completeness and the accuracy of data being processed. Normally, the processing controls are enforced through database management system that stores the data.

4) **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. Output controls have to be enforced both in a batch- processing environment as well as in an online environment. Detailed discussion on the same is given in Chapter 6 of the Study Material.

5) **Database Controls:** Protecting the integrity of a database when application software acts as an interface to interact between the user and the database, are called update controls and report controls. Major update controls are given as follows:
   a) **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 updation, insertion or deletion of records in the master file with respect to the transaction records. If errors, in this stage are overlooked, it leads to corruption of the critical data.

   b) **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.

   c) **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.

   d) **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.

6) **Major Report controls are given as follows:**
   a) **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. Periodic monitoring of these internal tables by means of manual check or by calculating a control total is mandatory.

   b) **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.

   c) **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.

   d) **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. Recovery strategies involve roll-forward (current state database from a previous version) or the roll- back (previous state database from the current version) methods.

CHAPTER-3
PROTECTION OF SYSTEM

3.13. Controls over Data Integrity and Security

The classification of information and documents is essential if one has to differentiate between that which is of little (if any) value, and that which is highly sensitive and confidential. When data is stored, whether received, created or amended, it should always be classified into an appropriate sensitivity level. For many organizations, a simple 5 scale grade will suffice as follows:

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.

3.14. Data Integrity.

The primary objective of data integrity control techniques is to prevent, detect, and correct errors in transactions as they flow through various stages of a specific date processing program. Data integrity controls protect data from accidental or malicious alteration or destruction and provide assurance to the user that the information meets expectations about its quality and integrity. Data integrity is a reflection of the accuracy, correctness, validity, and currency of the data. The primary objective in ensuring integrity is to protect the data against erroneous input from authorized users.

CHAPTER-3
PROTECTION OF SYSTEM

Data Integrity Controls

Threats and Risks	Controls
Source Data Control	
Invalid, incomplete, or inaccurate source data input	Forms design; sequentially pre- numbered forms, turnaround documents; storage of documents, review for appropriate authorization; segregation of duties, visual scanning; check-digit verification; and key verification.
Input Validation Routines	
Invalid or inaccurate data in computer-processed transaction files	As transaction files are processed, edit programs check key data fields using these edit checks, sequence, field, sign, validity, limit, range, reasonableness, redundant data, and capacity checks. Enter exceptions in an error log; investigate, correct, and resubmit them on time; re-edit them, and prepare a summary error report.
Online Data Entry Controls	
Invalid or inaccurate transaction input entered through on-line terminals	Field, limit, range, reasonableness, sign, validity, and redundant data checks; user-ids and passwords; compatibility tests; automatic system date entry; prompting operators during data entry, pre- formatting, completeness test; closed-loop verification; a transaction log maintained by the system; clear error messages, and data retention sufficient to satisfy legal requirements.
Data Processing and Storage Controls	
Inaccurate or incomplete data in computer-processed master files	Policies and procedures (governing the activities of data processing and storage personnel; data security and confidentiality, audit trails, and confidentiality agreements); monitoring and expediting data entry by data control personnel; reconciliation of system updates with control accounts or reports; reconciliation of database totals with externally maintained totals; exception reporting, data currency checks, default values, data marching; data security (data library and librarian, backup copies of data files stored at a secure off-site location, protection against conditions that could harm stored data); use of file labels and write protection mechanisms, database protection mechanisms (data wise administrators, data dictionaries, and concurrent update controls); and data conversion controls.
Output Controls	
Inaccurate or incomplete computer output	Procedures to ensure that system outputs conform to the organization's integrity objectives, policies, and standards, visual review of computer output, reconciliation of batch totals; proper distribution of output; confidential outputs being delivered are protected from unauthorized access, modification, and misrouting; sensitive or confidential out-put stored in a secure area; review of user of computer output for completeness and accuracy, shredding of confidential output no longer needed; error and exception reports.
Data Transmission Controls	
Unauthorized	Monitor network to detect week points, backup components, design network

access to data being transmitted or to the system itself; system failures; errors in data transmission`	to handle peak processing, multiple communication paths between network components, preventive maintenance, data encryption, routing verification (header labels, mutual authentication schemes, callback system parity checking; and message acknowledgement procedures

6) Data Integrity Policies

Major data integrity policies are given as under:

a) Virus-Signature Updating: Virus signatures must be updated automatically when they are made available from the vendor through enabling of automatic updates.

b) Software Testing: All software must be tested in a suitable test environment before installation on production systems.

c) Division of Environments: The division of environments into Development, Test, and Production is required for critical systems.

d) Offsite Backup Storage: Backups older than one month must be sent offsite for permanent storage.

e) Quarter-End and Year-End Backups: Quarter-end and year-end backups must be done separately from the normal schedule, for accounting purposes

f) Disaster Recovery: A comprehensive disaster-recovery plan must be used to ensure continuity of the corporate business in the event of an outage.

3.15. Data Security

Data security encompasses the 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, and security of the hardware and software controls, physical security over the user, and organizational policies. An IS auditor is responsible to evaluate the following while reviewing the adequacy of data security controls:

1) Who is responsible for the accuracy of the data?
2) Who is permitted to update data?
3) Who is permitted to read and use the data?
4) Who is responsible for determining who can read and update the data?
5) Who controls the security of the data?
6) If the IS system is outsourced, what security controls and protection mechanism does the vendor have in place to secure and protect data?
7) Contractually, what penalties or remedies are in place to protect the tangible and intangible values of the information?
8) The disclosure of sensitive information is a serious concern to the organization and is mandatory on the auditor's list of priorities.

3.16. Logical Access Controls

Logical access controls are the system-based mechanisms used to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted. Assessing logical access controls involves evaluating the following critical procedures:

1) Logical access controls restrict users to authorized transactions and functions.
2) There are logical controls over network access.
3) There are controls implemented to protect the integrity of the application and the confidence of the public when the public accesses the system.

CHAPTER-3
PROTECTION OF SYSTEM

3.17. Logical Access Paths

These are given as follows:

1) **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.
2) **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.
3) **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.

3.18. Logical Access Issues and Exposures

Controls that reduce the risk of misuse (intentional or unintentional), theft, alteration or destruction should be used to protect unauthorized and unnecessary access to computer files. Restricting and monitoring computer operator activities in a batch-processing environment provide this control.
Access control mechanisms should be applied not only to computer operators but also to end users programmers, security administrators, management or any other authorized user/s. Access control mechanisms should provide security to the following applications:

Access control software, Application software, Data, Data dictionary/directory, Dial-up lines, Libraries, Logging files, Operating systems Password library, Procedure libraries, Spool queues, System software, Tape files, Telecommunication lines, Temporary disk files, and Utilities.

3.19. Issues and Revelations related to Logical Access

Compromise or absence of logical access controls in the organization's may result in potential losses due to exposures that may lead to the total shutdown of the computer functions. Intentional or accidental exposure of logical access control encourage technical exposures and computer crimes. These are given as follows:

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

   b) **Bombs:** 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. However, these programs cannot infect other programs. Since, these programs do not circulate by infecting other programs, chances of a widespread epidemic are relatively low.
      Bombs are generally of two types, which are given as follows:
      i) **Time Bomb:** Computer time bomb causes a perverse activity, such as, disruption of computer system, modifications, or destructions of stored information etc. on a particular date and time for which it has been developed. The computer clock initiates it.

      ii) **Logic Bomb:** They resemble time bombs in their destruction activity. Logic bombs are activated by combination of events. For example, a code like; "If a file named DELETENOT is deleted then destroy the memory contents by writing ones

c) **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:

i) Change or steal the password or
ii) May modify records in protected files or
iii) May allow illicit users to use the systems.

Trojan Horses hide in a host and generally do not damage the host program. Trojans cannot copy themselves to other software in the same or other systems. Christmas Card is a well-known example of Trojan.

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

e) **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.

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

g) 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.

2) **Computer Crime Exposures**: Computers can be utilized both constructively and destructively. Computer systems are used to steal money, goods, software or corporate information. Crimes are also committed when false data or unauthorized transaction is made. Computer crimes generally result in Loss of customers, embarrassment to management and legal actions against the organizations. These are given as follows:

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

b) **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.

c) **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.

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

e) **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.

f) **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.

g) **Logical access violators** are often the same people who exploit physical exposures, although the skills needed to exploit logical exposures are more technical and complex. These are:

i) **Hackers:** Hackers try their best to overcome restrictions to prove their ability. Ethical hackers most likely never try to misuse the computer intentionally;
ii) **Employees** (authorized or unauthorized);
iii) **IS Personnel:** They have easiest to access to computerized information since they come across to information during discharging their duties. Segregation of duties and supervision help to reduce the logical access violations;
iv) End Users;
v) **Former Employees:** should be cautious of former employees who have left the organization on unfavorable terms.
vi) Interested or Educated Outsiders;
vii) Competitors;
viii) Foreigners;
ix) Organized criminals;
x) Crackers;
xi) Part-time and Temporary Personnel;
xii) Vendors and consultants; and
xiii) Accidental Ignorant – Violation done unknowingly.

h) **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 s/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.

3) **Asynchronous Attacks:** They occur in many environments where data can be moved asynchronously across telecommunication lines. Numerous transmissions must wait for the clearance of the line before data being transmitted. Data that is waiting to be transmitted are liable to unauthorized access called asynchronous attack. These attacks are hard to detect because they are usually very small pin like insertions. There are many forms of asynchronous attacks, some of them are given as follows:

a) **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.

b) **Wire-tapping:** This involves spying on information being transmitted over telecommunication network.

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

d) **Shutting Down of the Computer/Denial of Service:** This is initiated through terminals or microcomputers that are directly or indirectly connected to the computer. Individuals, who know the high-level systems log on-ID initiate shutting down process. The security measure will function effectively if there are appropriate access controls on the logging on through a telecommunication network. When overloading happens some systems have been proved to

be vulnerable to shutting themselves. Hackers use this technique to shut down computer systems over the Internet.

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

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

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

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

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

vi) In order to prevent the unauthorized users access to the system, there should be proper control mechanisms over system documentation and manuals.

vii) 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.

viii) 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.

4) Physical and Environmental Protection: Physical security and environmental security are the measures taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment. Assessing physical and environmental protection involves evaluating the following critical procedures :

a) Adequate physical security controls have been implemented and are commensurate with the risks of physical damage or access.

b) Data is protected from interception.

c) Mobile and portable systems are protected.

3.17. Logical Access Control across the System

Logical access controls serve as one of the means of information security. The purpose of logical access controls is to restrict access to information assets/resources. They are expected to provide access to information resources on a need to know and need to do basis using principle of least privileges. Logical access controls is all about protection of these assets wherever they reside.

Logical Access Controls

User Access Management	
User registration	Information about every user is documented. The following questions are to be answered: Why is the user granted the access? Has the data owner approved the access? Has the user accepted the responsibility? The de-registration process is also equally important.
User registration	Information about every user is documented. The following questions are to be answered: Why is the user granted the access? Has the data owner approved the access? Has the user accepted the responsibility? The de-registration process is also equally important.
Privilege Management	Access privileges are to be aligned with job requirements and responsibilities. For example, an operator at the order counter shall have direct access to order processing activity of the application system. S/he will be provided higher access privileges than others. However, misuse of such privileges could endanger the organization's information security. These

User Password Management	Passwords are usually the default screening point for access to systems. Allocations, storage, revocation, and reissue of password are password management functions. Educating users is a critical component about passwords, and making them responsible for their password.
Review of user access right	A user's need for accessing information changes with time and requires a periodic review of access rights to check anomalies in the user's current job profile, and the privileges granted earlier.
User responsibilities	
Password use	Mandatory use of strong passwords to maintain confidentiality.
Unattended user equipment	Users should ensure that none of the equipment under their responsibility is ever left unprotected. They should also secure their PCs with a password, and should not leave it accessible to others.
Network access control	
Policy on use of Network	An enterprise wide policy applicable to internet service requirements aligned with the business need for using the Internet services is the first step. Selection of appropriate services and approval to access them should be part of this policy.
Enforced Path	Based on risk assessment, it is necessary to specify the exact path or route connecting the networks; e.g., internet access by employees will be routed through a firewall and proxy.
Segregation of Network	The traffic between networks should be restricted, based on identification of source and authentication access policies implemented across the enterprise network facility
Security of Network Services	The techniques of authentication and authorization policy should be implemented across the organization’s network.
Operating system access control	
Automated Terminal	This will help to ensure that a particular session could only be initiated from a particular location or computer terminal.
User Identification and authentication	The users must be identified and authenticated in a foolproof manner. Depending on risk assessment, more stringent methods like Biometric Authentication or Cryptographic means like Digital Certificates should be employed.
Password Management System	An operating system could enforce selection of good passwords. Internal storage of password should use one-way hashing algorithms and the password file should not be accessible to users.
Use of System utilities	System utilities are the programs that help to manage critical functions of the operating system e.g. addition or deletion of users. Obviously, this utility should not be accessible to a general user. Use and access to these utilities should be strictly controlled and logged.
Dures alarm to safeguard user	If users are forced to execute some instruction under threat, the system should provide a means to alert the authorities

Terminal Time out	Log out the user if the terminal is inactive for a defined period. This will prevent misuse in absence of the legitimate user.
Limitation of Connection	Define the available time slot. Do not allow any transaction beyond this time period. For example, no computer access after 8.00 p.m. and before 8.00 a.m.—or on a Saturday or Sunday.
Application and monitoring system access control	
Information access restriction	The access to information is prevented by application specific menu interfaces, which limit access to system function. A user is allowed to access only to those items, s/he is authorized to access. Controls are implemented on the access rights of users, For example, read, write, delete, and execute. And ensure that sensitive output is sent only to authorized terminals and locations
Sensitive System isolation	Based on the critical constitution of a system in an enterprise, it may even be necessary to run the system in an isolated environment.
Event Logging	In Computer systems, it is easy and viable to maintain extensive logs for all types of events. It is necessary to review if logging is enabled and the logs are archived properly.
Monitor System use	Based on the risk assessment, a constant monitoring of some critical systems is essential. Define the details of types of accesses, operations, events and alerts that will be monitored. The extent of detail and the frequency of the review would be based on criticality of operation and risk factors. The log files are to be reviewed periodically and attention should be given to any gaps in these logs.
Clock Synchronization	Event logs maintained across an enterprise network plays a significant role in correlating an event and generating report on it. Hence, the need for synchronizing clock time across the network as per a standard time is mandatory.
Mobile Computing	Theft of data carried on the disk drives of portable computers is a high risk factor. Both physical and logical access to these systems is critical. Information is to be encrypted and access identifications like fingerprint, eye-iris, and smart cards are necessary security features.

3.18. Physical Access Controls

This section enumerates the losses that are incurred as result of perpetrations, accidental or intentional violation of access paths. In addition, the section emphasizes on physical access issues and exposures along with appropriate physical access controls. Afterwards, various access control mechanisms are also discussed.

CHAPTER-3
PROTECTION OF SYSTEM

1) Physical Access Issues and Exposures

Physical access controls are designed to protect the organization from unauthorized access or in other words, to prevent illegal entry. These controls should be designed in such a way that it allows access only to authorized persons.

The following points elaborate the results due to accidental or intentional violation of the access paths:

- **a)** Abuse of data processing resources,
- **b)** Blackmail,
- **c)** Embezzlement,
- **d)** Damage, vandalism or theft to equipments or documents,
- **e)** Public disclosure of sensitive information, and
- **f)** Unauthorized entry.

2) Possible perpetrators:

Perpetrations may be because of employees, who are:

- **a)** Accidental ignorant-someone who outrageously violates rules,
- **b)** Addicted to a substance or gambling,
- **c)** Discontented,
- **d)** Experiencing financial or emotional problems,
- **e)** Former employee,
- **f)** Interested or informed outsiders, such as competitors, thieves, organized crime and hackers,
- **g)** Notified for their termination,
- **h)** On strike, and
- **i)** Threatened by disciplinary action or dismissal.

3) Techniqies of Physical Access Controls

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

- **a) Locks on Doors:** These are given as follows:
  - **i) Cipher locks** (Combination Door Locks) - The cipher lock consists of a pushbutton panel that is mounted near the door outside of a secured area. There are ten numbered buttons on the panel. To enter, a person presses a four digit number, and the door will unlock for a predetermined period of time, usually ten to thirty seconds.
  - **ii) 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 be duplicated.
  - **iii) 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. The reader device upon reading the special code that is internally stored within the card activates the door locking mechanism
- **b) Physical Identification Medium:** These are discussed below:
  - **i) 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/her entry will be matched with the PIN number available in the security database.
  - **ii) Plastic Cards:** These cards are used for identification purposes. Customers should safeguard their card so that it does not fall into unauthorized hands.
  - **iii) 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.

c) Logging on Facilities: These are given as under:

i) 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.

ii) 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.

d) Other means of Controlling Physical Access: Other important means of controlling physical access are given as follows:

i) Video Cameras: Cameras should be placed at specific locations and monitored by security guards. Refined video cameras can be activated by motion. The video supervision recording must be retained for possible future play back.

ii) Security Guards: Extra security can be provided by appointing guards aided with CCTV feeds. Guards supplied by an external agency should be made to sign a bond to protect the organization from loss.

iii) Controlled Visitor Access: A responsible employee should escort all visitors. Visitors may be friends, maintenance personnel, computer vendors, consultants and external auditors.

iv) Bonded Personnel: All service contract personnel, such as cleaning people and off- site storage services, should be asked to sign a bond. This may not be a measure to improve physical security but to a certain extent can limit the financial exposure of the organization.

v) Dead Man Doors: These systems encompasses are 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.

vi) 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.

vii) Computer Terminal Locks: These locks ensure that the device to the desk is not turned on or disengaged by unauthorized persons.

viii) 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.

ix) Alarm System: Illegal entry can be avoided by linking alarm system to inactive entry point and the reverse flows of enter or exit only doors, so as to avoid illegal entry. Security personnel should be able to hear the alarm when activated.

x) Perimeter Fencing: Fencing at boundary of the facility may also enhance the security mechanism.

xi) **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

xii) **Secured Report/Document** Distribution Cart: Secured carts, such as mail carts, must be covered and locked and should always be attended.

3.19. Environmental Controls

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

1) **Hardware and Media:** Includes Computing Equipment, Communication equipment, and Storage Media.

2) **Information Systems Supporting Infrastructure or Facilities:** This typically includes the following:
   a) Physical Premises, like Computer Rooms, Cabins, Server Rooms, Data Centre premises, Printer Rooms, Remote facilities, Staging Room, and Storage Areas,
   b) Communication Closets,
   c) Cabling ducts,
   d) Power Source, and
   e) Heating, Ventilation and Air Conditioning (HVAC).

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

4) **Supplies:** The third 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.

5) **People:** The 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). Training of employees and other stake holders on control procedures is a critical component.

3.20. Environmental Issues and Exposures

1) Environmental exposures are primarily due to elements of nature. However, with proper controls, exposures can be reduced. Common occurrences are,
2) Fire, Natural disasters-earthquake, volcano, hurricane, tornado,
3) Power spike,
4) Air conditioning failure,
5) Electrical shock,
6) Equipment failure,
7) Water damage/flooding-even with facilities located on upper floors of high buildings. Water damage is a risk, usually from broken water pipes, and
8) Bomb threat/attack

Other environmental issues and revelations include the following

1) Is the power supply to the compiler equipment properly controlled so as to ensure that it remains within the manufacturer's specification?
2) Are the air conditioning, humidity and ventilation control systems protected against the effects of electricity using static rug or anti-static spray?
3) Is consumption of food, beverage and tobacco products prohibited, by policy, around computer equipment?
4) Are backup media protected from damage due to variation in temperatures or are they guarded against strong magnetic fields and water damage?
5) Is the computer equipment kept free from dust, smoke and other particulate matter?

CHAPTER-3
PROTECTION OF SYSTEM

Controls for Environmental Exposures

These are given as follows:

1) **Water Detectors:** In the computer room, even if the room is on high floor, water detectors should be placed under the raised floor and near drain holes. Water detectors should be present near any unattended equipment storage facilities. When activated, the detectors should produce an audible alarm that can be heard by security and control personnel. For easy identification and reach, the location of the water detectors should be marked on the raised computer room floor. A remedial action must be initiated on hearing the alarm by notifying the specific individuals and allotting the responsibility for investigating the cause. Other staff should be made aware of the risk of a possible electrocution.

2) **Hand-Held Fire Extinguishers:** Fire extinguishers should be in calculated locations throughout the area. They should be tagged for inspection and inspected at least annually.

3) **Manual Fire Alarms:** Hand-pull fire alarms should be purposefully placed throughout the facility. The resulting audible alarm should be linked to a monitored guard station.

4) **Smoke Detectors:** Smoke detectors are positioned at places above and below the ceiling tiles. Upon activation, these detectors should produce an audible alarm and must be linked to a monitored station (for example, a fire station) Fire repression systems should be supplemented and not replaced by smoke detectors.

5) **Fire Suppression Systems:** These alarms are activated when extensive heat is generated due to fire. Like smoke alarms they are designed to produce audible alarms when activated and should be regularly monitored. In addition to precautionary measures, the system should be segmented in to zones so that fire in one part of a large facility does not activate the entire system.
   The fire suppression techniques vary depending upon the situation but it is usually one of the following:
   a) **Dry-Pipe sprinkling systems:** These are typically referred to as sprinkler systems. These pipes remain dry and upon activation by the electronic fire alarm water is sent through the pipe. Dry pipe systems have the advantage that any failure in the pipe will not result in water leaking into sensitive equipment.

   b) **Water based systems:** These also function similar to the sprinkler systems. These systems are effective but also are unpopular because they damage equipment and property. Changed systems are more reliable but the disadvantage is that in the case of leakage or breakage of pipes facilities are exposed to extensive water damage,

   c) **Halon:** An alternative method can be usage of Halon. Halon systems contain pressurized halon gases that remove oxygen from the air. Halon is preferred to others because of its inertness and it does not damage equipment like water does. There should be an audible alarm and brief delay before discharge to permit personnel time to evacuate the area or to override and disconnect the system in case of false alarm. The drawback is, since halon adversely affects the ozone layer, its usage is banned; alternative to Halon is effective.

6) **Strategically Locating the Computer Room:** To reduce the risk of flooding, the computer room should not be located in the basement or ground floor of a multi-storey building. Studies reveal that the computer room located in the top floors is less prone to the risk of fire, smoke and water.

7) **Regular Inspection by Fire Department:** An annual inspection by the fire department should be carried out to ensure that all fire detection systems act in accordance with building codes. Also, the fire department should be notified of the location of the computer room, so it should be equipped with tools and appropriate electrical fires.

8) **Fireproof Walls**, Floors and Ceilings surrounding the Computer Room: Information processing facility should be surrounded by walls that should control or block fire from spreading. The surrounding walls should have at least three hour fire resistance rating.

9) **Electrical Surge Protectors:** The risk of damage due to power spikes can be reduced to a great extent using electrical surge protectors. The incoming current is measured by the voltage regulator and depending upon the intensity of electric current regulators can increase or decrease the charge of electricity and ensures that a consistent current passes through. Such protectors are typically built into the Uninterruptible Power System (UPS).

10) **Uninterruptible Power System (UPS)/Generator:** A UPS system consists of a battery or gasoline powered generator that interfaces between the main electrical power entering the facility and the electrical power supplied to the computer. The system typically cleanses the power to ensure wattage into the computer is consistent. In case of a power failure, the UPS provides the back up by providing electrical power from the battery to the computer for a certain span of time. Depending on the sophistication of the UPS, electrical power supply could continue to flow for days or for just a few minutes to permit an orderly computer shutdown.

11) **Power Leads from Two Substations:** Electrical power lines that are exposed to many environmental dangers such as waters fire, lightning, cutting due to careless digging etc. To avoid these types of events, redundant power links should feed into the facility. Interruption of one power supply does not adversely affect electrical supply.

12) **Emergency Power-Off Switch:** When there arises a necessity of immediate power shut down during situations like a computer room fire or an emergency evacuation, an emergency power-off switch at the strategic locations would serve the purpose. They should be easily accessible and yet secured from unauthorized people.

13) **Wiring Placed in Electrical Panels and Conduit:** Electrical fires are always a risk. To reduce the risk of such a fire occurring and spreading, wiring should be placed in the fire resistant panels and conduit. This conduit generally lies under the fire-resistant raised floor in the computer room.

14) **Prohibitions against Eating, Drinking and Smoking within the Information Processing Facility:** These activities should be prohibited from the information processing facility. This prohibition should be clear, e.g. a sign on the entry door.

15) **Fire Resistant Office Materials:** The materials used in the information processing facility such as Wastebaskets, curtains, desks, cabinets and other general office materials should be fire proof.

16) **Documented and Tested Emergency Evacuation Plans:** Relocation plans should emphasize human safety, but should not leave information processing facilities physically unsecured. Procedures should exist for a controlled shutdown of the computer in an emergency situation. In all circumstances saving human life should be given paramount importance.

3.21. Cyber Frauds

Cyber Fraud shall mean frauds committed by use of technology. Cyber fraud refers to any type of deliberate deception for unfair or unlawful gain that occurs online. The most common form is online credit card theft. Other common forms may be monetary cyber frauds include non-delivery of paid products purchased through online auction etc. With the advancements in the technology, cyber frauds are also increasing day-by-day across the world.

1) Major reasons behind the rise of frauds are:

- **a)** Failure of internal control system
- **b)** Failure of organizations to update themselves to new set of risk, and
- **c)** Smart fraudsters: These are people who are able to target the weaknesses in system, lacunae's in internal controls, even before the organization realizes that such gaps are there.

On the basis of the functionality, these are of two types:

a) Pure Cyber Frauds: Frauds, which exists only in cyber world. They are borne out of use of technology. For example: Website hacking.

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

The fraudster may be from within the organization or from outside the organization. But, it has been observed that most of cyber frauds include more than one individual and one of the team members in many cases is a person within the organization.

2) Types of Cyber Attacks: Each of the above is discussed as follows:

a) 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.

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

c) 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;

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

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

f) Others: These are given as follows

i) Cracking: Crackers are hackers with malicious intentions.

ii) Eavesdropping (Spying): It refers to the listening of the private voice or data transmissions, often using a wiretap.

iii) E-mail Forgery: Sending e-mail messages that look as if someone else sent it is termed as E-mail forgery.

iv) E-mail Threats: Sending a threatening message to try and get recipient to do something that would make it possible to defraud him is termed as E-mail threats

v) Scavenging (Searching): This is gaining access to confidential information by searching corporate records.

2) Impact of Cyber Frauds on Enterprises

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

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

b) 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. These entities need to ensure that such data is well protected. In case a fraudster breaks into such database, it adds to the liability of entities.

c) **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. There have been instances where share prices of such companies went down, as the news of such attach percolated to the market.

d) **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.

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

3) Techniques to Commit Cyber Frauds

Following are the major techniques to commit cyber frauds:

a) **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.

b) **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.

c) **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.

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

e) **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.

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

g) **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.

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

i) **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.

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

k) **Round Down:** Computer rounds down all interest calculations to 2 decimal places.

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

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