CHAPTER 3

CONTROL OBJECTIVES

⇨ CONTROL

- ☞ Defines as set of policies, procedures, practices and organizational structures implements to **REDUCE RISKS TO ASSETS.**
- ☞ For e.g.: any visitor to the computer centre should be escorted by a staff of the organization, restriction access to SW thorough a login ID/Password.
- ☞ Control objectives:
  Desired outcome to be attained by implementing a control procedure.
  For e.g. Data confidentially = encryption.

⇨ NEED FOR CONTROL AND AUDIT OF INFORMATION SYSTEMS

Factors influencing an organization toward control and audit of computers and the impact of the information systems audit function on organizations are as follow

I. Organizational Costs of Data Loss :
   - ✳ Data is a critical resource of an organization for its present and future process and
   - ✳ its ability to adapt and survive in a changing environment.

II. Incorrect Decision Making:
   - ✳ Management and operational controls taken by managers involve detection, investigations and correction of out-of-control processes.
   - ✳ These high level decisions require accurate data to make quality decision rules.

III. Costs of Computer Abuse:
   - ✳ Unauthorized access to computer systems,
   - ✳ computer viruses,
   - ✳ unauthorized physical access to computer facilities and
   - ✳ Unauthorized copies of sensitive data can lead to destruction of assets (hardware, software, documentation etc.)

IV. Value of Computer Hardware, Software and Personnel: These are critical resources of an organization which has a credible impact on its infrastructure and business competitiveness.

V. High Costs of Computer Error: In a computerized enterprise environment where many critical business processes are performed a data error during entry or process would cause great damage.

VI. Maintenance of Privacy:
   - ✳ Today data collected in a business process contains details about an individual on medical, educational, employment, esidence etc.
   - ✳ These data were also collected before computers but now there is a fear that privacy has eroded beyond acceptable levels.

VII. Controlled evolution of computer Use :
   - ✳ Technology use and reliability of complex computer systems cannot be guaranteed and

- ✳ The consequences of using unreliable systems can be destructive.

VIII. Information Systems Auditing:
- ✳ It is the process of attesting objectives (those of the external auditor)
- ✳ that focus on asset safeguarding and data integrity, and management objectives (those of the internal auditor)
- ✳ That includes not only attest objectives but also effectiveness and efficiency objectives.

IX. Asset Safeguarding Objectives: The information system assets (hardware, software, data files etc.) must be protected by a system of internal controls from unauthorized access.

X. Data Integrity Objectives:
- ✳ It is a fundamental attribute of IS Auditing.
- ✳ The importance to maintain integrity of data of an organization depends on the
  - Value of information,
  - The extent of access to the information and
  - The value of data to the business from the perspective of the decision maker,
  - Competition and
  - The market environment.

XI. System Effectiveness Objectives:
- ✳ Effectiveness of a system is evaluated by auditing the characteristics and
- ✳ Objective of the system to meet substantial user requirements.

XII. System Efficiency Objectives : To optimize the use of various information system resources (machine time, peripherals, system software and labour) along with the impact on its computing environment.

⇨ EFFECT OF COMPUTERS ON INTERNAL CONTROLS

The internal controls within an enterprise in a computerized environment the major areas of impact with the goal of asset safeguarding, data integrity, system efficiency and effectiveness are discussed below.

I. Personnel : Whether or not staffs are trustworthy, if they know what they are doing and, if they have the appropriate skills and training to carry out their jobs to a competent standard.

II. Segregation of duties:
- ✳ A key control in an information system.
- ✳ Segregation basically means that the stages in the processing of a transaction are split between different people, such that one person cannot process a transaction through from start to finish.
- ✳ The various stages in the transaction cycle are spread between two or more individuals.
- ✳ However, in a computerized system, the auditor should also be concerned with the **SEGREGATION OF DUTIES WITHIN THE IT DEPARTMENT**.
- ✳ IT staff may also be in a position to alter transaction data or even the financial applications which process the transactions.

- ✳ This gives them the knowledge and means to alter data, all they would then require is a motive.

III. Authorization procedures:
- ✳ To ensure that transactions are approved.
- ✳ In some on-line transaction systems written evidence of individual data entry authorization, e.g. a supervisor's signature, may be replaced by computerized authorization controls such as automated controls written into the computer programs (e.g. programmed credit limit approvals)

IV. Record keeping: the controls over the protection and storage of documents, transaction details, and audit trails etc.

V. Access to assets and records:
- ✳ In the past manual systems could be protected from unauthorized access through the use of locked doors and filing cabinets.
- ✳ Computerized financial systems have not changed the need to protect the data.
- ✳ A client's financial data and computer programs are vulnerable to unauthorized amendment at the computer or from remote locations.
- ✳ The nature and types of control available have changed to address these new risks.

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

VII. 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.

⇨ IMPACT OF COMPUTERISATION AUDIT
1. Changes in Evidence Collection
2. Changes in Evidence Evaluation

1. CHANGES TO EVIDENCE COLLECTION
- ✳ Changes in the audit trail say the existence of an audit trail is a key financial audit requirement, since without an audit trail, the financial auditor may have extreme difficulty in gathering sufficient, appropriate audit evidence to validate the figures in the client's accounts.
- ✳ The performance of evidence collection and understanding the reliability of controls involves issues like
  - ☞ Data retention and storage
  - ☞ Absence of input documents
  - ☞ Lack of a visible audit trail
  - ☞ Lack of visible output
  - ☞ Audit evidence
  - ☞ Legal issues

- **Data retention and storage:**
  - In computerized system data retention is primarily done in electronic form on storage devices.
  - It is difficult for auditor to read data directly from devices.
  - Audit need to use specialized techniques & software to interrogate the data & check the audit trail and validity of retained data.
- **Absence of input documents:** Transaction data may be entered in to computer directly **WITHOUT THE PRESENCE OF SUPPORTING DOCUMENTATION**
- **Lack of a visible audit trail:**
  - The audit trails in some computer systems may exist for only a short period of time.
  - The absence of an audit trail will make the auditor's job very difficult and may call for an audit approach which involves **AUDITING AROUND THE COMPUTER SYSTEM** by seeking other sources of evidence to provide assurance that the computer input has been correctly processed and output.
- **Lack of visible output:**
  - The result of transaction processing MAY NOT PRODUCE A HARD COPY OF OUTPUT, i.e. a printed record.
  - In absence of physical output it may be necessary for the auditor to directly access the electronic data retained on the clients computer.]
  - This is normally achieved by having client provide a computer terminal and being granted- READ ACCESS to the required data files.
- **Audit evidence:** Certain transaction may be GENERATED AUTOMATICALLY by the computer system.
- **Legal issues:** Advent of information system also causes impact on legal issues

2. Changes in Evidence Evaluation:
   - Evaluation of audit trail and evidence is to trace consequences of control strength and weakness through the system.
   - The evidence evaluation function of information systems leads to identify periodic and deterministic errors.
     - System generated transactions :
       - Financial systems may have the ability to initiate, approve and record financial transactions.
       - This is likely to become increasingly common as more organizations begin to install expert systems and electronic data interchange (EDI) trading systems.
       - Automated transaction processing systems can cause the auditor problems.
       - For example when gaining assurance that a transaction was properly authorized or in accordance with delegated authorities.
       - The auditor may need to look at the application's programming to determine if the programmed levels of authority are appropriate.

- Automated transaction generation systems are frequently used in 'just in time' (JIT) inventory and stock control systems.

- Systematic Error:
  - Computers are designed to carry out processing on a consistent basis.
  - Given the same inputs and programming, they invariably produce the same output.
  - This consistency can be viewed in both a positive and a negative manner

⇨ THE IS AUDIT PROCESS

The IS audit process includes evaluation of control, logic and operation of Information System. Specially, the IS audit process includes the following:

- Assessment of **INTERNAL CONTROLS** within the IS environment to assure validity, reliability, and security information.
- Assessment of the **EFFICIENCY AND EFFECTIVENESS** of the IS environment in economic terms.

- **Responsibility of IS Auditor:**

  The set of skills that is generally expected of an IS auditor include:
  - Sound knowledge of business operations, practices and compliance requirements,
  - Should possess the requisite professional technical qualification and certifications,
  - An good understanding of information Risks and Controls,
  - Knowledge of IT strategies, policy and procedure controls,
  - Ability to understand technical and manual controls relating to business continuity, and
  - Good knowledge of Professional Standards and Best practices of IT controls and security.

- **Functions of IS Auditor**

  IT auditors review risks relating to IT systems and processes, some of them are:
  - Inadequate information security (e.g. missing or out of date antivirus controls, open computer ports, open systems without password or weak passwords etc.)
  - Inefficient use of corporate resources, or poor governance (e.g. huge spending on unnecessary IT projects like printing resources, storage devices, high power servers and workstations etc.)
  - Ineffective IT strategies, policies and practices (including a lack of policies for use of Information and Communication Technology (ICT) resources, Internet usage policies, Security practices etc.)
  - IT-related frauds (including phishing, hacking etc)

- **Categories of IS audits**

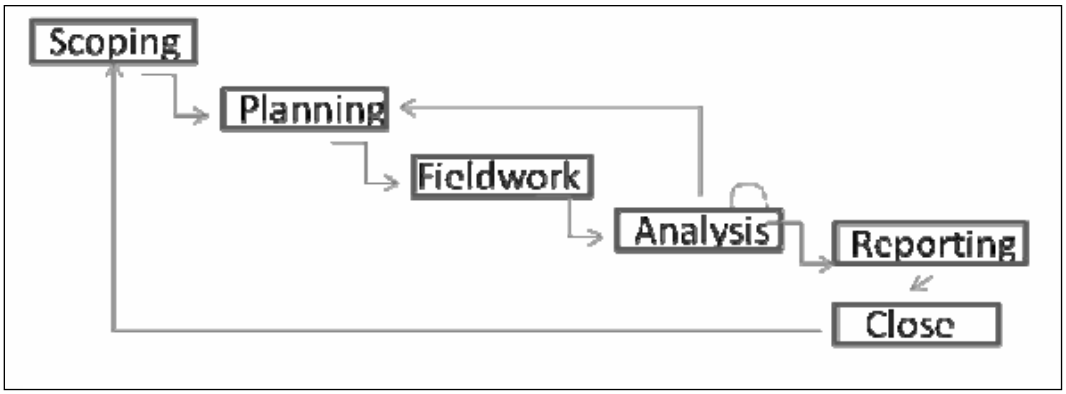
  IT audits has been categorized in to five types:
  - Systems and Applications: An audit to verify that systems and applications are **APPROPRIATE, EFFICIENT, AND ADEQUATELY CONTROLLED** to ensure valid, reliable, timely, and secure input, processing, and output at all levels of a system's activity
  - Information Processing Facilities: An audit to verify that the processing facility is controlled to ensure **TIMELY, ACCURATE, AND EFFICIENT**

PROCESSING of applications under normal and potentially disruptive conditions.

- ✳ Systems Development :
  - An audit to verify that the systems under development **MEET THE OBJECTIVES OF THE ORGANIZATION** and
  - To ensure that the systems are developed in accordance with generally accepted standards for systems development.
- ✳ Management of IT and Enterprise Architecture: An audit to verify that IT management has developed **AN ORGANIZATIONAL STRUCTURE AND PROCEDURES** to ensure a controlled and efficient environment for information processing.
- ✳ Telecommunications, Intranets, and Extranets: An audit to verify that controls are in place on the client (computer receiving services), server, and on the network connecting the clients and servers.

☞ **Steps in Information Technology Audit**

Different audit organizations go about IT auditing in different ways and individual auditors have their own favorite ways of working. It can be categorized into six stages-



I. Scoping and pre-audit survey:
   - ✳ The auditors determine the main area/s of focus and any areas that are explicitly out-of-scope, based normally on some form of risk-based assessment.
   - ✳ Information sources at this stage include background reading and web browsing, previous audit reports, pre audit interview, observations.

II. Planning and preparation: during which the scope is broken down into greater levels of detail, usually involving the generation of an audit work plan or risk-control-matrix.

III. Fieldwork: gathering evidence by interviewing staff and managers, reviewing documents, printouts and data, observing processes etc.

IV. Analysis:
   - ✳ This step involves desperately sorting out, reviewing and trying to make sense of all that evidence gathered earlier.
   - ✳ SWOT (Strengths, Weaknesses, Opportunities, and Treats) or PEST (Political, Economic, Social, and Technological) techniques can be used for analysis.

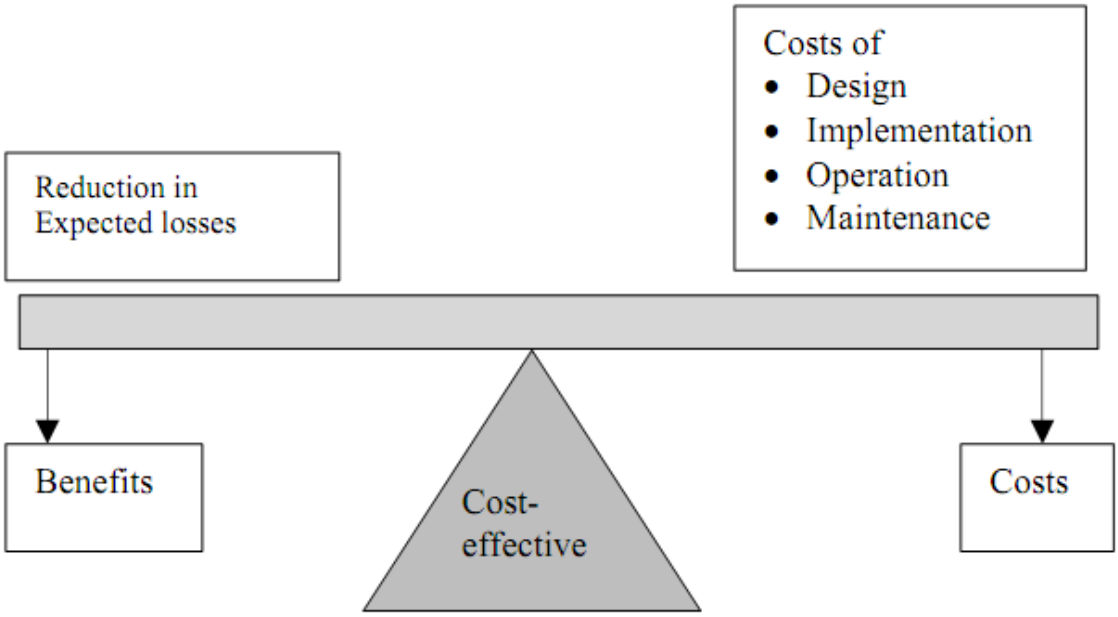
V. Reporting: reporting to the management is done after analysis of data gathered and analysis.

VI. Closure: closure involves preparing notes for future audits and following –up

management to complete the actions they promised after previous audits.

⇨ COST EFFECTIVENESS OF CONTROL PROCEDURES

- ☞ No internal control system can provide foolproof protection against all internal control threats.
- ☞ The cost of a foolproof system would be prohibitive.
- ☞ In addition, because many controls negatively affect operational efficiency, too many controls slow the system and make it inefficient.
- ☞ Therefore, the objective in designing an internal control system is to provide reasonable assurance that control problems do not take place.



Cost-Effectiveness of Controls

- ☞ To determine if a control is effective an auditor must compare the reduction in expected losses that will occur by virtue of having the control with the costs of designing, implementing, operating and maintaining the control.
- ☞ IMPLEMENTING AND OPERATING CONTROLS in a system involves the following five costs-

I. Initial setup cost:
   - ✳ This cost is incurred to **DESIGN AND IMPLEMENT** controls.
   - ✳ For example, a security specialist must be employed to design a physical security system.

II. Executing cost:
   - ✳ This cost is associated with the **EXECUTION OF A CONTROL**.
   - ✳ For example, the cost incurred in using a processor to execute input validation routines for a security system.

III. Correction costs: The control has operated reliably in signalling an error or irregularity, the cost associated with the **CORRECTION OF ERROR OR IRREGULARITY**.

IV. Failure cost:
- ✳ The control malfunctions or not designed to detect an error or irregularity.
- ✳ These **UNDETECTED OR UNCORRECTED ERRORS CAUSE LOSSES**.

V. Maintenance costs:
- ✳ The cost associated in ensuring the **CORRECT WORKING OF A CONTROL**.
- ✳ For example, rewriting input validation routines as the format of input data changes.

⇨ INFORMATION SYSTEMS CONTROL TECHNIQUES

"While reviewing a client's control system, an information system auditor will identify three components of internal control." State and briefly explain these three components.
(M'09- 5Marks)

- ☞ The basic purpose of information system controls in an organization is to ensure that the business objectives are achieved and undesired risk events are prevented or detected and corrected.
- ☞ This is achieved by designing an effective information control framework, which comprises of policies, procedures, practices, and organization structure to give reasonable assurances that the business objectives will be achieved.
- ☞ While reviewing a client's control systems, the auditor will be able to identify three components of internal controls.
- ☞ Each component is aimed at achieving different objectives as stated below:

I. Accounting Controls: These controls are **EXTENDED TO SAFEGUARD THE CLIENT'S ASSETS** and ensure reliability of financial records.

II. Operational Controls: These deals with the day to day operations, functions and activities to ensure that the operational activities are **CONTRIBUTING TO BUSINESS OBJECTIVES**.

III. Administrative Control: These are concerned with ensuring **EFFICIENCY AND COMPLIANCE** with management policies, including the operational controls

☞ OBJECTIVE CONTROLS

CLASS OF CONTROL	FUNCTION	EXAMPLES
PREVENTIVE CTRL (M'09)	✳ Are those input, which are **DESIGN TO PREVENT AN ERROR, OMISSION OR MALICIOUS ACT FORM OCCURRING** ✳ E.g. Password Protection. ✳ Characteristics: 1. A clear-cut understanding about the vulnerabilities of the asset	✳ Proper Training of personnel ✳ Job definitions and SOD ✳ Physical & Logical Access ✳ Maker-checker or authorization process ✳ Firewall ✳ Anti-virus software ✳ Password ✳ Access control

	2. Understanding probable threats 3. Provision of necessary controls	
DETECTIVE CTRL	✳ CTRLS that **DETECT AND REPORT THE OCCURRENCE OF AN ERRORS, OMISSION OR MALICIOUS ACT** ✳ Characteristics: 1. Clear understanding of lawful activities and deviation 2. An established mechanism to refer the reported unlawful activities to the appropriate person or group 3. Interaction with the preventive control 4. Surprise checks by supervisor	✳ Review of Audit Logs ✳ ECHO Checks in network ✳ CCTV ✳ Hash totals ✳ Check points in production jobs ✳ The internal audit functions ✳ Intrusion detection system ✳ Cash counts and bank reconciliation ✳ Monitoring expenditures against budgeted amount ✳ Past-due accounts report
CORRECTIVE CTRL	✳ are designed to **REDUCE THE IMPACT OR CORRECT AN ERROR ONCE IT HAS BEEN DETECTED** ✳ Characteristics: 1. Minimize impact of threat 2. Correct problems indentified 3. Remedy problems discovered by detective controls 4. Get feedback from preventive and detective controls 5. Correct error arising from a problem 6. Modify the processing systems to minimize future occurrences of the problem	✳ Contingency planning ✳ Backup procedure ✳ Rerun procedures ✳ Treatment procedures for a disease ✳ Change input value to an application system ✳ Investigate budget variance and report violations.
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. ✳ Some time organization 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, can definitely reduce the probability of threats to the assets. ✳ Such measures are called compensatory controls.	

- MANAGEMENT CONTROLS (IMP)
  - The controls adopted by the management of an enterprise are to ensure that the information systems function **CORRECTLY AND THAT THEY MEET THE STRATEGIC BUSINESS OBJECTIVES**.
  - 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 controls flow from the top of an organization down (i.e.) the responsibility still lies with the senior management.
  - The controls to consider when reviewing the organization and management controls in an IS System shall include:
    - Responsibility: The strategy to have a **SENIOR MANAGEMENT PERSONNEL** responsible for the IS within the overall organizational structure.
    - An official IT structure: There should be a **PRESCRIBED ORGANIZATION STRUCTURE** with all staff deliberated on their roles and responsibilities by written down and agreed job descriptions.
    - An IT steering committee:
      - The steering committee shall comprise of **USER 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.

- ORGANIZATIONAL CONTROLS
  - Enterprise controls are concerned with the decision-making processes that lead to management authorization of transactions.
  - Companies with large data processing facilities separate data processing from business units to provide control over its costly hardware, software, and human resources.
  - Combining data processing into the business units would be too much responsibility for one manager.
  - Organizational control techniques include documentation of:
    - Reporting responsibility and authority of each function,
    - Definition of responsibilities and objectives of each functions,
    - Policies and procedures,
    - Job descriptions, and
    - Segregation of duties.

- FINANCIAL CONTROL TECHNIQUES
  - 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:

- ✳ Authorization
- ✳ Budgets
- ✳ Cancellation of documents
- ✳ Documentation
- ✳ Dual control
- ✳ Input/ output verification
- ✳ Safekeeping
- ✳ Segregation of duties
- ✳ Sequentially numbered documents

☞ AUDIT TRAILS

The management of ABC Ltd wants to design a detective control Mechanism for achieving security policy objective in computerized environment. As an auditor explain, how audit trails support security objectives. (M'10 - 10 Marks)

☞ Audit trails are logs that can be designed to record activity at the system, application, and user level.

☞ When properly implemented, audit trails provide an important detective control to help accomplish security policy objectives.

☞ Many operating systems allow management to select the level of auditing to be provided by the system.

☞ This determines which events will be recorded in the log.

☞ Audit trails can be used to support security objectives in three ways:

- ✳ Detecting unauthorized access to the system,
- ✳ Facilitating the reconstruction of events, and
- ✳ Promoting personal accountability.

Each of these is described below:

a. <u>Detecting Unauthorized Access</u>:

- ✳ Detecting unauthorized access can occur in real time or after the fact.
- ✳ The primary objective of real-time detection is to protect the system from outsiders who are attempting to breach system controls.
- ✳ A real-time audit trail can also be used to report on changes in system performance that may indicate infestation by a virus or worm.
- ✳ Depending upon how much activity is being logged and reviewed; real-time detection can impose a significant overhead on the operating system, which can degrade operational performance.
- ✳ After-the-fact detection logs can be stored electronically and reviewed

periodically or as needed.

- ✳ When properly designed, they can be used to determine if unauthorized access was accomplished, or attempted and failed.

b. Reconstructing Events:

- ✳ Audit analysis can be used to reconstruct the steps that led to events such as system failures, security violations by individuals, or application processing errors.
- ✳ Knowledge of the conditions that existed at the time of a system failure can be used to assign responsibility and to avoid similar situations in the future.
- ✳ Audit trail analysis also plays an important role in accounting control.
- ✳ For example, by maintaining a record of all changes to account balances, the audit trail can be used to reconstruct accounting data files that were corrupted by a system failure.

c. Personal Accountability:

- ✳ Audit trails can be used to monitor user activity at the lowest level of detail.
- ✳ This capability is a preventive control that can be used to influence behavior.
- ✳ Individual are likely to violate an organization's security policy if they know that their actions are recorded in an audit log.

- ☞ Audit trails are used measured the potential damage and financial loss associated with application errors, abuse of authority, or unauthorized access by outside intruders.
- ☞ Logs also provide valuable evidence or assessing both the adequacies of controls in place and the need for additional controls.

⇨ USER/APPLICATION LEVEL CTRLS

- ☞ Application system controls are undertaken to accomplish reliable information processing cycles that perform the processes across the enterprise.
- ☞ Applications represent the interface between the user and the business functions
- ☞ Can be achieved through a well defined user manual which defines roles and responsibilities.
- ☞ Classifies CTRLS in to input, processing & output CTRLS
- ☞ Also defines Segregation of Duties (SOD).
- ☞ The following key controls can be established as user control

a. Boundary Controls
b. Input Controls
c. Processing Controls
d. Output Controls
e. Database Controls

a. 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 must ensure that they are given authentic resources.
- ✳ Users allowed using resources in restricted ways.

- ✳ The following key access controls mechanism are used by boundary control
  - Identification: Name, Account Number, address, card number
  - Authentication: ID and password, PIN, Finger Prints
  - Authorization: Access rights for access of resources
  - Data encryption: Transfer of Data between users and system in a code from

b. Input Controls :

- DATA BROUGHT IN TO THE SYSTEM ARE
  - ✳ VALID,
  - ✳ ACCURATE &
  - ✳ COMPLETE.
- TYPES OF INPUT CTRLS
  - ✳ Sources Document CTRLS: it is a system where physical source documents (Voucher, purchase order & indent forms) are used to initiate a transaction, control should be exercise over these instruments.
  - ✳ Controls:
    - Pre-numbered source document
    - Use of document in sequence
    - Audit of sources documents.
- DATA CODING CONTROLS refers to CTRLS that checks the integrity of code (e.g. product code, account code) used for data processing.

TYPES OF ERRORS	EXAMPLE
TRANSCRIPTION ERRORS	
Addition Errors	9865 is 98655
Truncation Errors	9865 is 986
Substitution Errors	9865 is 8966
TRANSPOSITION ERRORS	
Single transposition Errors	9865 is 8965
Multiple Transposition Errors	9865 is 6895

- CTRL for Data Coding Errors
  - ✳ Check Digit: These CTRL digits are added to code @ the time of originally assessing the code.
  - ✳ Can be located any where- prefix, suffix or in the middle of the code.
  - ✳ Check is affected whenever code is keyed in.

c. 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 the database management system that stores the data.
- Data processing controls are:

- Run to run controls: refers to using control totals to monitor a batch as it move from one program module to another.
- Reasonableness verification: Checks whether value generated are reasonable. E.g. if sales generated > production & stock.
- Exception Reports: Some Errors code are appended by the programmer while developing/coding a SW. when the SW encounters that error condition, it throws up the relevant message.

d. Output Controls :

- CTRLS that ensure outputs are not
  - Lost,
  - Misdirected,
  - Corrupted.
- Output can be in MULTIPLE FROMS LIKE PRINTED OUTPUT, ON SCREEN OUTPUT, ETC.
- CONTROL OVER OUTPUT
  - Control over Spool/ Chache Files:
    - A speed difference between processor & devices brings out need for a temporary memory to hold files before printing.
    - Spool file need to be protected against unauthorized modification.
  - Exception Reports:
    - Refers to variation thrown out by the system.
    - Cannot be controlled by control Totals but by correct functioning of the system.
- CONTROL OVER DISTRIBUTION OF OUTPUT
  - A: if user dept. checks the CTRLs & ACTS on the output reports: no Problem
  - B: if one dept. checks the CTRLS & different dept. uses the output: Procedures should be place-output registers and sequential numbers.
- RETENTION CONTROLS: Period up to which the output are to be retained, which is guided by the data retention policy of the organization.
- RECOVERY/RESTORATION CTRLS: This is to ensure organization recovers/restore output lost.

e. 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 the update controls and report controls.
- The update controls are :
  - Sequence Check when Transaction file updated the Master File to ensure correct order
  - Ensure All Records in transaction Files are processed
  - Process multiple transactions for a single record in the correct order
  - Maintain a suspense account for transaction not having their master.
- The Report controls are:
  - Maintain integrity of internal tables used for various calculations.
  - Print run-to-run controls: i.e. option to print each step of transaction processing

- ✳ Printing of suspense account to view orphan transactions.
- ✳ Review existence of backup and recovery controls to ensure safe recovery of data in any adverse situation.

☞ SYSTEM DEVELOPMENT AND ACQUISITION CONTROLS

Write a short note on Key elements in System Development and Acquisition Control (N'08-5 Marks)

- ☞ It is important to have a formal, appropriate, and proven methodology to govern the development, acquisition, implementation, and maintenance of information systems and related technologies.
- ☞ Methodology should contain appropriate controls for management review and approval, user involvement, analysis, design, testing, implementation, and conversion.
- ☞ Key elements in system Development and acquisition controls and given in following table:

Control	Threats/Risks	Controls
System development and acquisition controls	System development projects consume excessive resources.	Long-range strategic master plan, data processing schedules, assignment of each project to manage team, project development plan, project milestones, performance evaluations, system performance measurements.
Change management controls	Systems development projects consume excessive resources, unauthorized systems changes.	Change management control policies and procedures, periodic review of all systems for needed changes, standardized format for changes, log and review change requests, assess impact of changes on system reliability, categorize and rank all, changes, procedures to handle urgent matters, communicate changes to management and users, management approval of changes, assignspecific responsibilities while maintaining adequate segregation of duties etc.

☞ QUALITY CONTROL

Explain the role of IS Auditor with respect to quality control of systems.

- ☞ IS Auditor's Role: In case, the auditor intends to carry out detailed reviews of, for example, logical design, it will probably be necessary either to employ expert assistance, or to undertake training in the particular technical skills required.

The following are the general questions that the IS Auditor needs to consider for quality control:

- ✳ Does system design follow a defined and acceptable standard?
- ✳ Are completed designs discussed and agreed with the users?
- ✳ Does the project's quality assurance procedures ensure that project documentation is reviewed against the organization's technical standards and policies, and the user requirements specification.
- ✳ Do quality reviews follow a defined and acceptable standard?
- ✳ Are quality reviews carried out under the direction of a technically competent person who is managerially independent from the design team;
- ✳ Are auditors/security staff invited to comment on the internal control aspects of system designs and development specifications?
- ✳ Are statistics of defects uncovered during quality reviews and other forms of quality control maintained and analyzed for trends? Is the outcome of trend analysis fed back into the project to improve the quality of other deliverables?
- ✳ Are defects uncovered during quality reviews always corrected?
- ✳ Are all configuration items (hardware, software, documentation) that have passed quality review been placed under configuration management and version control?
- ✳ Has a Training Plan been developed and quality reviewed? Has sufficient time and resources been allocated to its delivery?
- ✳ Has a system installation plan been developed and quality reviewed?
- ✳ Has an acceptance testing plan been drawn up? Is it to an acceptable standard?

☞ SYSTEM MAINTENANCE

System maintenance is an important phase during the implementation of the system. If so, what are the three categories in which maintenance can be undertaken? As an IS auditor of the organization, how will you evaluate the effectiveness and efficiency of the system maintenance process? (N'10 – 8 Marks)

- ☞ System maintenance is an important phase during the implementation of system; day-to-day operations bring out the strength and weaknesses which may need periodic modification to meet its objective.
- ☞ Maintenance can be undertaken under the following three categories:
  - ✳ Corrective maintenance: Emergency program fixes and routine debugging-logical errors.
  - ✳ Adaptive maintenance: Accommodations of change-in the user environment.
  - ✳ Perfective maintenance: User enhancements, improved documentation, and recoding for improving processing efficiency.

- Auditor's Role

  The effectiveness and efficiency of the system maintenance process is evaluated with the following metrics:

  - The ratio of actual maintenance cost per application/operation versus the average of all applications/process.
  - Average time to deliver change requests.
  - The number of change requests for the system application that were related to bugs, critical errors, and new functional specifications.
  - The number of production problems per application and per respective maintenance changes
  - The instances of divergence from standard procedures such as undocumented applications, unapproved design, and testing reductions.
  - The quantity of modules returned to development due to errors discovered in acceptance testing.
  - Time elapsed to analyze and fix problems.

- POST IMPLEMENTATION REVIEW
  - After a development project is completed a post implementation review should be performed to determine if the anticipated benefits were achieved.
  - Reviews help to control project development activities and to encourage accurate and objective initial cost and benefit estimates.
  - The full scope of a post implementation review ("PIR") will depend largely on the scale and complexity of the project.
  - The post implementation review should be performed jointly by the project development team and the appropriate end users or alternatively, either internal or external, should carry out the audit, to meet the following objectives:
    - Business objectives: delivered within budget and deadline; is producing predicted savings and benefits, etc.;
    - User expectations: user friendly, carries the workload, produces the required outputs, good response time, reliable, good ergonomics, etc.;
    - Technical requirements: capable of expansion, easy to operate and maintain, interfaces with other systems, low running cost, etc.
  - If there are obvious and significant problems with a new system a PIR may need to be undertaken sooner than would otherwise have been the case in order to identify the nature of the problem(s), their case(s), and to recommend a suitable course of action.
  - The PIR team
    - In order to achieve an impartial outcome, the team should be substantially independent of the original system development team.
    - It may therefore be advisable to employ an external IS consultant to manage the review.
    - It may also be necessary to employ other external support to assist in evaluating the delivery of technical (e.g. project management, system design) and specialized

functions (e.g. in financial and management accountancy), and to make appropriate recommendations where necessary. Internal Audit might help assess the effectiveness of internal controls.

- Activities to be undertaken: During a PIR, the team should, according to their terms of reference, review:-
  - the main functionality of the operational system against the User Requirements Specification;
  - system performance and operation;
  - the development techniques and methodologies employed;
  - estimated time-scales and budgets, and identify reasons for variations;
  - changes to requirements, and confirm that they were considered, authorized and implemented in accordance with change and configuration management standards;
  - set out findings, conclusions and recommendations in a report for the authorizing authority to consider.
- Following their deliberations on the PIR Report, the authorizing authority may either:
  - endorse continuation of the system;
  - approve plans to modify the system;
  - Terminate the system and made arrangements for a new course of action.

What are the issues that should be considered by a system auditor at post implementation review stage before preparing the audit report? (M'09- 5 Marks)

- Auditor's Role: The following issues should be considered when judging the effectiveness either of a PIR, or to form the basis for the auditor to undertake one.
  - Interview business users in each functional area covered by the system, and assess their satisfaction with, and overall use of, the system.
  - Interview security, operations and maintenance staff and, within the context of their particular responsibilities, assess their reactions to the system.
  - Based on the User Requirements Specification, determine whether the system's requirements have been met. Identify the reason(s) why any requirements are not to be provided, are yet to be delivered, or which do not work properly.
  - Confirm that the previous system has been de-commissioned or establish the reason(s) why it remains in use.
  - Review system problem reports and change proposals to establish the number and nature (routine, significant, major) of problems, and changes being made to remedy them. The volume of system change activity can provide an indicator of the quality of systems development.
  - Confirm that adequate internal controls have been built into the system, that these are adequately documented, and that they are being operated correctly. Review the number and nature of internal control rejections to determine whether there are any underlying system design weaknesses.
  - Confirm that an adequate Service Level Agreement has been drawn up and implemented. Identify and report on any area where service delivery either falls below the level specified, or is inadequate in terms of what was specified.
  - Confirm that the system is being backed up in accordance with user requirements, and that it has been successfully restored from backup media.
  - Review the Business Case and determine whether:-

- anticipate benefits have/are been achieved;
- any unplanned benefits have been identified;
- costs are in line with those estimated;
- Benefits and costs are falling with the anticipated time-frame.

✳ Review trends in transaction throughput and growth in storage use to identify the anticipated growth of the system is in line with that forecast.

☞ CONTROL OVER DATA INTEGRITY, PRIVACY AND SECURITY

☞ INFORMATION CLASSIFICATION

✳ Information classification does not follow any predefined rules.

✳ It is a conscious decision to assign a certain **SENSITIVITY LEVEL TO INFORMATION** that is being created, amended, updated, stored, or transmitted.

✳ The sensitivity level depends upon the nature of business in an organization and the market influence.

✳ The classification of information further determines the level of control and security requirements.

✳ Classification of information is **ESSENTIAL TO UNDERSTAND AND DIFFERENTIATE BETWEEN THE VALUE OF AN ASSET AND ITS SENSITIVITY AND CONFIDENTIALITY**.

✳ When data is stored, whether received, created or amended, it should always be classified into an appropriate sensitivity level to ensure adequate security.

✳ For many organizations, a very simple classification criteria is as follows:

a. Top Secret:
   - The information is classified as Top Secret/ confidential that can **CAUSE SERIOUS DAMAGE** to the organization if **LOST OR MADE PUBLIC**.
   - Information is relating to pending mergers or acquisitions; investment strategies; plans or designs etc is highly sensitive.
   - Many restrictions are imposed on the usage of such information and is protected at the **HIGHEST LEVEL OF SECURITY POSSIBLE**.

b. Highly Confidential:
   - This class of information, is considered **CRITICAL FOR THE ONGOING BUSINESS OPERATIONS** and can cause serious impediment, if shared around the organization
   - e.g. sensitive customer information of bank's, solicitors and accountants etc., patient's medical records and similar highly sensitive data.
   - It should not be copied or removed without the consent of appropriate authority and must be kept under operational vigilance.
   - Security at this level should be **VERY HIGH**.

c. Proprietary:
   - Information relating to **PROCEDURES, OPERATIONAL WORK ROUTINES, PROJECT PLANS, DESIGNS AND SPECIFICATIONS** are of propriety in nature.
   - Such information is for proprietary use to authorized personnel only.
   - Security at this level is **HIGH**.

d. Internal Use only:
   - This class of information **CANNOT BE CIRCULATED OUTSIDE** the organization where its loss would inconvenience the organization or management but disclosure is unlikely to result in financial loss or serious damage to credibility.
   - For e.g.: Internal memos, minutes of meetings, internal project reports
   - Security at this level is **CONTROLLED BUT NORMAL.**

e. Public Documents:
   - This Information is **PUBLISHED IN THE PUBLIC DOMAIN**; annual reports, press statements etc.; which has been **APPROVED FOR PUBLIC USE**.
   - Security at this level is **MINIMAL**.

☞ DATA INTEGRITY

- ✳ Once the information is classified, the organization has to decide about various data integrity controls to be implemented.
- ✳ The primary objective of data integrity control techniques is to **PREVENT, DETECT, AND CORRECT ERRORS IN TRANSACTIONS** as they flow through the various stages of a specific date processing program.
- ✳ In other words, they ensure the integrity of a specific application's inputs, stored data, programs, data transmissions, and outputs.
- ✳ Data integrity controls protect data from accidental or malicious alteration or destruction.
- ✳ Assessing data integrity involves evaluating the following critical procedures:
  - Virus detection and elimination software is installed and activated.
  - Data integrity and validation controls are used to provide assurance that the information has not been altered and the system functions as intended
- ✳ 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.

Control	Threats/Risks	Controls
Source data control	✳ Invalid, ✳ incomplete, or ✳ inaccurate source data input	✳ Forms design; ✳ sequentially pre-numbered forms, ✳ Turnaround documents; ✳ cancellation and 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	✳ Enter exceptions in an error log; ✳ Investigate, correct, and resubmit chem. ✳ On a timely basis; ✳ re-edit them and ✳ Prepare a summary error report.
On-line 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; ✳ 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 conversion controls.
Output controls	✳ Inaccurate or ✳ incomplete computer output	✳ 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; ✳ users review computer output for completeness and accuracy, shred confidential output no longer needed; ✳ Error and exception reports.
Data transmission controls	✳ Unauthorized access to data being transmitted or ✳ to the system itself; system failures; ✳ errors in data transmission	✳ Monitor network to detect week points, ✳ backup components, ✳ design network to handle peak processing, ✳ multiple communication paths between network components, ✳ preventive maintenance, ✳ data encryption, ✳ routing verification

"Once the information is classified on various levels, the organization has to decide about the implementation of different data integrity controls" Do you agree? If yes, explain about data integrity and its policies. (N'10 – 8 Marks)

- Yes, we agree statement given in the question.
- 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.
- Data Integrity Policies
  - Virus-Signature Updating: Virus signatures must be updated immediately when they are made available from the vendor.
  - Software Testing: All software must be tested in a suitable test environment before installation on production systems.
  - Division of Environments: The division of environments into Development, Test, and Production is required for critical systems.
  - Version Zero Software: Version zero software (1.0, 2.0, and so on) must be avoided whenever possible to avoid undiscovered bugs.
  - Offsite Backup Storage: Backups older than one month must be sent offsite for permanent storage.
  - Quarter-End and Year-End Backups: Quarter-end and year-end backups must be done separately from the normal schedule, for accounting purposes
  - Disaster Recovery: A comprehensive disaster-recovery plan must be used to ensure continuity of the corporate business in the event of an outage.

☞ 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.
- An IS auditor is responsible to evaluate the following when reviewing the adequacy of data security controls:
  - Who is responsible for the accuracy of the data?
  - Who is permitted to update data?
  - Who is permitted to read and use the data?
  - Who is responsible for determining who can read and update the data?
  - Who controls the security of the data?
  - If the IS system is outsourced, what security controls and protection mechanism does the vendor have in place to secure and protect data?
  - Contractually, what penalties or remedies are in place to protect the tangible and intangible values of the information?

- The disclosure of sensitive information is a serious concern to the organization and is mandatory on the auditor's list of priorities.

☞ SECURITY CONCEPTS AND TECHNIQUES

Explain the term "Cryptosystems'. Briefly discuss Data Encryption Standard. (N'09- 5 Marks)

☞ CRYPTOSYSTEMS:

- ✳ A cryptosystem refers to a suite of algorithms
- ✳ needed to implement a particular form of
- ✳ encryption and
- ✳ Decryption.

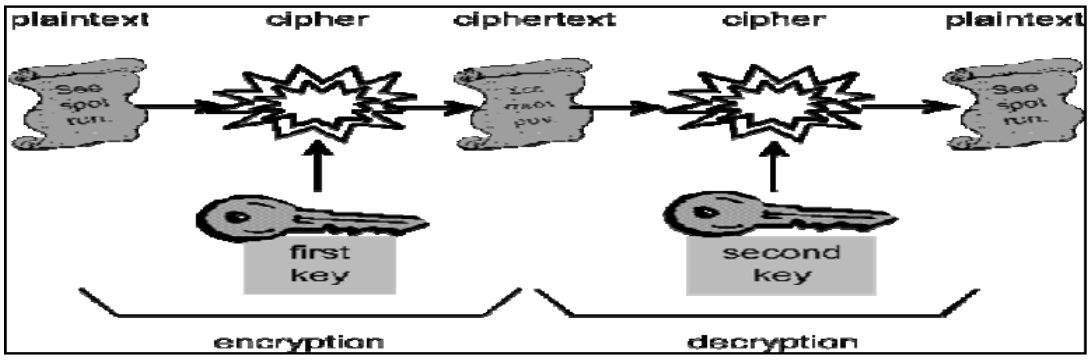
☞ Typically, it consists of following three algorithms:

- ✳ Key Generation Algorithm,
- ✳ Encryption Algorithm and
- ✳ Decryption Algorithm.

☞ The pair of algorithms of Encryption and Decryption is referred as Cipher or Cypher.

☞ DATA ENCRYPTION STANDARD (DES):

- ✳ It is a cipher.
- ✳ It is a mathematical algorithm for encrypting and decrypting binary coded information.
- ✳ Encrypting of data converts it to an unintelligible form called cipher.
- ✳ Decrypting cipher converts the data back to its original form called plaintext.
- ✳ Encryption and Decryption operations are done by using a binary number called a key. A
- ✳ Key consists of 64(bits) binary digits. Among these 64 bits, 56 bits are used for encryption/decryption and remaining 8 bits are used for error detection.
- ✳ Authorized users of the encrypted data must have the unique key that was used to encipher the data in order to decrypt it.
- ✳ Selection of a different key causes the cipher that is produced for any given set of inputs to be different.
- ✳ The cryptographic security of the data depends on the security provided for the key used to encipher and decipher the data.
- ✳ A standard algorithm based on a secure key thus provides a basis for exchanging encrypted computer data by issuing the key used to encipher it to those authorized to have the data.
- ✳ The encryption and decryption processes are depicted in the following diagram:



☞ PUBLIC KEY INFRASTRUCTURE (PKI)

- ✳ Public key infrastructure, if properly implemented and maintained, can provide a strong means of authentication.
- ✳ By combining a variety of hardware components, system software, policies, practices, and standards, PKI can provide for authentication, data integrity, defenses against customer repudiation, and confidentiality.
- ✳ The system is based on public key cryptography in which each user has a key pair—a unique electronic value called a public key and a mathematically related private key.
- ✳ The public key is made available to those who need to verify the user's identity.
- ✳ The private key is stored on the user's computer or a separate device such as a smart card.

Discuss the policies and control that financial institution need to be consider when utilizing public key infrastructure. (M'11- 8 Marks)

When utilizing PKI policies and controls, financial institutions need to consider the following:

- ✳ Defining within the certificate issuance policy the methods of initial verification that are appropriate for different types of certificate applicants and the controls for issuing digital certificates and key pairs;
- ✳ Selecting an appropriate certificate validity period to minimize transactional and reputation risk exposure—expiration provides an opportunity to evaluate the continuing adequacy of key lengths and encryption algorithms, which can be changed as needed before issuing a new certificate;
- ✳ Ensuring that the digital certificate is valid by such means as checking a certificate revocation list before accepting transactions accompanied by a certificate;
- ✳ Defining the circumstances for authorizing a certificate's revocation, such as the compromise of a user's private key or the closing of user accounts;
- ✳ Updating the database of revoked certificates frequently, ideally in real-time mode;
- ✳ Employing stringent measures to protect the root key including limited physical access to CA facilities, tamper-resistant security modules, dual control over private keys and the process of signing certificates, as well as the storage of original and back-up keys on computers that do not connect with outside networks;
- ✳ Requiring regular independent audits to ensure controls are in place, public and private key lengths remain appropriate, cryptographic modules conform to industry standards, and procedures are followed to safeguard the CA system;
- ✳ Recording in a secure audit log all significant events performed by the CA system, including the use of the root key, where each entry is time/date stamped and signed;
- ✳ Regularly reviewing exception reports and system activity by the CA's employees to detect malfunctions and unauthorized activities; and
- ✳ Ensuring the institution's certificates and authentication systems comply with widely accepted PKI standards to retain the flexibility to participate in ventures that require the acceptance of the financial institution's certificates by other CAs.

⇨ FIREWALLS (M'09- 5 Marks &M'11- 4 Marks)

- ☞ A firewall is a collection of components (computers, routers, and software) that mediate access between different security domains.
- ☞ All traffic between the security domains must pass through the firewall, regardless of the direction of the flow.
- ☞ Since the firewall serves as an access control point for traffic between security domains, they are ideally situated to inspect and block traffic and coordinate activities with network intrusion detection systems (IDSs).
- ☞ Basic for selection of a firewall
  - ✳ Amount of traffic
  - ✳ Sensitivity of the system & data & Applications
  - ✳ Ease to firewall administration
  - ✳ Degree of firewall monitoring support through automated logging & log analysis
  - ✳ Capability to provide alerts for abnormal activity.
- ☞ Types of firewall:
  - ✳ Router packet filtering firewall
  - ✳ Application firewall system
  - ✳ Stateful inspection firewall
  - ✳ Proxy server firewall

a. ROUTER PACKET FILTERING

- ✳ Packet filter firewall evaluate the **HEADERS** of the each incoming & outgoing packet to ensure it has a valid internal address, originated from a permitted external address, connects to an authorized protocol or service and contains valid basic header instruction.
- ✳ If the pact **DOES NOT MATCH THE PREDEFINED POLICY FOR ALLOWED TRAFFIC, THEN THE FIREWALL DROPS THE PACKET**.
- ✳ Packet filtering is now also available in many routers, which contain **ACCESS CONTROL LISIS (ACLS)** for the same.

b. APPLICATION FIREWALL SYSTEM

- ✳ Application level firewall perform application level screening, typically including the filtering capabilities of the packet filter firewall with additional validation of the packet content based on the application.
- ✳ Application level firewalls capture and compare packets to state information in the connection tables.
- ✳ Unlike a packet filter firewall an application level firewall provide additional screening of the packet length, authorization, content, or invalid headers.
- ✳ Advantage: Application level firewalls provide the strongest level of security.
- ✳ Disadvantage: Application level firewall are slower and require greater expertise to administer properly

c. STATEFUL INSPECTION

- ✳ Stateful inspection firewalls use dynamic packet filtering for performance benefits.

- ✳ Firewall checks each packet as it arrives to determine whether it is part of existing connection. If it verifies that packet belongs to an established connection then it forwards the packet without subjecting in to the firewall rule set.
- ✳ When a connection is established the firewall adds the connection information to a table.
- ✳ The firewall can then compare future packets to the connection or state table.
- ✳ This essentially verifies that inbound traffic is in response to requests initiated from inside the firewall.

d. PORXY SERVER FIREWALL: A proxy severs is a server (a computer system or an application program) that acts as an intermediary for requests from clients seeking resend from other server.

⇨ CONTROLLING OVER UNAUTHORISED INTRUSION

- ☞ IDS: INTRUSION DETECTION SYSTEM
- ☞ ANTI-VIRUS SOFTWARE

☞ INTRUSION DETECTION SYSTEM

- ✳ What:
  - 🖋 Intrusion detection is the set of mechanisms
  - 🖋 that should be put in place to warn
  - 🖋 to attempted unauthorized access to the computer.
- ✳ Why: To protect the data and system integrity.
- ✳ Categories:

NETWORK BASES	HOST BASE
✳ These types of systems are place on the network, near by the **SYSTEM OR SYSTEM BEING MONITOR** ✳ They examine the network **TRAFFIC** and determine whether it falls within acceptable boundaries	✳ These types of systems actually run on the **SYSTEM BEING MONITOR**. ✳ These examine the system to determine whether the **ACTIVITY** on the system is acceptable.

☞ ANTI-VIRUS SOFTWARE (N'09- 5 Marks)

- ✳ Anti-virus software is the most widely used techniques to **DETECT VIRUSES & PREVENT THEIR FURTHER PROPAGATION & HARM.**
- ✳ These are 3 types of anti-virus software.
  - I. Scanners
  - II. Active monitor/ Heuristic scanner
  - III. Integrity Check

I. **Scanners:**

- ✳ The software looks for a sequence of bits called virus **SIGNATURES** that are characteristic of virus codes.
- ✳ They check memory, executables and system fillies to find matching bit **PATTERNS**

II. **Active monitor/ Heuristic scanner:**

This looks for critical interrupt calls and critical operating system functions such as OS calls & BIOS calls, which **RESEMBLE VIRUS ACTION**.

III. **Integrity Check:**

- ✳ These can detect any unauthorized changes to files on the system computer binary check data call the **CYCLIC REDUNDANCY CHECK (CRC)**
- ✳ When a program called for execution the software computer the CRC again and checks with the parameter stored on the disk.

☞ HACKING:

✳ It is an act of **PENETRATING** computer systems to gain knowledge about the system and how it works.

Hacker:

✳ Hacker is someone who is enthusiastic about computer programming and all things relating to the technical workings of a computer.

Crackers:

✳ Crackers are people who try to gain unauthorized access to computers.

✳ This is normally done through the use of a "backdoor" program installed on the machine.

✳ A lot of crackers also try to gain access to resources through the use of password cracking software, which tries billions of passwords to find the correct one for accessing a computer.

How do hackers hack? :

✳ There are many ways in which a hacker can hack. These are:

- Net BIOS
- ICMP Ping
- FTP
- RPC. Statd
- HTTP.

a. NetBIOS:

- ✳ NetBIOS hackers are the **WORST KIND, SINCE THEY DON'T REQUIRE YOU TO HAVE ANY HIDDEN BACKDOOR PROGRAM** running on your computer.
- ✳ This kind of hack exploits a **BUG IN WINDOWS** 9x.
- ✳ NetBIOS is meant to be used on local area networks, so machines on that network can share information.
- ✳ Unfortunately, the bug is that NetBIOS can also be used across the Internet - so a hacker can access your machine remotely.

b. ICMP 'Ping' (Internet Control Message Protocol):
   - ICMP is one of the main protocols that **MAKE THE INTERNET WORK**.
   - It stands for Internet Control Message Protocol. '
   - **PING' IS ONE OF THE COMMANDS** that can be sent to a computer using ICMP.
   - Ordinarily, a computer would respond to this ping, telling the sender that the computer does exist.
   - Pings may seem harmless enough, but a large number of pings can make a Denial-of-Service attack, which overloads a computer.
   - If a computer responds to a ping, then the hacker could launch a more serious form of attack against a computer.

c. FTP (File Transfer Protocol) :
   - FTP is a standard Internet protocol, standing for File Transfer Protocol.
   - It can be **USED FOR FILE DOWNLOADS** from some websites.
   - If you have a web page of your own, you may use FTP to upload it from your home computer to the web server.
   - However, FTP can also be used by some hackers.
   - FTP normally requires some form of authentication for access to private files, or for writing to files.
   - FTP backdoor programs, such as-
     - Doly Trojan
     - Fore
     - Blade Runner

d. RPC Statd:
   - This is a problem specific to Linux and UNIX.
   - The problem is the infamous unchecked buffer overflow problem.
   - This is where a fixed amount of memory is set aside for storage of data.
   - If data is received that is larger than this buffer, the program should truncate the data or send back an error, or at least do something other than ignore the problem.
   - This can cause crashes of various different kinds.
   - However, a skilled hacker could write bits of program code into memory that may be executed to perform the hacker's evil deeds.

e. HTTP – HTTP stands for Hypertext Transfer Protocol:
   - HTTP hacks can only be harmful if you are using **MICROSOFT WEB SERVER SOFTWARE**, such as Personal Web Server.
   - There is a bug in this software called an **'UNCHECKED BUFFER OVERFLOW'**.
   - If a user makes a request for a file on the web server with a very long name, part of the request gets written into parts of memory that contain active program code.
   - A malicious user could use this to run any program they want on the server.

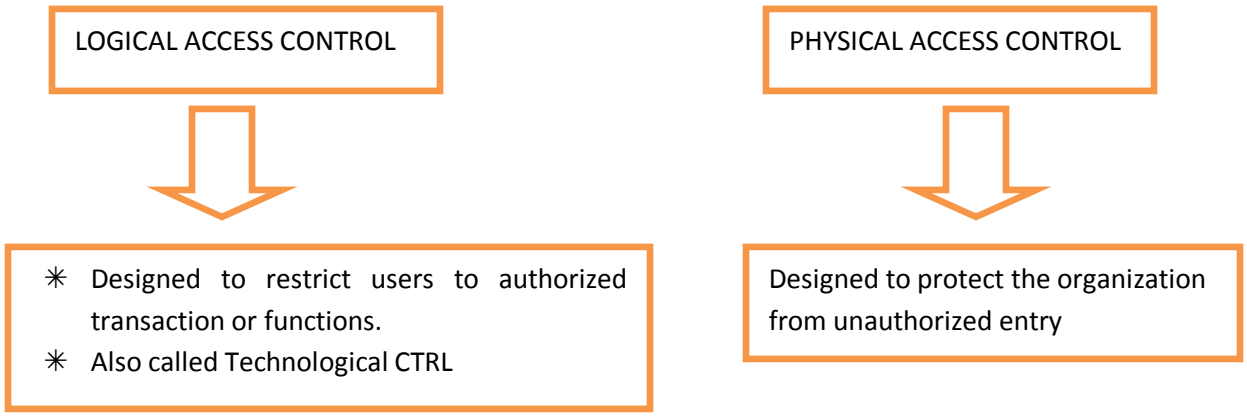
⇨ DATA CONTOLS OBJECTIVE (IMP)

OBJECTIVE	MEANING
DATA INTEGRITY	No unauthorized modification
DATA CONFIDENTIALITY	Access to data should be restricted only to authorized personnel
DATA AVAILABILITY	There should be no data loss or in case of loss backup should be available.

⇨ DATA PRIVACY

- ☞ This refers to the evolving relationship between
  - ✳ technology and the legal right to, or
  - ✳ public expectation of privacy in the collection and sharing of data.
- ☞ Privacy problems exist wherever uniquely identifiable data relating to a person or persons are collected and stored, in digital form or otherwise.
- ☞ Improper or non-existent disclosure control can be the root cause for privacy issues.
- ☞ The most common sources of data that are affected by data privacy issues are:
  - ✳ Health information
  - ✳ Criminal justice
  - ✳ Financial information
  - ✳ Genetic information
  - ✳ Location information
- ☞ Protecting data privacy in information systems:
  - ✳ Increasingly, as heterogeneous information systems with different privacy rules are interconnected, technical control and logging mechanisms (policy appliances) will be required to reconcile, enforce and monitor privacy policy rules (and laws) as information is shared across systems and to ensure accountability for information use.
  - ✳ There are several technologies to address privacy protection in enterprise IT systems.
  - ✳ These falls into two categories: communication and enforcement.
    - i. Policy Communication: P3P -
      - ✳ The Platform for Privacy Preferences.
      - ✳ P3P is a standard for communicating privacy practices and comparing them to the preferences of individuals.
    - ii. Policy Enforcement
      - ✳ XACML - The extensible Access Control Markup Language together with its Privacy Profile is a standard for expressing privacy policies in a machine-readable language which a software system can use to enforce the policy in enterprise IT systems.
      - ✳ EPAL - The Enterprise Privacy Authorization Language is very similar to XACML, but is not yet a standard.
      - ✳ WS-Privacy - "Web Service Privacy" will be a specification for communicating privacy policy in web services. For example, it may specify how privacy policy information can be embedded in the SOAP envelope of a web service message

⇨ ACCESS CTRLS



⇨ 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 :

- ✳ Logical access controls **RESTRICT USERS TO AUTHORIZED TRANSACTIONS AND FUNCTIONS**.
- ✳ There are logical controls over **NETWORK ACCESS**.
- ✳ There are controls implemented to **PROTECT THE INTEGRITY OF THE APPLICATION** and the **CONFIDENCE OF THE PUBLIC** when the public accesses the system.

☞ **Logical Access Paths**

a. Online Terminals
b. Batch Job Processing
c. Dial-up Port
d. Telecommunication Network

a. Online Terminals:
   - ✳ To access an online terminal a user has to provide a valid logon-ID and password.
   - ✳ If additional authentication mechanisms are added along with the password, it will strengthen the security.

b. Batch Job Processing:
   - ✳ In a batch processing environment all jobs are processed in a batch.
   - ✳ These batches are processed at regular intervals.
   - ✳ The jobs are accumulated and sent as batches.
   - ✳ Even the accumulated jobs, which are waiting to be processed, should be controlled appropriately.

c. 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
   - ✳ Thus the modem can act as an interface between remote terminal and the

telephone line.

d. 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 or public, security is provided in the same manner as it is applied to online terminals.

☞ **Issues and Revelations related to Logical Access**

- Logical access controls are used to increase the organization's potential for the losses that result due to exposures that may lead to the total shutdown of the computer functions.
- Intentional or accidental exposure of logical access control encourages technical exposures and computer crimes.

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

- Data Diddling: Data diddling involves the **CHANGE OF DATA BEFORE** or as they are **ENTERED** into the system.
- 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.
  - Christmas card is a well-known example of Trojan.
- Worms:
  - 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.
  - Examples of worms are Existential Worm, Alarm clock Worm etc
- Rounding Down:
  - This refers to rounding of small fractions of a denomination and transferring these small fractions into an authorized account.
  - As the amount is small it gets rarely noticed.
- Salami Techniques:
  - This involves slicing of small amounts of money from a computerized transaction or account and is similar to the rounding down technique.
  - A Salami technique is slightly different from a rounding technique in the sense only last few digits are rounded off here.
  - For example, in the rounding down technique, Rs. 21,23,456.39 becomes Rs. 21,23,456.35, while in the Salami technique the transaction amount Rs. 21,23,456.39 is truncated to either Rs. 21,23,456.30 or Rs. 21,23,456.00, depending on the calculation.
- Trap Doors:
  - Trap doors allow they are **EXISTS OUT OF AN AUTHORIZED PROGRAM AND ALLOW INSERTION OF SPECIFIC LOGIC**, such as program interrupts that

permit a review of data.
- They also permit insertion of unauthorized logic.

b. Computer Crime Exposures: Computer crimes generally result in Loss of customers, embarrassment to management and legal actions against the organizations.

- Financial Loss: Financial losses may be direct like loss of electronic funds or indirect like expenditure towards repair of damaged electronic components.
- Legal Liabilities:
  - An organization has to adhere to many human rights laws while developing security policies and procedures.
  - These laws protect both the perpetrator and organization from trial.
  - The IS auditor should take legal counsel while reviewing the issues associated with computer security.
- Loss of Credibility or Competitive Edge: Company may **GAIN A BAD NAME** if customer's data/funds are manipulated.
- Blackmail/Industrial Espionage: By knowing the confidential information, the perpetrator can **OBTAIN MONEY** from the organization by threatening and exploiting the security violation.
- Disclosure of Confidential, Sensitive or Embarrassing Information:
  - These events can **SPOIL THE REPUTATION** of the organization.
  - Legal or regulatory actions against the company are also a result of disclosure.
- Sabotage:
  - People who may **NOT BE INTERESTED IN FINANCIAL GAIN BUT WHO WANT TO SPOIL THE CREDIBILITY OF THE COMPANY** or to will involve in such activities.
  - They do it because of their dislike towards the organization or for their intemperance
- Spoofing:
  - A spoofing attack involves **FORGING ONE'S SOURCE ADDRESS**.
  - One machine is used to impersonate the other in spoofing technique.
  - Spoofing occurs only after a particular machine has been identified as vulnerable.

c. Asynchronous Attacks: They occur in many environments where data can be moved asynchronously across telecommunication lines. These attacks are hard to detect because they are usually very small pin like insertions. There are many forms of asynchronous attacks.

- Data Leakage:
  - Data is 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.
- Wire-tapping: This involves **SPYING ON INFORMATION BEING TRANSMITTED OVER TELECOMMUNICATION NETWORK.**
- Piggy backing: 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**.
- Shut 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.
- **HACKERS USE** this technique to shut down computer systems over the Internet.

- METHODS OF IDENTIFICATION AND AUTHENDICATION
  - What one remembers: Name, User ID password, PIN etc?
  - What one has (possesses): bachge, plastic cards, smart card, kets etc.
  - What one is (Physiological Traits): Bio-metrics- Finger points, voice print, palm scan, retina scan, hand geometry, etc.
  - Dialog- around the computer
- LOGICAL ACCESS CTRL
  - User Management:
    - User registration: user creation forms, authorization by respective departmental heads.
    - Privilege management
    - Password management
    - Periodical review of user rights to ensured that the privileges granted are inline with their CURRENT BUSINESS REQUIRMENTS.
  - Operating System Access CTRL:
    - First line of defense
    - Terminal Identification: Few accesses are only for particular machine.
    - Securing sensitive system utilities like disk formatting
    - Terminal time out/idle
  - Application software Access CTRL
    - Logging of user activities
    - Monitoring user access through IDS
    - Clock synchronization = critical for event logging
    - User Access right management.
- ROLE OF AN IS AUDITOR IN EVALUATING LOGICAL ACCESS CONTROLS (M'10- 5 Marks)

  An IS auditor should keep the following points in mind while working with logical access control mechanisms.
  - Reviewing the relevant documents pertaining go logical facilities and risk assessment and evaluation techniques and understanding the security risks facing the information processing system.
  - The potential access paths into the system must be evaluated by the auditor and documented to assess their sufficiency.
  - Deficiencies or redundancies must be identified and evaluated.
  - By supplying appropriate audit techniques, he must be in a position to verify test controls over access paths to determine its effective functioning

- He has to evaluate the access control mechanism, analyze the test results and other auditing evidences and verify whether the control objectives have been achieved.
- The auditor should compare security policies and practices of other organizations with the policies of their organization and assess its adequacy.

⇨ PHYSICAL ACCESS CONTROLS

☞ This section enumerates the losses that are incurred as result of perpetrations, accidental or intentional violation of access paths. The following issues are discussed:

- Physical Access Issues and Exposures
- Physical Access Controls
- Audit and evaluation techniques for physical access

☞ PHYSICAL ACCESS ISSUES AND EXPOSURES

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

- Abuse of data processing resources.
- Blackmail
- Embezzlement
- Damage, vandalism or theft to equipments or documents
- Modification of semester equipment and information.
- Public disclosure of sensitive information.
- Unauthenticated entry

☞ POSSIBLE PERPETRATORS: Perpetrations may be because of employees who are:

- Accidental ignorant-someone who outrageously violates rules
- Addicted to a substance or gambling
- Discontented
- Experiencing financial or emotional problems
- Former employee
- Interested or informed outsiders, such as competitors, thieves, organized crime and hackers
- Notified or their termination
- On strike
- Threatened by disciplinary action or dismissal

☞ ACCESS CONTROL MECHANISM

Discuss the three processes of Access Control Mechanism, when a user requests for resources. (N'09- 5 Marks)

- Access control mechanism processes the user request for resources in three steps. They are:
  - Identification
  - Authentication
  - Authorization
- The access control mechanisms operate in the following sequence:
  1. The users have to identify themselves, thereby indicating their intent to request the usage of system resources,
  2. The users must authenticate themselves and the mechanism must authenticate

itself, and

3. The users request for specific resources, their need for those resources and their areas of usage of these resources.

- The mechanism accesses
  - ✳ previously stored information about users,
  - ✳ the resources they can access, and
  - ✳ The action privileges they have with respect to these resources.
- The mechanism verifies this information against the user entries and it then permits or denies the request.
- Identification and Authentication:
  - ✳ Users identify themselves to the access control mechanism by providing information such a name, account number, badge, plastic card, finger print, voice print or a signature.
  - ✳ To validate the user, his entry is matched with the entry in the authentication file.
  - ✳ The authentication process then proceeds on the basis of information contained in the entry, the user having to indicate prior knowledge of the information.
- Authorization: There are two approaches to implementing the authorization module in an access control mechanism:
  - ✳ Ticket oriented:
    - In this approach the access control mechanism assigns the users a ticket for each resource they are permitted to access.
    - Ticket oriented approach operates via a row in the matrix.
    - Each row along with the user resources holds the action privileges specific to that user
  - ✳ List oriented: In this approach, the mechanism associates with each resource a list of users who can access the resource and the action privileges that each user has with respect to the resource.

☞ LOCKS ON DOORS:

Different types of locks on doors for physical security are discussed below:

- ✳ 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 sequence, and the door will unlock for a predetermined period of time, usually ten to thirty seconds.
  - Cipher Locks are used in **LOW SECURITY SITUATIONS** or when a large number of entrances and exists must be usable all the time.
  - More sophisticated and expensive cipher locks can be computer coded with a person's handprint.
  - A matching handprint unlocks the door.
- ✳ 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 not be duplicated.

* Electronic Door Locks:
  - A **MAGNETIC** or embedded **CHIP BASED PLASTICS CARD KEY** or token may be entered into a sensor reader to gain access in these systems.
  - The sensor device upon reading the special code that is internally stored within the card activates the door locking mechanism.
* Biometric Door Locks:
  - These locks are **EXTREMELY SECURE** where an individual's unique body features, such as voice, retina, fingerprint or signature, activate these locks.
  - This system is used in instances when **EXTREMELY SENSITIVE FACILITIES MUST BE PROTECTED**, such as in the military.

☞ PHYSICAL IDENTIFICATION MEDIUM

* Personal Identification numbers (PIN):
  - A secret number will be assigned to the individual, in conjunction with some means of identifying the individual, serves to verify the authenticity of the individual.
  - The visitor will be asked to log on by inserting a card in some device and then enter their PIN via a PIN keypad for authentication.
  - His entry will be matched with the PIN number available in the security database.
* Plastic Cards:
  - These cards are used for identification purposes.
  - Controls over card seek to ensure that customers safeguard their card so it does not fall into unauthorized hands.
* Cryptographic Control:
  - These types of controls help a lot in scheming unauthorized access to data.
  - Cryptography deals with transformation of data into codes that are meaningless to anyone who does not possess the system for recovering initial data.
  - Only a crypt analyst can do the translation.

☞ LOGGING ON UTILITIES

* 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 the front 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 gaining entry inside the company.
* Electronic Logging:
  - This feature is a combination of electronic and biometric security systems.
  - The users logging in can be monitored and the unsuccessful attempts being highlighted

☞ OTHER MEANS OF CONTROLLING PHYSICAL ACCESS

* 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.

- Security Guards :
  - Extra security can be provided by appointing guards aided with video cameras and locked doors.
  - Guards supplied by an external agency should be made to sign a bond to protect the organization from loss.
- Controlled Visitor Access:
  - A responsible employee should escort all visitors.
  - Visitors may be friends, maintenance personnel, computer vendors, consultants and external auditors.
- Bonded Personnel: All service contract personnel, such as cleaning people and off-site storage services, should be asked to sign a bond.
- 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 person permitted in the holding area.
  - Only a single person is permitted at a given point of time and this will surely reduce the risk of piggybacking, when an unauthorized person follows an authorized person through a secured entry.
- 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.
- Computer Terminal Locks: These locks ensure that the device to the desk is not turned on or disengaged by unauthorized persons.
- 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.
- Alarm System :
  - Illegal entry can be avoided by linking alarm system to inactive entry point motion detectors 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.
- Perimeter Fencing: Fencing at boundary of the facility may also enhance the security mechanism.
- 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

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

☞ ROLE OF IS AUDITOR IN PHYSICAL ACCESS CONTROLS (M'11 4 Marks):

Auditing Physical Access requires the auditor to review the physical access risk and controls to form an opinion on the effectiveness of the physical access controls. This involves the following:

i. Risk Assessment: The auditor must satisfy himself that the **RISK ASSESSMENT PROCEDURE ADEQUATELY COVERS PERIODIC AND TIMELY ASSESSMENT** of all assets, physical access threats, vulnerabilities of safeguards and exposures there from.

ii. Controls Assessment: The auditor based on the risk profile evaluates whether the physical access controls are in **PLACE AND ADEQUATE TO PROTECT THE IS ASSETS AGAINST THE RISKS**.

iii. Planning for review of physical access controls: It requires **EXAMINATION OF RELEVANT DOCUMENTATION** such as the security policy and procedures, premises plans, building plans, inventory list and cabling diagrams.

iv. Testing of Controls: The auditor should **REVIEW PHYSICAL ACCESS CONTROLS TO SATISFY FOR THEIR EFFECTIVENESS.** This involves:

- ✳ Tour of organizational facilities including outsourced and offsite facilities.
- ✳ Physical inventory of computing equipment and supporting infrastructure.
- ✳ Interviewing personnel can also provide information on the awareness and knowledge of procedures.
- ✳ Observation of safeguards and physical access procedures.
- ✳ Examination of physical access logs and reports. This includes examination of incident reporting logs and problem resolution reports.

⇨ ENVIRONMENTAL CTRLS

- ☞ Water detector
- ☞ Smoke detector
- ☞ Fire suppression system
- ☞ Placement of the computer room (no ground floor/ no top floor)
- ☞ Ups/ Electrical surge protectors (Spikes)/Generator
- ☞ Enclosed wiring
- ☞ Prohibition against eating & drinking within IPF (Information Processing Facilities)
- ☞ Emergency power off switch.

⇨ Role of Auditor in Environment Controls:

The attack on the World Trade Centre in 2001 has created a worldwide alert bringing focus on business continuity planning and environmental controls. Audit of environment controls should form a critical part of every IS audit plan. The IS auditor should satisfy not only the effectiveness of various technical controls but that the overall controls assure safeguarding the business against environmental risks. Some of the critical audit considerations that an IS auditor should take into account while conducting his audit are given below:

- Audit Planning and Assessment:

  As part of risk assessment:

  - The risk profile should include the different kinds of environmental risks that the organization is exposed to. These should comprise both natural and man-made threats. The profile should be periodically reviewed to ensure updation with newer risk that may arise.
  - The controls assessment must ascertain that controls safeguard the organization against all acceptable risks including probable ones and are in place.
  - The security policy of the organization should be reviewed to access policies and procedures that safeguard the organization against environmental risks.
  - Building plans and wiring plans need to be reviewed to determine the appropriateness of location of IPF, review of surroundings, power and cable wiring etc.
  - The IS Auditor should interview relevant personnel to satisfy himself about employees' awareness of environmental threats and controls, role of the interviewee in environmental control procedures such as prohibited activities in IPF, incident handling, and evacuation procedures to determine if adequate incident reporting procedures exist.
  - Administrative procedures such as preventive maintenance plans and their implementation, incident reporting and handling procedures, inspection and testing plan and procedures need to be reviewed.

- Audit of Technical Controls:

  Audit of environmental controls requires the IS Auditor to conduct physical inspections and observe practices. S/he must verify:

  - The IPF and the construction with regard to the type of materials used for construction.
  - The presence of water and smoke detectors, power supply arrangements to such devices, and testing logs.
  - The location of fire extinguishers, fire fighting equipment and refilling date of fire extinguishers.
  - Emergency procedures, evacuation plans and making of fire exists. If necessary, the IS Auditor may also use a mock drill to test the preparedness with respect to disaster.