

3.1 Control : An Introduction

- ◆ Information is now recognized as an enterprise's most valuable assets, so its protection from predators, both within and outside is very important. Organization need to be protected from both known and unknown threats and all the varieties and forms.
- ◆ Businesses today are under intense pressure to open up their networks, comply with increasingly rigorous regulatory requirements, and ensure their IT assets are protected from attack.
- ◆ Controls can be 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 or detected and corrected.

3.2 Need for control

- ◆ Reduction in the cost of data Loss
- ◆ Correct Decision Making
- ◆ Reduced costs of computer Abuse
- ◆ Increased value of computer hardware, software, personnel
- ◆ Reduced cost of computer error
- ◆ Maintenance of Privacy
- ◆ Controlled evolution of computer use
- ◆ Information system auditing
- ◆ Asset Safeguarding
- ◆ Data Integrity
- ◆ System Effectiveness
- ◆ System Efficiency

3.3 Effect of Computer on Internal Controls

The major areas of impact are as follows –

- (1) **Personnel** : We need to check whether or not staffs are trustworthy; they have the appropriate skills and training to carry out their jobs or not.
- (2) **Segregation of duties** : Segregation basically means to see that one person cannot process a transaction through from start to finish. However, in a computerised system, the auditor should also be concerned with the segregation of duties between the departments and within the IT department.

- (3) **Authorisation procedure** : In some online transaction systems written evidence of individual data entry authorization may be replaced by computerised authorization controls such as user name and password.
- (4) **Record keeping** : Automated controls will be required to protect the storage of documents, transaction details, and audit trails as they are in machine readable form.
- (5) **Access to assets & records** : In the manual systems assets could be protected from unauthorized access through the use of locked doors and filing cabinets. In the computerised systems computer programs and data are vulnerable to unauthorized amendment from remote locations. The use of wide area networks, including the internet, has also increased the risk of unauthorized access. The nature and types of control available have changed, to address these new risks.
- (6) **Management supervision** : Increased management's supervision and review helps to deter and detect both errors and fraud.
- (7) **Concentration of programs & 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 and 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 unauthorized access to, and alteration of financial data.

Internal controls used within an organisation comprise of the following five interrelated components:

1. Control Environment:

Management's policy and procedure, organization hierarchy and the ways authority and responsibility are assigned makes the control environment. This element implements controls in the CBIS.

2. Risk Assessment:

It is the elements that identify and analyze the risks faced by an organisation and the ways the risk can be managed.

3. Control Activities:

This element operates to ensure that transactions are authorized, duties are segregated, adequate documents and records are maintained, assets and records are safeguarded, and independent checks on performance occur. These are called Accounting controls.

4. Information and Communication:

It is the element, in which information is identified, captured and exchanged in a timely and appropriate form.

5. Monitoring:

This element ensure that internal controls operate reliably over time.

3.4 Effect of computer on Internal Audit

The move towards more automated financial systems has the following impact in the way auditors carry out their work -

- ◆ Changes in the evidence collection and;
- ◆ Change in evidence evaluation

3.4.1 Changes in the Evidence Collection

Audit trail is the key requirement in financial audit. Automated systems have made the following changes in audit trail and evidences.

3.4.1.1 Data retention and storage

- ◆ A client's storage capabilities may restrict the amount of historical data that can be retained on-line and readily accessible to the auditor. If the client has insufficient data retention capacities the auditor may not be able to review a whole reporting period's transactions.
- ◆ If the client uses a computerized financial system all or part of the audit trail may only exist in machine readable form. It can not be understood by the auditor what the Is and Os mean. The data must be translated into normal text by an additional process before it can be read and understood by the auditor.
- ◆ When a client gives the auditor a magnetic disk containing transaction details and data has been uploaded onto the auditor's machine, special audit software may be required to interrogate the information.

3.4.1.2 Absence of input document

In many accounting system transaction data may be entered into the computer directly without the presence of supporting document. The increasing use of EDI will result in less paperwork being available for audit examination.

3.4.1.3 Lack of visible audit trail

The audit trails in some computer systems may exist for only a short period of time. It calls 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.

3.4.1.4 Lack of visible output

In many systems processing may not produce a hard copy form of output, that makes it necessary for the auditor to directly access the electronic data retained on the client's computer. This is normally achieved by having the client provide a terminal and being granted "read" access to the required data files.

3.4.1.5 Audit evidence of automated transaction

Certain transactions may be generated automatically by the computer system. For e.g. a fixed asset system may automatically calculate depreciation on assets. Where transactions are system generated, the process of formal transaction authorization may not have been explicitly provided in the same way as in a manual environment. This may alter the risk that transaction may be irregular.

3.4.1.6 Legal issues

More and more organizations intend to make use of EDI and Electronic Trading over the Internet. This can create problems with contracts e.g. when is the contract made, where is it made, what are the terms of the contract and the parties to the contract.

The laws regarding computer evidence varies state to state, country to country and even court to court. If the auditor intends to gather evidence for use in a court, he should firstly find out what the local or national laws stipulate on the subject.

3.4.2 Changes in Evidence Evaluation

a. System generated transactions

Computerised financial systems may have the ability to initiate, approve and record financial transactions. Clients are starting to use these types of systems because they can increase processing efficiency and there will be no need to employ someone to do it manually. Automated transaction generation system are frequently used in inventory control system when a stock level falls below re-order level, the system automatically generates a purchase order and sends it to the supplier.

Automated transaction processing systems can cause the auditor problems. The auditor may need to look at the application's programming to determine if the programmed levels of authority (internal control) are appropriate.

b. Systematic Error

Computers are designed to carry out processing on a consistent basis. If the computer is doing the right thing, then with all other things being equal, it will continue to do right thing every time. Similarly, if the computer is doing the wrong thing or processing a transaction incorrectly, it will continue to handle the same type of transactions incorrectly, every time. Therefore, whenever an auditor finds an error in a computer processed transaction, he should be thorough in determining the underlying reason for the error. If the error is due to a systematic problem, the computer may have processed hundreds or more of similar transactions incorrectly.

Responsibility of Controls :-

Management is responsible for establishing and maintaining control to achieve the objectives of effective and efficient operations, and reliable information systems. Therefore, management must take systematic and proactive approach to do the following -

Long range planning	Long range planning and IT department
Short-range planning	Personnel management controls

3.4.3 Long range planning

The elements of long-range planning incorporate -

- ◆ Documented goal & objectives of the plan 0 Revenue and expense estimates.
- ◆ Time allowance and target date
- ◆ Strengths and weakness

3.4.4 Long -range planning and IT department

The information system manager must take systematic and proactive measures to -

- ◆ Develop & implement appropriate, cost-effective internal control structure
- ◆ Assess the adequacy of internal control
- ◆ Assess internal control to check their adherence to the information security policy of the organisation.
- ◆ Identify needed improvements;
- ◆ Take corresponding corrective action; and
- ◆ Report annually on internal control

3.4.5 Shot-range planning or Tactical Planning

The management is also responsible to develop plan for the functions and activities performed every day to meet the long range goals. For example Data processing job plan that defines daily processing activities.

3.4.6 Personnel Management controls

The management is responsible to develop plan to accomplish the administration of individuals. The control technique are-

- ◆ Job descriptions-
- ◆ Salary and benefits budget-
- ◆ Recruiting standards and criteria-
- ◆ Job performance evaluations -
- ◆ Screening and security standards-

3.5 The Audit Process :-

The focus of the audit process is not only on security which comprises confidentiality, integrity and availability but also on effectiveness and efficiency. The Audit of an IS environment may include one or both of the following:

- ◆ Assessment of internal controls.
- ◆ Assessment of the efficiency and effectiveness of the IS environment in economic terms.

3.5.1 Responsibility of IS Auditor

The audit objective and scope require some set of skills that is generally expected of an IS auditor. It include-

- ◆ Sound knowledge of business operations, practices and compliance requirements,
- ◆ Should possess the professional technical qualification and certifications,
- ◆ Good understanding of information Risks and Controls,
- ◆ Knowledge of IT strategies, Policy and procedure controls,
- ◆ Ability to understand technical and manual control,
- ◆ Good knowledge of Professional Standards and Best practices of IT controls.

3.5.2 Function of IS Auditor

IT Auditor often is the communicator of IT related business risk, to management. He can check, understand, assess the risk and present risk-oriented advice to management. IT auditors review risks relating to IT systems and processes, some of the IT related risks, reviewed by auditor, are:

- (i) Inadequate information security
- (ii) Inefficient use of corporate resources, or poor governance
- (iii) Ineffective IT strategies, policies and practices
- (iv) IT-related frauds

3.5.3 Categories of IS audits

IT audits has been categorized into five types:

(i) Systems and Applications:

To ensure valid, reliable, timely, and secure input, processing, and output at all levels of a system's activity.

(ii) Information Processing Facilities:

To ensure timely accurate, and efficient processing.

(iii) Systems Development:

To ensure 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.

(iv) Management of IT and Enterprise Architecture:

To verify that IT management has developed an organizational structure and procedures to ensure a controlled and efficient environment for information processing.

(v) Telecommunications Intranets and Extranets:

To verify that controls are in place on the client, server, and on the network connecting client and server.

3.5.4 Steps in Information Technology Audit

IT auditing can be categorized into six stages-

(i) Scoping and pre-audit survey:

In this stage the auditors determine the main areas of focus based on some risk-based assessment. Information sources at this stage include background reading, previous audit reports, pre audit interview, observations etc.

(ii) Planning and preparation:

In this stage scope is converted into plan including risk-control-matrix.

(iii) Fieldwork:

In this stage the actual audit work is performed by gathering evidence by interviewing staff and managers, reviewing documents, observing processes etc.

(iv) Analysis:

In this stage auditor sort and review all that evidence gathered earlier. SWOT or PEST techniques can be used for analysis.

(v) Reporting:

In this stage reporting to the management is done after analysis.

(vi) Closure:

In this stage preparing notes for future audits and following-up is done.

Steps 3 and 4 may on occasions involve the use of automated data analysis tools such as ACL or IDEA, Excel, Access and SQL queries.

3.5.5 Audit Standards

IS auditors need guidance and a different yardstick to measure the Economy, Efficiency and Effectiveness of a system. Such as -

- ◆ How IS should be assessed to plan their audits effectively?
- ◆ How to focus their effort on high-risk areas and;
- ◆ How to assess the severity of any errors or weaknesses found.

The Institute of Chartered Accountants of India has issued AASs covering various aspects. Although these standards are primarily concerned with the audit of financial information, they can be adapted for the purposes of IS Audit. Several well known organizations have given practical and useful information on IS Audit.

3.5.6 ISACA (Information Systems Audit and Control Association)

ISACA is a global leader in information governance, control, security and audit. ISACA developed the following to assist IS auditor while carrying out an IS audit.

- ◆ IS auditing standards
- ◆ IS auditing guidelines
- ◆ IS auditing procedures

3.5.7 ISO 27001

Also known as ISMS (Information Security Management Standard), it is a global standard issued by ISO and IEC in October 2005. ISO/IEC 27001 : 2005 is designed to ensure the selection of adequate and proportionate security controls that protect information assets. It helps organizations in -

- ◆ Identification of existing information security management.
- ◆ Formulating security requirements
- ◆ Managing security risks in cost effective manner
- ◆ To ensure compliance with laws and regulations
- ◆ To provide relevant Information about information security policies to trading partners and other organizations.

3.5.8 IIA (The Institute of Internal Auditors)

IIA has issued Global Technology Audit Guide(GTAG) which provides IS auditors with guidance on different information technology associated risks and recommended practices.

3.5.9 ITIL (IT Infrastructure Library)

It is the best practice in IT Service Management, developed by OGC. It gives a detailed description of a number of important IT practices with comprehensive checklists, tasks and procedures that can be tailored to any IT organization. ITIL provides a systematic and professional approach to the management for IT services. ITIL consists of a series of books giving guidance on the provision of quality IT services

3.5.10 Control Objectives for Information related Technology

- ◆ The IS Audit and Control Foundation (ISACF) developed the Control Objective for Information and related Technology(COBIT). COBIT help managers learn to balance the risk and control investment.
- ◆ It provides users with greater assurance that the security and IT controls provided are adequate. It also guides auditor to review the existing control structure and advice management on internal control.
- ◆ COBIT is a framework of generally applicable information systems security and control. The framework allows -
 1. Benchmarking of the security and control arrangement.
 2. Users of IT services to be assured that adequate security and control exist
 3. Auditor to review internal controls and advise on IT security matters.

The framework addresses the issue of control from 3 vantage point -

- 1) Business Objectives : To satisfy business objectives, information must satisfy some criteria that COBIT refers to as business requirement for information. The criteria are divided into 7 categories : Effectiveness, Efficiency, Confidentiality, Integrity, Availability, Compliance with legal requirement and Reliability.
- 2) IT Resources : To protect the IT resources which includes People, Application system, Hardware devices, Facilities and Data, security controls must be developed.
- 3) IT Processes : Controls are required to be implemented in all the processes, which are broken into 4 domains: Planning and organization, Acquisition and implementation, Delivery and support, & Monitoring.

3.5.11 Cost-Effectiveness of Control

- ◆ Cost effectiveness of controls means benefits of an internal control must exceed its cost. Since too many controls can negatively affect operational efficiency, therefore, the objective of designing internal control system is to provide reasonable assurance that control problems do not take place.
- ◆ Costs are easier to measure than benefits because most of the control benefits are intangible, however, the primary cost elements are -

Implementing & 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 cost:** The control has operated reliably in signaling 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 cost:** The cost associated in ensuring the correct working of a control. For example, rewriting input validation routines as the format of input data changes.
- ◆ Internal control benefits can be seen in the form of Reduced losses. One way to calculate benefits involves expected loss i.e. mathematical product of risk and exposure. Here benefits of a control procedure is the difference between the expected loss with the control procedure and the expected loss without it.
 - ◆ After estimating benefits and costs, management determines whether the control structure is cost-effective or not.
 - ◆ In evaluating cost / benefit of control procedure, management must consider factors other than those in the expected benefit calculation. For e.g. if an exposure threatens an organization's existence, it may be worthwhile to spend more than indicated by the cost-benefit analysis.

3.6 Information system control technique

The basic purpose of IS 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 control framework, which comprise policies, procedures, practices and organization structure that gives reasonable assurance that the business objectives will be achieved.

3.6.1 Objectives of Controls

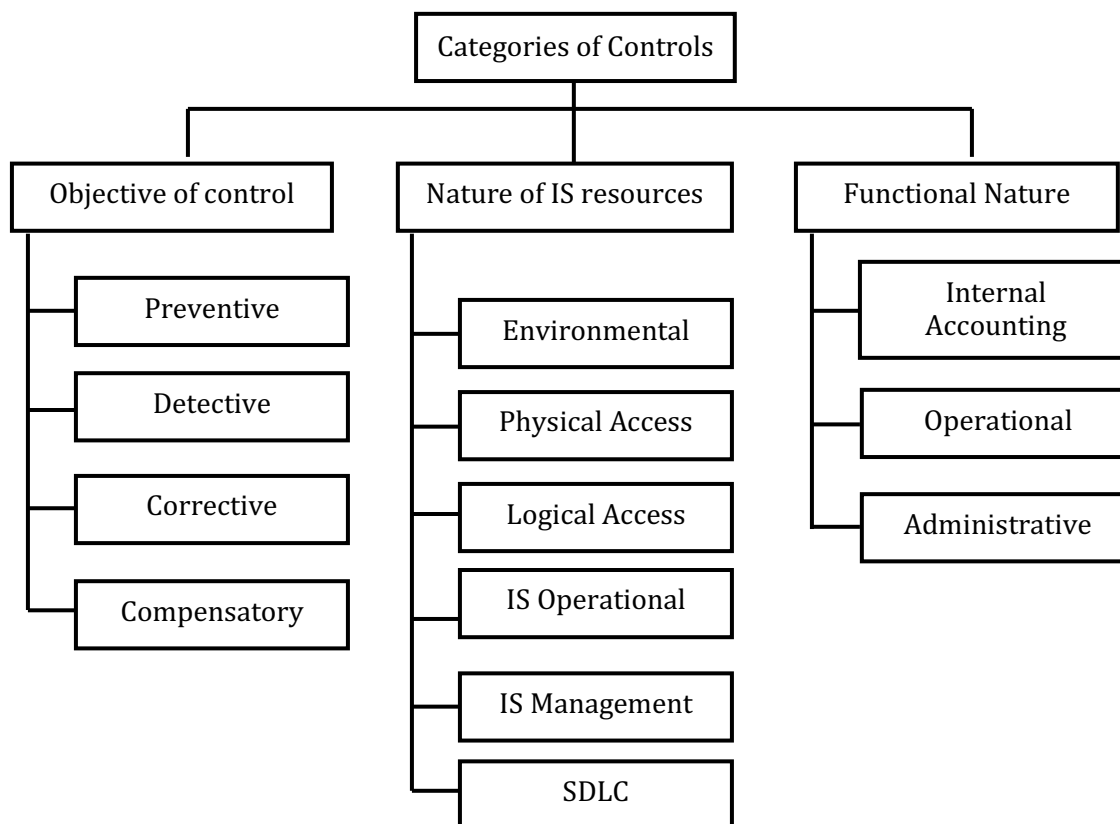
The objective of controls is to reduce or if possible eliminate the causes of the exposure to potential loss. Some categories of exposures are :

- ◆ Errors or omissions
- ◆ Improper authorizations and improper accountability
- ◆ Inefficient activity in processing
- ◆ Lack of management understanding of IS risks
- ◆ Absence or inadequate IS control framework
- ◆ Weak general control
- ◆ Lack awareness and knowledge of IS risk.
- ◆ Distributed computing environments
- ◆ Inappropriate technology implementations

Control objective is defined as "A statement of the purpose to be achieved by implementing control procedures in IT process". The statement of controls serve two main purposes:

1. Outline the policies of the organization as laid down by the management.
2. A benchmark for evaluating whether control objectives are met.

3.6.2 Categories of Controls



3.6.2.1 Controls on the basis of Objectives

We put controls into 4 categories depending on the objectives of control -

(i) Preventive controls:

Preventative controls are those which are designed to prevent an error, omission or malicious act that may occur in financial system. For implementing preventive controls knowledge of the following is required -

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

Some of the preventive controls are -

- | | |
|--------------------------------|----------------------------|
| ◆ Employ qualified personnel | ◆ Segregation of duties |
| ◆ Login procedure | ◆ Access privilege control |
| ◆ Documentation | ◆ Training of staff |
| ◆ Authorization of transaction | ◆ Data validation controls |
| ◆ Firewalls | ◆ Anti-virus software |

(ii) Detective Controls:

These controls are designed to detect error, omission or malicious acts that occur in the system and report the occurrence. The main characteristics of these controls are -

1. It require clear understanding of lawful activities so that anything which deviates from these is reported.
2. It require an established mechanism to refer the reported unlawful activities to the appropriate person.
3. It interacts with the preventive control to prevent such acts in future.
4. It ensures surprise checks by supervisor.

Some of the Detective controls are -

- ◆ Hash total
- ◆ Check points during processing
- ◆ Echo check
- ◆ Duplicate checking of calculations
- ◆ The internal audit functions
- ◆ Intrusion detection system
- ◆ Bank reconciliation
- ◆ Monitoring expenditures against budgeted amount

(iii) Corrective Controls:

Corrective controls are designed to reduce the impact of an error or correct an error, once it has been detected. The main characteristics of these controls are -

1. They minimizes the impact of the threat.
2. They help in identifying the cause of the problem.
3. They provide remedy of the problem discovered by detective controls.
4. They get feedback from preventive and detective controls.
5. They correct error arising from a problem.
6. They help in modifying the processing systems to minimize future occurrences of the problem.

Some of the Corrective controls are -

- ◆ Contingency planning
- ◆ Backup procedure
- ◆ Rerun procedure
- ◆ Change input value to an application systems
- ◆ Investigate budget variance and report violations

(iv) Compensatory Controls:

While designing the appropriate control one thing should be kept in mind that the cost of the lock should not be more than the cost of the asset it protects. Sometimes while designing and implementing controls, organizations may not be able to implement appropriate controls because of different constraints such as financial, administrative or operational. In such a scenario, there should be adequate compensatory measure which may although not be as efficient as the appropriate control, should be implemented.

These controls are basically designed to reduce the probability of threat that causes a loss to an asset. Some of the Compensatory controls are -

- ◆ Audit Trail
- ◆ User controls
- ◆ Error Correction

a. Audit Trails

Audit trails are logs that can be designed to record activity at the system, application and user level. When implemented properly, it provide an important detective tool.

Logs also provide valuable evidence on assessing both the adequacies of controls in place and the need for additional controls.

Audit logs, however, can generate data in high volume, thus poorly designed logs can actually be dysfunctional. Although, many operating systems allow management to select event will be recorded in the log. Audit trail can be used to support security objectives in three ways -

1. *Detecting unauthorised access to the system*- It can occur in real time or after the event. The objective of real time detection is to protect system from attempts to breach the system control. A real time audit trail can also be used to report the breach attempts. After the event log file can be used to record system activities electronically and can be reviewed periodically.
2. *Facilitating the reconstruction of events* - Knowledge of the condition that existed at the time of a system failure can be used to reconstruct the system and to avoid similar situation in the future.
3. *Promoting personal accountability* - Audit trail can be used to monitor user activity at the lowest level of detail. This can be used to influence behavior and promote personal accountability.

b. User Controls

User controls over data being processed should include -

- ◆ Development of user instruction manuals
- ◆ Input controls that identify all data entering the processing cycle
- ◆ Processing controls that includes data validation, error handling, audit trails etc.
- ◆ Output controls to verify the correctness of the reports.
- ◆ Separation of duties between preparing the input and verifying the output.

c. Error Correction

Following controls are exercised over error correction -

1. Identify all data and processing errors and determine their impact on processing
2. Determine if errors are cumulated into a suspense file
3. Determine how errors are corrected

4. Determine if the corrected transactions are authorised
5. Verify that the corrected transactions are re-inserted into mainstream processing.
6. Determine if the error correction process removes the item from error suspense file.
7. Determine the timeliness of error correction.
8. Is there an appropriate separation of duties for custody, authorization, recording and re-conciliation of data updation.
9. Documentation of all error correction and re-conciliation procedure.
10. Verify the existence of exception error reports for long outstanding error transactions.

3.6.2.2 Controls on the basis of nature of IS resources

Another classification of controls is based on the nature of such controls with regard to the nature of resource to which they are applied -

- (i) Environmental controls:** Controls relating to Power, Air-conditioning, UPS, Smoke detection, Fire-extinguishers, de-humidifiers etc.
- (ii) Physical Access controls :** Controls relating to physical security of the IS resources include Access control doors, Security guards, door alarms, restricted entry to secure areas, visitor logged access, video monitoring etc.
- (iii) Logical Access controls:** Controls relating to logical access to information resources such as OS controls, Application software controls, Networking controls, Encryption controls etc.
- (iv) IS Operational Controls :** Controls relating to IS operation and administration such as Timing controls, IS infrastructure management, Help desk operations etc.
- (v) IS Management Controls:** Controls relating to IS management, policies, procedures, standards and practices, monitoring of IS operations, Steering committee etc.
- (vi) SDLC Controls:** Controls relating to planning, design, development, testing, implementation and post implementation, change management.

3.6.2.3 Controls on the basis of Functional Nature

Another category of controls is based on their functional nature. The controls in this category are:

(i) Internal Accounting controls :

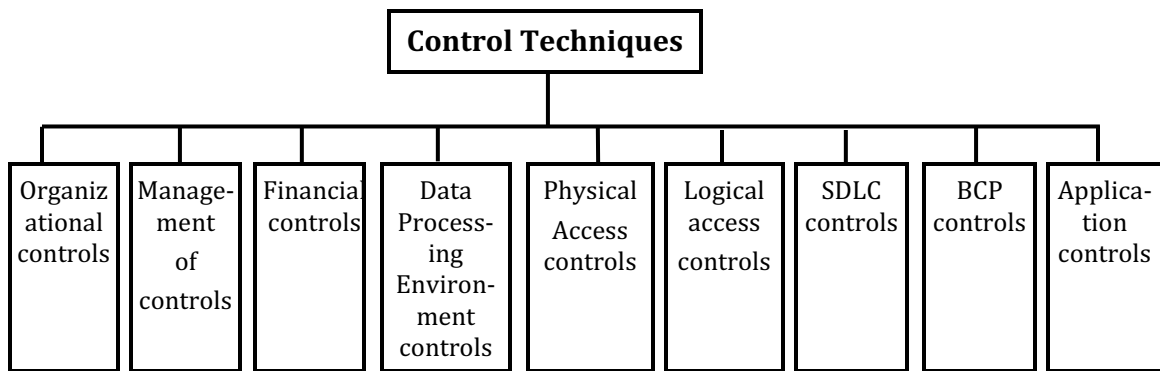
Controls to safeguard the client's assets and to ensure the reliability of the financial records.

(ii) Operational controls :

These controls deals with the day to day operations to ensure that the operational activities are contributing to business objectives.

(iii) Administrative controls:

Controls to ensure efficiency and compliance with management policies.

3.6.3 Control Techniques**3.7 Organizational Controls :-**

These controls are concerned management authorization of transactions. Organizational control techniques include the followings -

3.7.1 Responsibilities and objectives

Each IS function must be clearly defined and documented, including systems software, application programming and systems development, database administration and operations. The IS management team is responsible for the effective and efficient utilization of IS resources, so they set the objectives to be achieved and responsibilities of resource utilization. Their responsibilities include:

- ◆ Providing information to senior management on the IS resources
- ◆ Planning for expansion of IS resources
- ◆ Controlling the use of IS resources
- ◆ Implementing activities that support companies strategic plan

3.7.2 Policies, Standards, Procedures and Practices

These are the standards and instructions that all IS personnel must follow when completing their assigned duties. Policies establish the rules delegated to individuals in the enterprise.

Procedures establish the instructions that individuals must follow to compete their daily assigned tasks. Documented policies should exist in IS for:

- ◆ Use of IS resources,
- ◆ Physical security,
- ◆ Data security
- ◆ On-line security,
- ◆ Microcomputer use,
- ◆ Reviewing, evaluating, and purchasing hardware and software,
- ◆ System development methodology, and
- ◆ Application program changes.

3.7.3 Job descriptions

These communicate management's expectations for job performance. It provides instructions on how to do the job. All jobs must have a current, documented job description readily available to the employee. It establishes responsibility and the accountability.

3.7.4 Segregation of duties

It is aimed at separating conflicting job duties to discourage fraud. Such separation can also force an accuracy check of one-person work by another. Examples of segregation of duties are :

- ◆ Systems software programming from the application programming
- ◆ Database administration from other data processing activities
- ◆ Computer hardware operations from the other groups
- ◆ Application programming group into various subgroups for individual application systems
- ◆ Systems analyst function from the programming function
- ◆ Physical, data, and online security group(s) from the other IS functions.
- ◆ IS Audit

From a functional perspective, segregation of duties should be maintained between the following functions:

- ◆ Information systems use
- ◆ Computer operation
- ◆ System administration
- ◆ Change management
- ◆ Security audit
- ◆ Data entry
- ◆ Network management
- ◆ Systems development and maintenance
- ◆ Security administration

3.8 Management Controls

The controls adopted by the management to ensure that the information systems functions correctly and meet the strategic business objectives. The scope of control includes framing IT policies, procedures and standards on a holistic view. The controls to consider when reviewing management controls in an IS system shall include:

Responsibility : A senior management personnel responsible for the IS within the organisational structure.

An official IT structure : There should be a prescribed organisation structure with clear roles and responsibilities through written and agreed job descriptions.

An IT steering committee : The steering committee shall comprise of user representatives from all areas of the business, management representative & IT personnel.

3.9 Financial Control

These controls are exercised by the system user personnel over source of transactions and documents before system input. The financial control techniques are numerous. A few examples are highlighted here:

- i) **Authorization:** Access to such assets as accounting entries must be authorised.
- ii) **Budgets:** These are the estimates of the amount of time or money expected to be spent during a particular period of time, project, or event.
- iii) **Cancellation of documents:** This is atypical control over invoices marked with a "paid" or "processed" stamp or punching a hole in the document to prevent its reuse..
- iv) **Documentation:** This includes written instructions to explain how to perform the task and also written explanations of actual task performed.
- v) **Dual control:** This entails having two people simultaneously access an asset. For example, the filling of money in ATM should be performed by two people present.
- vi) **I/O verification:** This entails comparing the information provided by a computer system to the input documents.
- vii) **Safekeeping:** This entails physically securing assets under lock and key.
- viii) **Segregation of duties:** This entails assigning similar functions to separate people to provide reasonable assurance against fraud and provide an accuracy check.
- ix) **Sequentially numbered documents:** These are working documents with preprinted sequential numbers, which enables the detection of missing documents.
- x) **Supervisory review:** This control requires a sign-off on the documents by the supervisor, in order to provide evidence that the supervisor at least handled them.

3.10 Data processing Environment Controls

These controls are hardware and software related and exercised in the IS environmental areas that include system software programming, on-line programming, database administration, media library, application program change control etc.

3.11 Physical Access Controls

These controls are exercised on access to IT resources by employees/outside. These Physical security and access controls should address not only the area containing system hardware, but also locations of wiring used to connect elements of the system, supporting services (such as electric power), backup media and any other elements required for the system's operation. Access should be restricted to authorized individuals. IT management should ensure a low profile is kept and the physical identification of the site of the IT operations is limited. The other measures relate to Visitor Escort, Personnel Health and Safety, Protection against environmental Factors and Uninterruptible Power Supply.

3.12 Logical Access Controls

These controls are software related controls used to ensure that access to systems, data and programs is restricted to authorized users. The key factors in designing logical access controls include authorization, authentication and access control, user identification and authorization profiles, incident handling, reporting and followup, virus prevention and detection, firewalls user training and intrusion testing and reporting etc.

3.13 SDLC (System Development Life Cycle) controls

These are functions that control the development of application systems. The first control is system development standards that specify the activities that should occur in each system development life cycle (SDLC) phase. Second control is the standards that specify the type and quantity of testing that should be conducted. The third element of controls is documented procedures.

3.14 Business Continuity (BCP) Controls

These controls relate to having an operational and tested IT continuity plan. The controls include criticality classification, alternative procedures, backup and recovery, systematic and regular testing and training, monitoring and fallback and resumption plans, risk management activities, assessment of single point of failure.

3.15 Application Control Techniques

These include the programmatic routines within the application program code to ensure that data remains complete, accurate and valid during its input, update and storage. The specific controls include form design, source document controls, input, processing and output controls, media identification, data back-up and recovery.

3.16 Audit Trails

Audit trails are logs that can be designed to record activities at the system, application, and user level. It is an important detective control to help accomplish security policy objectives.

Audit trail controls attempt to ensure that a chronological record of all events that have occurred in a system is maintained. This record is needed to answer queries, fulfill statutory requirement, detect the consequences of error and allow system monitoring and tuning.

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

i. Detecting Unauthorized Access:

Detecting unauthorized access can occur in real time or after the fact, to protect the system from outsiders who are attempting to breach system controls. 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.

ii. Reconstructing Events :

Audit analysis can be used to reconstruct the steps that led to event 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 avoid similar situations in the future. The audit trail can be used to reconstruct accounting data files that were corrupted by a system failure.

iii. 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, if they know that their actions are recorded in an audit log.

Implementing an Audit Trail:

The information contained in audit logs is useful in measuring the potential damage associated with application errors, abuse of authority, or unauthorized access by outside intruders. Logs also provide valuable evidence on both the adequacies of controls and the need for additional controls. Audit logs, however, can generate data in overwhelming detail, thus, poorly designed logs can actually be dysfunctional.

3.17 User Controls

A counter clerk at a bank is required to perform various business activities as part of his job description and assigned responsibilities. He is able to relate to the advantages of technology when he is able to interact with the computer system from the perspective of meeting his job objectives. The following user controls are exercised for system effectiveness and efficiency.

3.17.1 Boundary Controls

The major controls of the boundary system are the access control mechanisms. The access control mechanism has three steps - Identification, Authentication and Authorization with respect to the access control policy. The user can provide three classes of input information for the authentication process and gain access to his required resources.

Class of information	Types of input
Personal Information	Name, Birth date, account number, password, PIN
Personal characteristics	Fingerprint, voice, palm print, Signature, Retinal pattern.
Personal objects	Identification cards, badge, key, finger ring:

Boundary control techniques are:

3.17.1.1 Cryptography

It involves transforming data into codes that are meaning less to anyone who does not possess the authentication to access the respective data/file. The three techniques of cryptography are Transposition, Substitution and product cipher (combination of transposition and substitution).

3.17.1.2 Passwords

User identification by 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. The best practices followed to avoid failures in this control system are; minimum password length, avoid usage of common dictionary words, periodic change of passwords, encryption of passwords and number of entry attempts.

3.17.1.3 Personal Identification Numbers (PIN)

The personal identification number is similar to a password assigned to a user by an institution. PIN is vulnerable to exposed while issuance, delivery, transmit or store.

3.17.1.4 Identification Cards

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

3.17.2 Input Controls

These are responsible for ensuring the accuracy and completeness of data and instruction input into an application system. Input controls are important since input of data, involve human intervention and are therefore error and fraud prone. Poorly designed data codes cause recording and keying errors. Types of data coding errors:

Addition	:	Addition of an extra character in a code e.g. 54329 coded as 543219
Truncation	:	Omission of characters in the code e.g. 54329 coded as 5439
Transcription:		Recording wrong characters 54329 coded as 55329
Transposition:		Reversing adjacent characters 54329 coded as 45329
Double transposition:		Reversing characters separated by one or more characters i.e. 54329 is coded as 52349

Factors affecting coding errors as follows:

- **Length of the code:** Long codes are naturally prone to more errors therefore they should be broken using hyphens, slashes or spaces to reduce coding errors.
- **Alphabetic numeric mix:** The code should provide for grouping of alphabets and numerical separate if both are used. Intermingling both would result in more errors.
- **Choice of characters:** Certain alphabets are confused with numerical such as B, 1,0, S, V and Z would be confused with 8,1,0,5,U, 2. Such characters should be avoided.
- **Mixing uppercase / lowercase fonts :** Upper case and lower case should NOT be mixed when using codes since they delay the process of keying in due to usage of the shift key.
- **Sequence of characters:** Character sequence should be maintained as much as possible. Such as using ABC instead of ACB.

Control used to guard against these types of errors is a "Check Digit". Check digits are redundant digits that helps verify the accuracy of other characters in the code that is checked. The program recalculates the check digits and compares with the check digit in the code when the code is entered to verify If the code is correct. Check digits may be prefixes or suffixes to the actual data.

3.17.3 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 the DBMS, however, adequate controls should be enforced through the front end application system also to have consistency in the control process. Data processing controls are:

- ◆ **Run-to-Run totals:**
- ◆ **Reasonableness verification :** Two or more fields can be cross verified to ensure their correctness.
- ◆ **Edit check:** The data validation controls to verify accuracy and completeness of data.
- ◆ **Field initialization:** Setting all values to zero before.
- ◆ **Exception reports :** Exception reports are generated to identify errors in data processed. Such exception reports give the transaction code and reason why the particular transaction was not processed.
- ◆ **Existence/Recovery Controls:** The check point/Restart logs facility is a short-term backup and recovery control that enables a system to be recovered if failure is temporary and localized.

3.17.4 Output Controls

These ensure that the data delivered to users will be presented, formatted and delivered in a consistent and secured manner.

- ◆ **Storage and logging of sensitive, critical forms :** Pre-printed stationery should be stored securely to prevent unauthorized destruction or removal and usage.
- ◆ **Logging of output program execution :** When programs used for output of data are executed, it should be logged and monitored.
- ◆ **Spooling/Queuing:** When a file is to be printed the operating system stores the data stream to be sent to the printer in a temporary file on the hard disk. This file is sent to the printer as soon as the printer is read to accept the data. This intermediate storage of output could lead to unauthorized disclosure or modification
- ◆ **Controls over printing :** Users must be trained to select the correct printer and access restrictions may be placed on the workstations that can be used for printing.

- ♦ **Report distribution and collection controls** : Distribution of reports should be made in a secure way to prevent unauthorised disclosure of data. Distribution should be made immediately after printing to ensure that the time gap between generation and distribution is reduced. A report log should be maintained.
- ♦ **Retention controls** : Retention controls consider the duration for which outputs should be retained before being destroyed.
- ♦ **Existence/Recovery Controls** : are needed to recover out in the event that it is lost or destroyed. Check point /restart log helps in recovery when a hardware problem causes a program that prints customer invoices to abort in midstream.

3.17.5 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 database controls. They are classified into two categories as Update controls and Report controls. The update controls are -

- ♦ **Sequence Check:** 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.
- ♦ **Ensure entire file processing:** While processing; the transaction file records check processing upto end-of-file.
- ♦ **Process multiple transactions for a single record in the correct order:** Multiple Tr. can occur based on a single master record (e.g. dispatch of a product to different distribution centers).
- ♦ **Maintain a suspense account:** When mapping between the master record to transaction record results in a mismatch then these transactions are maintained in a suspense account.

The Report controls are:

Standing Data: Application programs use many internal tables to perform various functions say billing calculation based on a price table. Maintaining integrity of the pay rate table, price table and interest table is critical within an organization. Periodic monitoring of these internal tables by means of manual check or by calculating a control total is mandatory.

- ♦ **Run-to-Run control:** Run-to-Run control totals help in identifying errors or irregularities like wrong sequence of updating.
- ♦ **Print Suspense Account Entries** : Similar to the update controls the suspense account entries are to be periodically monitored with the respective error file and action taken on time.
- ♦ **Existence/Recovery Controls:** The back-up and recovery strategies required to restore failure in a database. Recover strategies involve roll-forward (current state database from a previous version) or the roll-back (previous state database from the current version) method.

3.18 System Development and Acquisition controls

It is important to have a formal, appropriate, and proven methodology to govern the development, acquisition, implementation, and maintenance of information systems. Methodology should contain appropriate controls for management review and approval, user involvement, analysis, design, testing, implementation, and conversion.

Many institutes have provided framework that helps organizations to design their control structure. Some of them are : Acquire and Implement-7 (AI7), Control Objectives for Information and related Technology (COBIT) Capability Maturity Model (CMM), IT Infrastructure Library (ITIL), ISO/IEC 17799 and COSO. The following controls are put in place in system development process:

3.18.1. Problem definition

The stakeholders must understand the nature of the problem they are addressing. This can be done through a formal process. The controls are -

- Determine the need for the IS in the view of business objectives
- Support and priority for the information system by the management.
- Level of acceptance among the stakeholders on the need for change.
- Investigate to justify the need for the system.

Auditor's Role -

The Auditors are concerned with-

- Check whether the stakeholders have reached an agreement on the existence of a problem.
- Understand the threats to asset safeguarding, data integrity, system effectiveness and system efficiency associated with the solutions proposed for the system.

3.18.2. Management of the change process

Change-facilitation deals with the following critical activities -

- Preparing the organization for change by feedback, training, participatory decision making and promote the need for change.
- Complete change over to the new system.
- To help users adapt to their new roles.

The Controls are -

- Budgeting
- Checkpoints
- Exception reporting,
- User coordination.

Auditor's Role

- To evaluate the quality of procedure of change facilitation.
- Suggest that change management can be done in-house, if the proposed system is small and has a localized impact on users.
- If the proposed system is large and has high-levels of requirements and technological uncertainty then determine the effect on organization structures and jobs.

3.18.3. Entry and feasibility assessment

The specific techniques used to evaluate the feasibility of systems depend on the type and size of the system being proposed. The controls are –

- **Technical Feasibility:** Can technology be acquired, developed or available to support the proposed project?
- **Operational Feasibility:** Can the system be designed to process inputs and give required outputs?
- **Economic Feasibility:** The proposed system is deemed feasible only if the benefits exceed all the cost requirements.
- **Behavioral Feasibility:** Can the system improve the quality of work life of the users?

Auditor's Role

- Determine that the change proposed is not imposed upon stakeholders.
- Determine the behavioral impact on the users and the problems that arise.
- Determine the material losses incurred as result of the development, implementation, operation or maintenance of the system.

3.18.4. Analysis of the existing system

It is essential to understand the existing system. The controls are -

- Study the history of the system in the organization.
- Study the existing information flows using modeling.

Auditor's Role

- Study the aspects of the present organizational structure, history & culture.
- Study the context in which the decisions for the new proposed system choice was made and its implications for the conduct of the audit.
- Evaluate the quality of methodologies used.
- Analyse the usage of high-quality tools in analysis and documentation.

3.18.5. Formulation of strategic Requirements (System Design)

The strategic requirements also called as the SRS document. The controls are -

- Align the business requirements with the management's objectives and user's goals.
- Elicitation of the requirements and system-design work concurrently.

Auditor's Role

- Evaluate the quality of the SRS design work.
- Evaluate the feasibility of the system-design proposed.
- Assess the identified procedures and substantial behavioral impact on the users.

3.18.6. Organizational and job design

Adapting the organizational structures and job responsibility with respect to the proposed system often leads to behavioral problems among its stakeholders and may result in implementation failure. The **Controls** are -

- The roles and responsibilities of users of the system are to be defined using formal traditional mechanism.
- A clear design of the responsibilities in the initial design phase.

Auditor's Role

- Assess the assigned responsibility and process used to resolve conflicts.
- Assess the control risk associated with the responsibilities during SDLC with substantive testing.

3.18.7. Information processing systems design

From efficiency viewpoint the reliability of the controls designed into the system are to be evaluated. The major control activities in the processing systems design phase are -

- **Requirements elicitation:** Interview, GD, Prototyping.
- **User interface design:** Source document, Screen layout, Report formats, Icons.
- **Data/Information flow design:** DFD.
- **Database design:** Conceptual modeling, data modeling, physical layout.
- **Platform design :** H/w and S/W design, modularity, generality.
- **Physical Design :** Identify boundaries, Modules, Packages and Programs.

Auditor's Role

- To evaluate the appropriateness of the requirements-elicitation strategy.
- To evaluate the system design needs to capture all data information flow within the system.
- To evaluate the structure of the database design and cost of the data model.
- To evaluate the design and quality of the interface that needs to follow best design practices.
- To evaluate the efficiency of the tasks assigned to the appropriate hardware and software resources of the physical design of the system.

3.18.8. Application Software Acquisition/Selection Process

Once the information processing is identified and designed then the application software may be acquired or developed in-house. The controls are -

- Information & system requirements need to meet business & system goals.
- A feasibility analysis to define the constraints or limitations for each alternative system from a technical as well as a business perspective.
- A detailed Request for Proposal (RFP) document needs to specify the acceptable requirements (functional, technical, and contractual).
- The vendor evaluation process considers the following:
 - Stability of the supplier company,
 - Volatility of system upgrades,
 - Existing customer base,
 - Supplier' s ability to provide support,
 - Cost-benefits of the hardware/software in support of me supplier application,
 - Customized modifications of the application software.

Auditor's Role

- To highlight risks before a vendor contract or a software agreement contract is signed.
- To ensure that the decision to acquire software should flow from the thorough feasibility study, vendor evaluation and RFP adequacy checked for.
- A RFP would include transaction volume, data base size, turnaround time and response time requirements and vendor responsibilities.
- Check the criteria for pre-qualification of vendors and sufficient documentation available to justify the selection of the final vendor.
- The auditor may also collect information through his own sources on vendor viability, support infrastructure, Service record.
- Review the contract signed with the vendor for adequacy of safeguards and completeness. The contract should address the contingency plan in case of vendor failures.
- To ensure that the contract went through legal scrutiny before it was signed.

3.19 Control over System and Program changes

3.19.1 Management of the change process

- ◆ The complexity of hardware, software, and application relationships in the operating environment needs well defined, planned, coordinated, tested, and implemented change management. The change process involves the following tasks:
 - Provide feedback to the system stakeholders
 - Prevents system disruptions
 - Accept changeover to a new system across the organization
 - Helps users to adapt to new roles
 - Documentation of the implemented process changes.
 - Review proposed change to identify potential conflicts with other Systems.
 - Review the change management process periodically to evaluate its effectiveness.
- ◆ All requests for change are set on priority of urgency by IT steering committee. The priority of changes is determined by assessing the cost of the change and its impact on the business.
- ◆ Quality assurance, security, audit, regulatory compliance, network, and end-user personnel should be appropriately included in change management processes.
- ◆ Change management must ensure that all changes are approved, documented, and disseminated.
- ◆ Change controls should address all aspects of an organization's technology environment including software programs, hardware and software configurations, operational standards and procedures, and project management activities.

3.19.2 System Change Controls

- ◆ Periodically review all systems for needed changes.
- ◆ All requests for change must be submitted in a standardized format.
- ◆ Maintain log of all the requests for changes to the system.
- ◆ Categorize and rank all change requests on the basis priorities and assess their impact on system reliability, objective and security.
- ◆ Implement specific procedures to handle urgent matters such as management review and approval. Make sure that audit trail for all urgent is maintained.
- ◆ Communicate all changes to management and obtain written approval.
- ◆ Require IT management to review, monitor, and approve all changes to hardware, software.

- ◆ Assign role and responsibility to those involved in the change and make sure that adequate segregation of duties is maintained.
- ◆ Control access rights to avoid unauthorised access to the system.
- ◆ Review the change procedure to ensure that all changes go step by step.
- ◆ Obtain test results to ensure that all changes are extensively tested, separately in non-production environment.
- ◆ Make sure there is a provision of rollback any changes in case it does not work properly.
- ◆ Implement a quality assurance to ensure that all standards are followed in change management.
- ◆ Update all documentation after all changes are implemented.

Auditor's Role

- ◆ To evaluate the quality of decisions made with respect to change facilitation.
- ◆ If the proposed system is small, the change management can be done in-house with less material concerns.
- ◆ The Change Control process of a system under development is to address the problems not detected during system design or testing. A change control evaluation includes checks on problems reporting, tracking; prioritizing, and resolving. The risks the change control processes deal with are:
 - System outages due to error, omissions, or malicious intent,
 - Data loss or errors due to error, omissions, or malicious intent,
 - Unauthorized changes,
 - Fraud / abuse to company systems and data,
 - Repeated errors, and
 - Reruns of system or application processes.
- ◆ The objective of a change management review are to ensure that changes made to the system and programs do not adversely affect system, application, or data.

3.19.3 Program Change Controls

- ◆ Implementing controls over the modification of application software programs is to ensure that only authorized programs and modifications are implemented.
- ◆ Failure of proper controls leads to risks in software security like threats deliberately omitted or turned off processing irregularities or malicious code.

Auditor's Role

- ◆ To ensure maintenance of software program code libraries.
- ◆ Ensure appropriate backups of the system's data and programs made before the change.
- ◆ Tracking of program changes are to be accounted for through version procedure.
- ◆ A formal handover process so that authorized personnel are involved in the software changes.
- ◆ Standardized software updation management policies, procedures, & tools;
- ◆ Thorough testing before the any new software release is applied in a production environment

3.19.4 Authorization Controls

Authorization controls ensure that all information and data entered or used in processing is authorized management and representatives of events that actually occurred.

Auditor's Role

- ◆ Transactions in an application system are manually authorized, the controls that ensure that no authorized modifications take place after authorization.
- ◆ If transaction authorization is facilitated by logical access restrictions, then verify if the appropriate people have these capabilities.
- ◆ Identify any allowable overrides or bypasses of data validation and edit checks and verify that they are in a management position that should have this authority.
- ◆ Implement specific procedures to handle urgent matter, such as logging all emergency changes and approve them after the fact. Make sure there is an audit trail for all urgent matters.
- ◆ Review by IT management to monitor, and approve all changes to hardware, software, and personnel responsibilities.
- ◆ Assigned and authorized responsibilities to those involved in the change.

3.19.5 Document Controls

Documentation contains descriptions of the hardware, software, policies standards, procedures, and approvals related to the system. A user instruction manual document defines:

- ◆ Input controls that identify all data entering the processing cycle;
- ◆ Processing control information that includes edits, error handling, audit trails and master file changes;
- ◆ Output controls that define how to verify the correctness of the reports;
- ◆ Separation of duties between preparing the input and balancing the output.

To provide the user with the tools to achieve their responsibilities, the user manual should include:

- ◆ A narrative description of the system
- ◆ A detailed flowchart of all clerical processes.
- ◆ A detailed document flowchart.
- ◆ A copy of each input document,
- ◆ A list of approvals required on each input document.
- ◆ A copy of any batch control forms or other transmittal forms.
- ◆ A listing of computerized input and processing edits performed.
- ◆ A copy of each report produced by the system with a description of its purpose, no. of copies.
- ◆ A list of retention periods for: input source documents, data file, output report.
- ◆ A system recovery section including user responsibilities for assisting.

Auditor's Role

Assessing documentation involves evaluating -

- ◆ There is sufficient documentation that explains how software/hardware is to be used.
- ◆ There are formal, documented security and operational procedures.
- ◆ The auditor will need to obtain documents with the following details:
 - Name (title) of the computer product
 - Purpose of the product
 - Date the system was implemented
 - Type of computer used and location
 - Frequency of processing and type of processing
 - Person(s) responsible for the computer application and database that generates the computer output.
 - Point of origin for each source document
 - Each operating unit or office through which data is processed
 - Destination of each copy of the source document
 - Actions taken by each unit or office in which the data is processed
 - Controls over the transfer of source documents between units to assure that no documents are lost, added or changed.

3.19.6 Testing and Quality Control

- ◆ Testing commences during the design phase and continues during the system development and acceptance testing phases.
- ◆ Computer system are tested to prove that they perform to the satisfaction of the various interested parties. This includes the developers, operations staff, and the end-users and may also include system administrators, security personnel and auditors.
- ◆ The overall objective of the testing process is to ensure that the delivered system is of adequate quality. To meet this objective it will be necessary to confirm that the new system:-
 - conforms with the organization's technical policies and standards;
 - performs all me required functions;
 - can be used by the staff for whom it is intended;
 - meets it performance objectives;
 - is reliable in operation.
- ◆ Tests must therefore be designed that attempt to demonstrate that the system:
 - does not do what it is supposed to do;
 - does what it is not supposed to do;
 - is not operable by the staff for whom it is intended.
- ◆ Other important principle that should govern testing are -
 - No testing without measurable objective
 - No testing without recording
 - No recording without analysis
 - No analysis without action
- ◆ If a defect is corrected, the system (or perhaps parts of it) will probably need to be re-tested to ensure that the change has not introduced other unforeseen problems. This process is known as "**regression testing**".

3.20 Quality Control

Quality control management is a process that impacts the effectiveness, efficiency, integrity, and availability of information systems. Quality controls encompass the following:

- Establishment of a quality culture
- Quality plans
- Quality assurance responsibilities
- Quality control practices
- System development life cycle methodology
- Program and system testing and documentation
- Quality assurance reviews and reporting
- Training and involvement of end-user and quality assurance personnel
- Development of a quality assurance knowledge base
- Benchmarking against industry norms

This control requires regular reviews and audits of the software products and activities to verify that process and personal comply with the applicable procedures and standards.

3.20.1 Quality Standards

- ◆ The best practices that identify the quality and assurance are governed by two key standards.
 - i) **Capability Maturity Model integration (CMM):**
Developed by Software Engineering Institute SEI; it is a framework for organizing and assessing the maturity level of IT processes for software development and maintenance.
 - ii) **9000 Quality Management and Quality Assurance Standards (ISO) :**
Defines quality control as the "operational techniques and activities that are used to fulfill requirements for quality".
- ◆ Quality control is concerned with the quality of individual product produced during the project, it is the responsibility of the Project Manager to ensure that effective quality control is carried out.
- ◆ Quality control costs both time and money, and project manager are often tempted to dispense with it, particularly when working to an unrealistic, imposed deadline. Removing what appears to be a "non-productive" activity apparently brings the project back on schedule. This is called "False Economy". But, it brings up greater problems for both system operation and maintenance.

3.20.2 Quality Reviews

Quality review covers various non-computer testing activities. For example, it determines whether a product is:

- ❖ Complete and free from cosmetic and mechanical defect.
- ❖ Is correct, comprehensive and appropriately targeted.
- ❖ Complies with relevant standard.

3.20.3 Auditor's Role

The general questions that the auditor will need to consider for quality control are:

- Does the 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 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 staffs invited to comment on the internal control aspects of system designs
- Are statistics of defects uncovered during quality reviews analyzed for trends?
- Are defects uncovered during quality reviews always corrected?
- Are all system resources (hardware, software, documentation) that have passed quality review been placed under change control management and version control?
- Has a System Installation Plan been developed and quality reviewed?
- Has a Training Plan been developed and quality reviewed?

3.20.4 Copyright Violations

Violation of copyright laws may lead to potential risk. The computing environment needs controlling to prevent software piracy and copyright violations. The scope of a Copyright Act is:

- The illegal copy of computer programs except for backup or archival purposes.
- Any business or individual convicted of illegally copying software is liable for both compensatory and statutory damages for each illegal copy of software in the premises.
- Employees and consultants about organizations that use illegal software are documented.

Any information owned/created by the company and considered its intellectual property in a written, printed, or stored as data, must be labeled with a copyright notice in the following format: Copyright © 2003 [Company Name], Inc. All Rights Reserved.

3.20.5 Contract / Warranties

On Acquisition of Software organizations enter into contracts for computer hardware, software, and services. IT contracts are to address these issues:

- Meet IT users expectations and the systems need to perform as intended;
- Able to file litigation in response to dissatisfaction with products or services.

IT auditors can help companies avoid contract failures, especially those lacking in-house computer contracting expertise. The review areas of IT related contracts are -

- Review of supplier contract terms that limit supplier liability.
- Review of performance measurements to ensure objectives have been met.
- Review contract clauses for protecting customer interests.
- Focus is on acceptance criteria.
- The three key goals to achieve:
 - ◆ Preparation of explicit criteria that can be used for acceptance
 - ◆ The process of negotiating the contract and
 - ◆ The process of monitoring contract compliance.
- To identify a major control weakness and contract issues which require immediate management attention.
- Does the contract reflect the organization's requirement.
- Have the requirements been translated into measurable acceptance criteria?
- Was the contracting officer present at all meetings and documentation of proceedings recorded?
- What changes or agreements were reached in refining contract terms?
- The contract has been executed.
- Acceptance tests are performed on all products or services.
- Acceptance tests are documented, evaluated, and the results are reviewed and signed off by customers.
- The organization exercises its right to accept or decline the contract.

3.20.6 Service Level Agreement (SLA)

The SLA is a formal agreement between a customer requiring services and the organization that is responsible for providing those services. It is not a legal contract in itself, but an essential component of it. An SLA state the required performance of the system in terms of its availability to users, response times, and numbers of transactions processed and any other suitable criteria meaningful to the user. Performance indicators are to be agreed, and the delivered level of service is to be regularly monitored against that specified.

Service : A set of deliverables that asses between a provider & a consumer.

Level : The measurement of services agreed and delivered and the gap between the two.

Agreement : Contract between two entities.

An SLA should also define:

- The level of technical support to be provided to users.
- The procedures for proposing change to the system.
- Standards of security provision, data access controls, monitoring system and network use.
- Emergency requirements
- A schedule of charges for the services to be provided.

The auditor is to ensure that the following form a part of the service level agreement:

- Service provider should comply with all legal requirements that are applicable to the outsourced activity.
- Should provide for a right to audit clause and control responsibilities.
- Responsibility of the service provider to establish performance monitoring procedures.
- Business continuity measures to be put in place to ensure continuity of service.
- Non disclosure requirements as regards information and processes of the audited organization Insurance requirements.

3.21 Control Over System Implementation

Activities during Implementation stage are discussed below -

3.21.1 Procedures Development

Covers who, what, when, where, and how of the implementation process. The design of procedures must match the job/task responsibility of a user within the organizational functional framework. The auditor is to assess the following in the procedure design phase:

- The quality of the procedures design must meet the minimum user requirements.
- Change management principles implemented and followed within the organization.
- The approach followed in testing and implementation.
- Quality of the procedures documentation, system manuals etc, in a consistent and formal style.

3.21.2 Conversion

- Defines the procedures for correcting and converting data into the new application, determining what data can be converted through software and what data manually.
- Performing data standardization before data conversion.
- Identifying the methods to access the accuracy of conversion like record counts & control total,
- Designing exception reports showing the data which could not be converted.
- Establishing responsibility for verifying and signing off and accepting overall conversion

The conversion strategies are:

- ◆ Direct implementation/Abrupt change-over:
- ◆ Parallel implementation: Phased implementation: Pilot implementation:

3.21.3 Auditor's Role

- Has a data conversion plan been drawn up?
- Does the Data Conversion Plan :
 - ◆ Describe the data conversion strategy to be followed (e.g. the procedures, the files to be converted; the conversion timetable)?
 - ◆ Allocate staff to each task and define specific roles and responsibilities.
 - ◆ Set out the criteria for identifying and resolving problems on the quality of the existing data (e.g. undertake file interrogation)
 - ◆ Acceptance tests using any custom built software.
 - ◆ Define the controls that are to give assurance that data has been transferred completely and accurately, and correctly posted
 - ◆ Implement an effective separation of roles between those involved in transferring data and those involved in verifying that it has been correctly transferred.
 - ◆ Define procedures to ensure that converted data is kept up-to-date following its transfer to the new system?
 - ◆ Define, backup and recovery procedures for the converted data on the new system
 - ◆ Define how the audit trail is to be preserved after cut over;

3.21.4 User Final Acceptance testing

Acceptance testing is a complete end-to-end test of the operational system. Appointing an experienced manager and following-up a pre-defined plan will help to ensure that testing is effective. It aims to provide the system users with confirmation that -

- ◆ The user requirement specification has been met.
- ◆ End-user & operational documentation is accurate, comprehensive & usable.
- ◆ Supporting clerical procedures work effectively.
- ◆ Help Desk and other support functions operate correctly and as expected.
- ◆ Backup and Recovery procedures work effectively.

The following types of acceptance testing is performed –

i) Performance testing

- ◆ Testing of average response time i.e. time between the user depressing the transmit key and the first character of the reply appearing on screen.
- ◆ Testing of maximum response time i.e. the response time that must not be exceeded.
- ◆ Testing of other response time such the response time to -
 - ❖ load an application
 - ❖ accept or move between fields on the screen
 - ❖ perform an update
 - ❖ run a complex query

ii) **Volume testing** - Testing whether the system can handle the volume of data specified in a acceptable time-frame.

iii) **Stress testing** - Testing whether the system can handle heavy stress i.e. peak volume of data over a short period.

iv) **Security testing** - Testing the internal controls and systems security against attempts to upset the security protection.

v) **Clerical procedure checking** - Testing to confirm that all supporting clerical procedures have been documented and work effectively.

vi) **Backup and Recovery testing** - Testing to confirm that software, configuration files, data and transaction logs can be backed up, either completely or selectively and also restored from backup.

vii) **Parallel Operation testing** - In this testing both the systems run parallelly and outputs are generated from both the systems. Outputs are then compared to accuracy.

On satisfactory completion of user acceptance testing, the Project Board should sign off a System Acceptance Document to signify that the development process has been completed.

3.21.5 Auditor's Role

The auditor is to assure management that the system:

- ◆ Possesses the built-in controls necessary to provide reasonable assurance of proper operation;
- ◆ Provides the capability to support audit of the system in operation;
- ◆ Meets the needs of the user and management;
- ◆ If the level of testing does not meet standards, the auditor must notify the development team or management who will then take corrective action;
- ◆ Has an Acceptance Test Plan been drawn up to cover all aspects of testing?
- ◆ Allocate adequate resources in terms of manpower, time and equipment to acceptance testing?
- ◆ Allocate individual roles and responsibilities for:
 - managing the test environment?
 - undertaking individual tests and test cycles?
 - recording test result?
 - analysing test results and prioritizing errors?
- ◆ Fully involve the end-users in the design and execution of the acceptance testing programme?
- ◆ Include ancillary procedures? (e.g. clerical control checks, the Help Desk, Network support, System Administration);
- ◆ Require the manager in charge to sign off individual tests and test cycles on successful completion?
- ◆ Is there an adequate separation of roles to help guard against unauthorized changes;
- ◆ Have test data been prepared for each test?
- ◆ Do tests cover events that ought not to happen as well as those that should?
- ◆ Does user Acceptance Testing Plan cover all aspects of the User Requirements?
- ◆ Is an adequate audit trail of changes maintained?
- ◆ Are regression tests carried out to ensure that previously accepted areas of the new system continue to work after significant changes have been implemented?
- ◆ Has the acceptance-testing programme been signed off by the Project Board on successful completion?

3.21.6 User training

Training both the end-users and the IS operations personnel is critical for the efficient and effective implementation of a system. Training would involve manager's training on overview and application of systems, operational user training on how to use the software, enter the data, and generate the output and systems training on the technical aspects.

3.22 System Maintenance

- ◆ The maintenance phase involves making changes to hardware, software, and documentation to support its operational effectiveness.
- ◆ To ensure modifications do not disrupt operations or degrade a system's performance or security, organizations should establish appropriate change management standards and procedures.
- ◆ System maintenance can be undertaken in the following three categories :

Corrective maintenance: Emergency error fixing and routine debugging-logical errors.

Adaptive maintenance: Accommodations of changes in the user environment.

Perfective maintenance: User enhancements, improved documentation, and re-coding.

3.22.1 Auditor's Role

The effectiveness and efficiency of the system maintenance process is evaluated by auditor using following parameters:

- The ratio of actual maintenance cost per application versus the average of all applications. Average time to deliver change requests.
- The number of change requests for the system application that were related to bugs.
- 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.

3.22.2 Performance Measurement

Performance measurement is dependent on the business strategy and objectives of the organization. The factors for measurement would involve:

- ◆ The value delivered by the IT system;
- ◆ The ratio to the cost of IT to the per unit business function;
- ◆ The response time of the system for a new or change in operation, and
- ◆ The ongoing costs of the system to maintain its effectiveness.

For a system to be evaluated properly, it must be assessed using system performance measurement. Common measurements include throughput, Utilization and response time.

3.23 Post implementation Review

3.23.1 Scope -

The scope of a post implementation review(PIR) is the check whether the new system has met its -

- ◆ Business Objective : Developed within budgeted cost and time; producing predicted results.
- ◆ User Objective : User friendliness; response time; work load; required output; reliability.
- ◆ Technical Objective: Modularity; ease of operation and maintain; interface with other system.

3.23.2 Timing -

- ◆ PIR should not be undertaken until any changes and tuning that are necessary to achieve a stable system have not been completed.
- ◆ Sufficient time should also be allowed for the system's user to become familiar with it.
- ◆ These criteria should be met between six and twelve months after implementation. If PIR is delayed beyond 12 months there will be an increasing risk of changing requirement -loading to further release of the system.

3.23.3 Team -

- ◆ In order to achieve undiasness, the team should be substantially independent of the original system development team. It may therefore be advisable to employ an external IS consultant to review.
- ◆ It may also be necessary to employ other external support to assist in evaluating the technical and specialised function of the system
- ◆ Internal auditor might help assess the effectiveness of internal controls.

3.23.4 Activities -

During PRI the team should review -

1. The functionality of the operational system against the User requirement specification.
2. System performance and operations
3. Development techniques and methodology employed
4. Estimated time and cost and reason for variation, if any.
5. All anticipated benefits both tangible and intangible, delivered by the system.
6. All unanticipated benefits both tangible & intangible, delivered by the system.
7. Preparation of reports having findings, conclusion and recommendations.

3.23.5 Auditor's Role -

The following issues should be considered when judging the effectiveness of a PIR or to form basis for auditing -

- a) Interview users in each functional area covered by the system and assess their satisfaction.
- b) Interview security, operation and maintenance staff and assess their reactions to the system.
- c) Determine whether the user's requirement from system have been met. Identify the reason why any requirement are yet to be delivered.
- d) Confirm that the previous system has been de-commissioned.
- e) Review system problem and change proposals to establish the number and nature of problem and changes being made to solve them. The frequency of changes can provide an indicator of the quality of system development.
- f) Confirm that adequate internal controls have been built into the system, and that they are being operated correctly.
- g) Confirm that an adequate Service level agreement has been drawn up and implemented,
- h) Confirm that the system is being backed up and it has been restored from backup media,
- i) Review the anticipated and unanticipated costs and benefits.
- j) Review trends in growth of transaction throughput and use of storage.

3.24 Control Over Data Integrity, Privacy and Security

All information maintained by the system does not require the same amount of security, therefore it is must to classify them on the basis their criticality and then security controls should be designed.

3.24.1 Classification of Information

Information classification is the decision to assign a level of sensitivity to information. This classification of the information should then determine the extent to which it needs to be controlled or protected. It is also indicative of its value in terms of business assets. Broadly information is classified into 5 categories -

(a) Top Secret

All highly sensitive internal information fall in this category. E.g. Business Strategies, corporate goals and objectives, Investment plans, Pending mergers or acquisitions or any futuristic information. Information security at this level is the highest possible.

(b) Highly Confidential

In this category we include all the information that, if made public or even shared around the organization, could seriously obstruct the organization's operations. E.g. Accounting information, business plans, sensitive customer's data, suppliers data etc. Security at this level should be very high.

(c) Proprietary

Information of a proprietary nature such as procedures, operational work routine, project plan, that define the way in which the organization operates, fall in this category. Security at this level is high.

(d) Internal Use only

It includes information not approved for general circulation outside the organization. The loss/disclosure of these informations would cause inconvenience to the organization but not result in financial loss or serious damage. Example-internal memo, minutes of meetings, project reports etc. Security at this level is controlled but normal.

(e) Public Documents

Information in the public domain such as annual reports, press statement etc. are called public document. Security at this level is minimal.

3.24.2 Data Integrity

Once the information is classified, the organization has to decided 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 data processing program.

Data integrity controls protects data from accidental or malicious alteration. There are six categories of integrity controls:-

(a) Source data control -

They protect against invalid, incomplete or inaccurate source data input. These controls include-

- | | |
|--------------------------|------------------------------------|
| ◆ Input form design | ◆ Sequentially pre-numbered forms |
| ◆ Turnaround document | ◆ Appropriate input authorisation, |
| ◆ Segregation of duties, | ◆ Appropriate input authorisation, |
| ◆ Key verification etc. | |

(b) Input validation -

They protect against invalid or inaccurate data in transaction files. These controls include -

- | | |
|--|------------------|
| ◆ File editing programs | ◆ Sequence check |
| ◆ Picture check | ◆ Limit check |
| ◆ Redundant data check | ◆ Error log |
| ◆ Procedure for error correction and resubmission. | |

(c) On-line data entry controls

They control invalid or inaccurate transaction entered through online terminals. These controls include -

- ◆ Limit check
- ◆ Redundent data check
- ◆ Completeness check
- ◆ Picture check
- ◆ User-ID and Password
- ◆ Error Log

(d) Data processing and Storage controls

They control in accurate or incomplete data in computer-processed master files. These controls include -

- ◆ Data control personnel
- ◆ Exception reporting
- ◆ Data Librarian
- ◆ File Label
- ◆ Data conversion control
- ◆ Standard policy and procedure for data processing
- ◆ Audit Trail
- ◆ Batch Total
- ◆ Default value control
- ◆ Backup & Recovery control
- ◆ Write protection control

(e) Output Controls -

They control inaccurate or incomplete output, misdirected output, these controls includes -

- ◆ Batch total
- ◆ Output distribution sheet
- ◆ Security control to sensitive / confidential output
- ◆ Users review of output for completeness and accuracy
- ◆ Error and Exception report

(f) Data Transmission controls -

They control unauthorised access of data being transmitted, communication disruption due hardware and software failure. These controls include-

- ◆ Network monitoring
- ◆ Multiple communication path
- ◆ Data Encryption
- ◆ Parity Check
- ◆ Echo check
- ◆ Communication data backup
- ◆ Preventive maintenance
- ◆ Routing verification
- ◆ Message acknowledgement procedure

3.24.3 Data Integrity Policies

- ◆ Virus-Signature Updating:
- ◆ Software Testing:
- ◆ Division of Environment:
- ◆ Version Zero Software:
- ◆ Offsite Backup Storage : Backups older than one month must be sent offsite for permanent storage.
- ◆ Quarter-End and Year-End Backups :
- ◆ Disaster Recovery:

3.24.4 Data Security

Data security encompasses the protection of data against accidental or intentional disclosure to unauthorized persons. 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.

3.25 Security Concepts and Techniques

3.25.1 Cryptosystems

A Cryptosystem refers to a set of algorithms needed to implement a particular form of encryption and decryption. Typically, a cryptosystem consists of three algorithms : one for key generation, one for encryption and one for decryption. The term "Cipher" is used to refer to a pair of algorithms one for encryption and one for decryption. Therefore, the term cryptosystems is most often used when the key generation algorithm is important.

3.25.2 Data Encryption Standard (DES)

- ❖ The DES is a cipher algorithm selected as an official Federal Information Processing Standard (FIPS) for the United States in 1976. It is a mathematical algorithm for encrypting and decrypting binary coded information. Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext.
- ❖ The algorithm described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a key. A key consists of 64 binary digits of which 56 bits are randomly generated and used directly by the algorithm. The other 8 bits, which are not used by the algorithm, are used for error detection. The 8 error detecting bits are set to make the parity of each 8 bits byte of the key odd.
- ❖ Authorised users of encrypted computer data must have the key that was used to encipher the data in order to decipher it. Unauthorised recipient of the cipher who know the algorithm but do not have the correct key cannot derive the original data algorithmically.
- ❖ DES is now considered to be insecure for many applications. This is mainly due to the 56 bit key size being too small; DES keys have been broken in less than 24 hours.

3.25.3 Public Key Infrastructure (PIK)

The system is based on public key cryptography in which each user has a pair-a unique electronic value called a public key and a mathematically related private key. The private key is stored on the user's computer or a separate device such as a smart card. The private key must be stored in encrypted text and protected with a password or PIN to avoid compromise or disclose. The private key is used to create an electronic identifier called a digital signature that uniquely identifies the holder of the private key and can only be authenticated with the corresponding public key.

It is important when issuing a digital certificate that the initially verifying the identity of users is adequately controlled. The Certifying Authority A) attests to the individual user's identity by signing the digital certificate with its own private key, known as the root key.

The user's private key exists electronically and is susceptible to being copied over a network as easily as any other electronic file. If it is lost or compromised, the user can no longer be assured that message will remain private or that fraudulent or erroneous transaction would not be performed.

The primary drawback of a PKI authentication system is that it is more complicated and costly to implement than user names and password. When utilizing PKI policies and controls, financial institution need to consider the following -

- ◆ Defining the methods of initial verification that are appropriate for different types of certificate applicants and controls for issuing digital certificates.
- ◆ Selecting an appropriate certificate validity period to minimize transactional and reputational risk exposure.
- ◆ Ensuring that the digital certificate is valid by such means as checking a certificate revocation list before accepting transactions.
- ◆ Defining the circumstances for authorizing a certificate's revocation, such as the compromise of a user's private key or the closing of user account.
- ◆ Updating the database of revoked certificates frequently.
- ◆ Employing measures to protect the root key including limited physical access to certifying authority facilities, tamper-resistant security modules.
- ◆ Requiring regular independent audit to ensure controls are in place, public and private key lengths remain appropriate, cryptographic module conform to industry standards.
- ◆ Recording all significant events performed by the CA system in a secure audit log.
- ◆ Regularly reviewing exception reports and system activity by the C A's employees to detect malfunctions and unauthorised activities.
- ◆ Ensuring the institution's certificates and authentication systems comply with widely accepted PKI standards to retain the flexibility to participate in ventures that require acceptance of the financial institution's certificates by other CA's.

3.26 Data Security and public Network

Nowadays corporations have to go outside their private nets, because so many people telecommute or log in while they're on the road. Network administrators as well as managers must balance security concerns with employees' demand for easy accessibility to data.

One solution is a virtual private network(VPN): a collection of technologies that creates secure connections over regular internet lines. Key advantages offered by a VPN include universal connectivity, security and low cost.

3.26.1 Firewalls

A firewall is a collection of components (h/w and s/w) that controls the communication between company server and the outside world. All traffic between the security domains must pass through the firewall.

There are 4 primary firewall types from which to choose : Packetfiltering, Stateful inspection, Proxy server and Application-level firewall. The selection of firewall type is dependent on the amount of traffic, the sensitivity of the system and data, and application.

Typically, firewall block or allow traffic based on the rules configured by he administrator. Rule set can be static or dynamic. A static rule set is an unchanged statement to be applied to packet header, such as blocking all incoming traffic with certain source addresses. A dynamic rule set often is a result of coordinating a firewall and an IDS. For eg. an IDS that alerts on malicious activity may send a message to the firewall to block the incoming IP address.

Firewalls may provide some additional services -

Network address translation(NAT) - NAT re-addresses outbound packets to mask the internal IP addresses of the network. NAT allows an institution to hide the topology and address schemes of its trusted network from untrusted networks.

Dynamic host configured protocol(DHCP) - It assigns IP addresses to machines that will be subject to the security controls of the firewall.

Virtual Private Network(VPN) gateway - A VPN gateway provides an encrypted tunnel between a remote external gateway and the internal network. Placing VPN capability on the firewall protects information from disclosure.

Firewall are subject to failure. When firewall fail, they typically should fail closed, blocking all traffic, rather than failing open and allowing all traffic to pass.

[A] Packet Filter firewall

It evaluate the headers of each incoming and outgoing packet to ensure it has a valid internal address, originates from a permitted external address, connects to an authorized protocol or service. If the packet does not match the pre-defined policy for allowed traffic, then the firewall drops the packet. Packet filter generally do not analyze the packet contents beyond the header information. Many routers contain access control lists that allow for packet-filtering capabilities.

Weaknesses associated with packet filtering firewall includes the following:

- ◆ The system is unable to prevent attacks that exploit application because the packet filter does not examine packet contents.
- ◆ Logging functionality is limited to the same information used to make access control decision.
- ◆ Most do not support advanced user authentication schemes
- ◆ Firewalls are generally vulnerable to attack and exploitation that take advantage of vulnerabilities in network protocols.
- ◆ Firewalls are easy to mis configure, which allows traffic to pass that should be blocked.

Packet filtering are appropriate in high-speed environment where logging and user authentication with network resources are not as important. Packet filter firewall are also commonly used in small office / home office (SOHO).

[B] Stateful inspection Firewall

These are packet filters that monitor the state of the TCP connection. Each TCP session starts with an initial "handshake" communicated through TCP flags in the header information. When a connection is established the firewall adds the connection information to a table. The firewall can then compare future packets to the connections or state table. This essentially verifies that inbound traffic is in response to requests initiated from inside the firewall.

[C] Proxy server firewall

It acts as an intermediary between internal and external IP addresses and block direct access to the internal network. They rewrite packet headers to substitute the IP of the proxy server for the IP of the internal machine and forward packets to and from the internal and external machines.

Due to that limited capabilities, proxy servers are commonly employed behind other firewall devices. The primary firewall receives all traffic, determines which application is being targeted, and hands off the traffic to the appropriate proxy server. Common proxy servers are Domain Name Server(DNS), Web server(HTTP), and Mail (SMTP) server.

Additionally, proxy servers provide another layer of access control by segregating the flow of internet traffic to support additional authentication and logging capability, as well as content filtering.

[D] Application-level firewalls

These combines the filtering capabilities of packet filter firewalls with additional validation of the packet content based on the application. Unlike a packet filter firewall, an application-level firewall continues to examine each packet after the initial connection is established for specific application or service such as telnet, FTP, HTTP, SMTP etc.

Application level firewall provides the strongest level of security, but are slower and require greater expertise to administer properly. Advantages are:-

- ◆ The time required to read and interpret each packet slows network traffic.
- ◆ It may provide only limited support for new network application and protocols.

3.27 Unauthorised Intrusion

Intrusion detection is the attempt to monitor and possibly prevent attempts to intrude into system and network resources of an organization. Typically, firewall or authentication system of some kind will be employed to prevent unauthorised access.

Sometimes simple firewall or authentication systems can be broken. Intrusion detection is the set of mechanisms that should be put in place to warn of attempted unauthorised access to the computer.

3.27.1 Why IDS

One wants to protect the data and systems integrity, hi today's internet environment using mechanisms such as ordinary password and file security it is difficult to protect. Firewalls and other access prevention mechanisms should always be put in place.

Intrusion detection takes that one step further. Placed between the firewall and the system being secured, a network based intrusion detection system can provide an extra layer of protection to that system.

3.27.2 Types of IDS

IDS fall into two broad categories. These are -

- 1. Network based system -** These types of systems are placed on the network, nearby the system or systems being monitored. They examine the network traffic and determine whether it falls within acceptable boundaries.
- 2. Host based system -** These types of IDS runs on the system being monitored. These examine the system to determine whether the activity on the system is acceptable.

3.28 Hacking

Hacking is an act of penetrating computer systems to gain knowledge about the system and how it works. A hacker is someone who is enthusiastic about computer programming. However, most people understand a hacker to be what is more accurately known as a cracker.

Cracker 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 cracker 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

What damage can a hacker do depends upon what backdoor program(s) are holding on the PC. However if a cracker can't do something using the backdoor program, he can easily put something else onto your computer. Hackers can see everything you are doing, and can access any file on your disk.

Hacker can write new file, delete files, edit file, and do practically anything to a file that could be done to a file. A hacker could install several programs on to your system without your knowledge. Such programs could also be used to steal personal information such as password and credit card information.

3.28.1 Type of Hacking

There are many ways in which a hacker can hack. Some are -

(i) NetBIOS

NetBIOS hacker don't require to have any hidden backdomnning on your computer. NetBIOS is meant to be used on local area networks, so machines on that network can share information.

(ii) ICMP 'Ping'(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.

Ping may seen harmless enough, but a large number of pings can make a Denial-of-Service attack, which overloads a computer. Hacker can use pings to see if a computer exist and does not have a firewall.

(iii) FTP

Standing for File Transfer Protocol, it can be used for file downloads from some websites. FTP can also be used by some hackers, to access to private files.

FTP backdo or programs such as Doly Trojan, Fore etc. simply turn your computer into an FTP server, without any authentication.

(iv) RPC statd

This is a problem specific to Linux and Unix. The problem is where a fixed amount of memory is set aside for storage of data. If data received larger than this buffer, the program should truncate the data or send back an error or atleast do something other than ignore the problem. Unfortunately, the data overflows the memory that has been allocated to it, and the data is written into parts of memory it shouldn't be in. This can cause crashes of various different kinds. A skilled hacker could write bits of program code into memory that may do this.

(v) HTTP

HTTP hackers can only be harmful if you are using microsoft web server software such as Personal Web Server. 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 that parts of memory that contain active program code. A malicious user could use this to run any program they want on the server.

3.28.2 Auditor's Role

The focus of IS Auditor is to examine all factors that adversely bear on the confidentiality, integrity and availability of the information, due to improper physical access. Confidentiality, Integrity and Availability (CIA) are the core principles information safety.

Confidentiality- Preventing disclosure of information to unauthorised individuals.

Integrity - Preventing modification of data by unauthorised personnel.

Availability - Information must be available when it is needed.

3.29 Data Privacy

It refers to the evolving relationship between technology and the legal right to public expectations of privacy in the collection and sharing of data. 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

The challenge in data privacy is to share data while protecting the personally identifiable information.

3.29.1 Protecting data privacy in information systems

In heterogeneous information systems with different privacy rules are interconnected, technical control and logging mechanisms will be required to reconcile, enforce and monitor privacy policy rules and to ensure accountability for information use. There are several technologies to address privacy protection IT systems. These fall into two categories -

(a) Policy communication

P3P- The platform for privacy preferences, P3P is a standard for communicating privacy practices and comparing them to the preferences of individuals.

(b) 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.

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.

3.29.2 Data Privacy Policies

- ◆ **Copyright Notice:** All information owned by the company and considered intellectual property, whether written, printed or stored as data, must be labeled with a copyright.
- ◆ **E-mail monitoring:** All e-mails must be monitored for: Non-business use, unethical or illegal content disclosure of company confidential information.
- ◆ **Customer Information Sharing:**
- ◆ **Encryption of data backups:**
- ◆ **Encryption of extranet connection:**
- ◆ **Data Access:** Access to corporate information, hard copy, and electronic data is restricted to individuals with a need to know for a legitimate business reason.

3.30 Control against viruses and other destructive programs

Destructive programs are responsible for huge amount of losses measured in terms of data corruption and destruction, degraded computer performance, hardware destructive, violations of privacy.

3.30.1 Virus

A virus is a program that attaches itself to a legitimate program to penetrate the operating system. One of the most insidious aspect of a virus is its ability to spread throughout the system and to other systems before perpetrating its destructive acts. Typically, a virus will have a built-in counter that will inhibit its destructive role until the virus has copied itself a specified no. of times to other programs and systems.

Virus programs usually attach themselves to the following types of files -

1. An .EXE or .COM program file
2. The OVL program file
3. The boot sector of a disk
4. A device driver program

3.30.2 Anti-virus software

There are three types of anti-virus software -

1. Scanner

The software looks for a sequence of bits called virus signatures that are characteristics of virus codes. They check memory, disk boot sectors, executables and systems filling to find matching bit patterns. It is necessary to frequently update the scanners with the data on virus code patterns for the scanners to be reasonably effective.

2. Active Monitor and Heuristic Scanner

This looks for critical interrupt calls such as OS calls and BIOS calls, which resemble virus action. However this also makes them inefficient since they cannot differentiate between genuine systems calls and virus action.

3. Integrity checkers

These can detect any unauthorised changes to files on the system. They require the software to compute a binary check data called the Cyclic Redundancy Check(RCR) for each file. When a program is called for execution, the software computes the CRC again and check with the parameter stored on the disk. Such checks assume that frequent changes to applications and systems utilities do not occur.

However, there is no single control, which can act as a panacea for all virus attacks. Virus control is in fact combination of management, technical, administrative, application and operational controls. The best policy for virus control is preventive control.

3.30.3 Recommended policy and procedure control

The security policy should address the virus threat, systems vulnerabilities and controls. A separate section on anti-virus is appropriate to address the various degree of risks and suitable controls thereof.

- ◆ Anti-virus awareness and training on symptoms of attacks, methods of reducing damage, cleaning should be given to all employees.
- ◆ Hardware installations and associated computing devices should be periodically verified for parameter settings.
- ◆ As part of SDLC controls the development area should be free of viruses and sufficient safeguard.
- ◆ Provision of disk drivers to read media should be restricted to certain controlled terminals and should be write-protected.
- ◆ Access to the internet should be restricted preferably to stand-alone computers.
- ◆ Networks should be protected by means of firewall that can prevent entry of known viruses.
- ◆ The server and all terminals must have rated anti-virus software installed.
- ◆ Procedure should ensure that systematic updates are applied to all anti-virus installations.
- ◆ External media such as disks, CDs, tapes need to be avoided. If necessary such media should be scanned on a stand-alone machine and certified by the department.
- ◆ Vendors and consultants should not be allowed to run their demonstration and presentation on organization systems.
- ◆ All new software acquisitions should follow a controlled procedure of centralized acquisition and testing for viruses.
- ◆ Operating systems and other softwares upgraded should be acquired from authentic sources and scanned installation.
- ◆ Reporting and incident handling procedures should be in suitable handle virus accidents.
- ◆ An effective backup plan must be implemented and monitored to ensure that back-up media is not infected and preferably encrypted.

3.31 Logical Access Control

Logical access controls are used to designate who or what is to have access to a specific system resource. The objectives of these controls are -

- ◆ Restrict users to authorized transactions and functions.
- ◆ Restrict the network access by authorised users only.
- ◆ Protect the confidentiality and integrity of the applications.

3.31.1 Logical access paths

Following are some logical access paths to the system and the controls that can restrict them to be used by authorised users only -

On-line Terminals - It is the terminal, directly connected by server and used by end user. To access an on-line terminal a user has to provide a valid login-ID and password.

Operator Console - It is the terminal connected to the server and used by authorised operator only. Access to operator console must be restricted by -

- ◆ Keeping the operator console at a place, which is visible, at all.
- ◆ Keeping the operator console in a protected room accessible to selected personnel.

Batch job Processing - In a batch processing jobs are accumulated and sent as batches. Thus during an accumulation there is possibility of an unknown job entering into a batch. To avoid this access should be granted to authorised people.

Dial-up ports - Using a dial up port user at one location can connect remotely to another computer (unknown location) via a telecommunication media. Security is achieved by providing a means of identifying the remote user to determine authorization to access. A dial back line can also be used to ensures security by confirming the presence of authorised user and data.

Telecommunication Network - In a telecommunication network a number of computer terminals, PCs etc are linked to the computer through network. Security is provided in the same manner as it is applied to on-line terminal.

3.31.2 Logical Access Issues and Exposures

Access control mechanism should be applied not only to computer operators but also to end user, programmers, security administrators, management or any other authorised user. Access control mechanism should protect the followings -

- | | |
|---------------------------|---------------------------|
| ◆ Access control software | ◆ Application software |
| ◆ Data files | ◆ Data Dictionary |
| ◆ Logging files | ◆ Password Library |
| ◆ System Software | ◆ Telecommunication lines |
| ◆ Temporary disk files | ◆ Spool queue |

Intentional or accidental exposure of logical access control encourage technical risks and crimes such as –

3.31.2.1 Technical Exposures -

Data Diddling

It involves the change of data before or as they entered into the system. A little technical knowledge is required to data diddling and the worst part of it is that it occurs before computer security can protect data.

Bombs

Bomb is a piece of a program code deliberately planted in the system. It explode when the condition of explosion get fulfilled, causing the damage. These program does not infect other programs. Generally they are of two kinds -

- **Time bomb** - It causes destructive activities on a particular date and time. The computer clock initiates it.
- **Logic Bomb** - Logic bombs are activated by some occurrence of events. For example a code like - if a file named DELETENOT is deleted then destroy the memory contents by writing 1s.

Trojan horse

These are malicious programs that are hidden under any authorised program. They cannot copy themselves to other software in the same or other system. The trojan may get activated only if the infected program is called explicitly. A Trojan may -

- ◆ Change or steal the password
- ◆ May modify records in protected files
- ◆ May allow unauthorised user to use the system

Worms

A worm does not require a host program like Trojan and it can copy itself to another machine on the network. Since worms are stand-alone program they can be detected easily.

Rounding Down

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

Salami Technique

In the Salami technique a very small amount of money is truncated from a computerized transaction. For example the amount 21,23,456.39 is truncated to either 21,23,456.30 or 21,23,456.00 depending on the calculation.

Trap Doors

These are the back doors that exists in an authorised program and allow to enter into a system without asking for login-ID and password.

3.31.2.2 Asynchronous Attacks

Numerous transmission must wait for the clearance of the line before data being transmitted. Data that are waiting to be transmitted are liable to unauthorised access called asynchronous attack. These attacks are hard to detect and has many forms:-

Data Leakage - It involves leaking information out of the computer by means of dumping files or reports on paper, tapes or disks.

Wire Tapping - This involves spying on information being transmitted over telecommunication network.

Piggybacking - This is the act of following an authorised person through a secured door or electronically attaching to an authorised telecommunication link. A special terminal is placed into the communication for this purpose.

Denial of Service - This is initiated through terminals that are directly or indirectly connected to the computer. Individuals who know the high-level systems logon-ID initiate shutting down process. Hackers use this technique to shut down computer system over the internet.

3.31.2.3 Computer Crimes

The crimes that are committed using computers & causes damage to the reputation, morale & very existence of an organization are called computer crimes.

Financial Loss : Financial losses may be direct like loss of electronic funds or indirect like false bills of expenditure.

Legal Repercussions : An organization has to adhere to many human rights laws while developing security policies and procedures. The organization will be exposed to lawsuit from investors and insurers if there are no proper security measures.

Loss of Credibility: In order to maintain competitive edge, many companies, especially service firms needs credibility and public trusts. This credibility will be shattered resulting in loss of business and prestige if any security violation occurs.

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

Disclosure of information: Exposure of confidential, sensitive or embarrassing information to the outside world can spoil the reputation of the organization.

Sabotage : People who may not be interested in financial gain but who want to spoil the credibility of the company will involve in such activities. They do it because of their dislike toward the organization.

Logical access violators: Hackers, Employees, IS Personnel, End users, Former employees. Interested or educated outsiders, Competitors, Foreigners, Criminals, Crackers, Temporary personnel, Vendors and consultants and accidental ignorant.

Spoofing: A spoofing attack involves forging one's source address. Spoofing occurs only after a particular machine has been identified as vulnerable. A penetrator makes the user think that he is interacting with the operating system. For example, a penetrator duplicate the logon procedure, captures the user's password.

3.31.2.4 Remote and distributed data processing

- ◆ Physical security can be provided by having the terminal lock when not in use.
- ◆ Applications that can be remotely accessed should be logically protected.
- ◆ Terminals at remote locations should be monitored carefully for violations.
- ◆ There should be proper control mechanisms over system documentation and manuals.
- ◆ Data transmission over remote locations should be controlled. The sender should attach needed control information that helps the receiving station to verify the genuineness.
- ◆ When replicated files exist at multiple locations it must be ensured that all are updated regularly.

3.31.3 Logical Access Controls Across the system

The purpose of logical access controls is to restrict access to information assets/resources. The access should not be so restrictive that it makes the performance of business functions difficult or it should not be so liberal that it can be misused.

The following table shows various categories and the controls in each categories:

Categories	Controls
1. User Access Management	User registration / De-registration Information about every user is documented Privilege management Access privileges are to be aligned with job requirements and responsibilities. User password management Password are usually the default screening point for access to systems. Allocation, storage, revocation and reissue of password are password management functions. Review of user access rights 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 privilege granted earlier.
2. 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.

3. Network access control	Policy on use of network services An enterprise wide applicable internet service requirements aligned with the business need policy based on business needs for using the internet services is the first step. Enforce path Based on risk assessment, it is necessary to specify the exact path or route connecting the networks; say for example internet access by employees will be routed through a firewall. Segregation of networks Based on the sensitive information handling function; say a VPN connection between a branch office and the head office this network is to be isolated from the internet usage service availability for employees. Network connection and routing control 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 implemented across the organisation's network.
4. Operating system access control	Automated terminal identification This will help to ensure that a particular session could only be initiated from a particular location or computer terminal. Terminal log-on procedures The log-on procedure does not provide necessary help or information, which could be misused by an intruder. 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 encryption 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 – for example, 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. Alarm to safeguard users If users are forced to execute some instruction under threat, the system should provide a means to alert the authorities. An example could be forcing a person to withdraw money from the ATM. Many banks provide a secret code to alert the bank about such transactions. 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 time 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.
5. Application and monitoring system access controls	Information access restriction The access to information is prevented by application specific menu interface, which limit access to system function. A user is allowed to access only to those items he is authorized to access. Controls are implemented on the access rights of users. For example, read, write, delete and execute. An ensure that sensitive output is sent only to authorised 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. Monitoring system access and use is a detective control, to check if preventive controls discussed so far are working. If not, this control will detect and report any unauthorised activities.

	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 all 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 critically 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 as per a standard time is mandatory.
6. Mobile computing	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.

3.31.4 Role of an IS auditor

An IS auditor should keep the following points in mind while evaluating logical access controls -

- ◆ Reviewing the relevant document pertaining to logical facilities and risk assessment.
- ◆ The potential access paths into the system must be evaluated by the auditor and assess their sufficiency.
- ◆ Deficiencies or redundancies must be identified and evaluated.
- ◆ By supplying appropriate audit technique, he must be in position to verify controls over access paths.
- ◆ He has to evaluate the access control mechanism, analyse the test results and other auditing evidences.
- ◆ The auditor should compare security policies and practices of other organizations with the policies of their organization and assess its adequacy.

Security policies

Every organization should have a security policy that defines acceptable behaviours and the reaction of the organization when such behaviours are violated. Security policies are not unique and might differ from organization to organization. Also legislation relating to Information technology is becoming more prolific, with many countries enacting laws on issues such as copyright and software privacy, intellectual property and personal data. These commercial competitive and legislative pressure require the implementation of proper security policies.

3.32 Physical Access Controls

This section enumerates the losses that are incurred as result of perpetrations, accidental or intentional violation of access paths.

3.32.1 Physical access issues and exposures

The following are some examples of accidental or intentional violations –

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

The possible perpetrators are –

- ◆ Employees who are Accidental ignorant
- ◆ Employee who are Addicted to gambling
- ◆ Discontented
- ◆ Employees Experiencing financial or emotional problems
- ◆ Former employee
- ◆ Interested or informed outsiders
- ◆ Employees notified about their termination
- ◆ Employees on strike
- ◆ Employees threatened by disciplinary action

The facilities that need to be protected from the auditor's perspective are:

- | | |
|-------------------------------|-----------------------------|
| ◆ Communication Circuit | ◆ Computer room |
| ◆ Front end processor | ◆ Telephone lines |
| ◆ Input/output control room | ◆ LAN |
| ◆ Micro computer | ◆ Backup storage facilities |
| ◆ On-line and remote printers | ◆ Power sources |
| ◆ Programming are | ◆ Storage room |
| ◆ Data libraries | |

3.32.2 Access Control Mechanism

An access control mechanism verifies users request for resources in three steps:

(1) Identification (2) Authentication (3) Authorisation

The following is the sequence in which access control mechanism operates :

- ◆ First and foremost, the users have to identify themselves, thereby indicating their intent to request the usage of system resources.
- ◆ Secondly, the users must authenticate themselves and the mechanism must authenticate itself.
- ◆ Third, the users request for specific resources, their need for those resources and their areas of usage of these resources.

3.32.2.1 Identification and Authentication

Users identify themselves by providing information such as name or account number. To validate the user, his entry is matched with the entry in the authentication file. User may provide 4 classes of authentication information -

- | | | |
|--------------------------------|---|--------------------------------------|
| ◆ Remembered information | : | Name, account number, password |
| ◆ Object Possessed by the user | : | Badge number, plastic card key |
| ◆ Personal characteristics | : | Finger print, Voice print, Signature |
| ◆ Dialog | : | computer generated information |

3.32.2.2 Authorisation

There are two approaches to implementing the authorization module in an access control mechanism

Ticket oriented approach - In this approach, the access control mechanism assigns user a ticket for each resource they are permitted to access. It operates via a row in the matrix.

List oriented approach - 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. This mechanism operates via a column in the matrix.

Procedure of the ticket oriented

When a user process is executing, its capability list can be stored in some fast memory device. When the process seeks access to a resource, the access control mechanism simply looks up the capability list to determine if the resource is present in the list and whether if the user is permitted to take the desired action.

Procedure of the list oriented :

Each user process has a pointer to the access control list for a resource. Thus the capabilities for a resources can be controlled since they are stored in one place. It is enough to examine the access control list just to know who has access over the resources and similarly to revoke access to a resource, a user's entry in the access control list simply needs to be deleted.

3.32.3 Physical Access Control

These are designed to protect the organization from unauthorized access/illegal entry. The authorization given by the management may be explicit, as in a door lock for which management has authorised someone to have a key; or implicit, like a job description which confirms the need to access confidential reports and documents.

Some of the more common access control techniques are –

3.32.3.1 Locks on Door Cipher Locks

Also known as combination door locks, it consists of push button 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 10 to 30 sec. More sophisticated and expensive cipher locks can be computer soded 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.

Electronic door lock

A magnetic or embedded chip-based plastic 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, activates the door locking mechanism. Advantages of electronic door lock over bolting and combinational lock are -

- ◆ Through the special internal code, cards can be made to identify the correct individual.
- ◆ Restrictions can be assigned to particular doors or to particular hours of the day.
- ◆ Degree of duplication is reduced.
- ◆ Card entry can be easily deactivated in the event an employee is terminated or a card is lost.
- ◆ An administrative process, which may deal with issuing, accounting for and retrieving the card keys are also parts of security.

Biometric Door Lock

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

3.32.3.2 Physical identification medium

Personal identification number(PIN)

A secret number will be assigned to the individual, as a means of identifying them and servers 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 PIN keypad. The user's entry will be matched with the PIN number available in the security database.

Plastic Cards

These cards are used for identification purpose. Controls over cards seek to ensure that customers safeguard their card so it does not fall into unauthorised hands.

Cryptographic control

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 transaction.

Identification Badges

Special identification badges can be issued to personnel as well as visitors. For easy identification purpose their colour of the badge can be changed.

3.32.3.3 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.

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.

3.32.3.4 Other means of controlling Physical Access

Video Camera

Cameras should be placed at specific location and monitored by security guards. The video supervision recording must be retained for possible play back.

Security Guards

Extra security can be provided by appointing guard. Guards supplied by an external agency should be made to sign a bond to protect the organizations from loss.

Controlled visitor Access

A responsible employee should escort all visitors.

Bonded Personnel

All service contract personnel, such as cleaning people and off-site storage service, should be asked to sign a bond.

Dead men doors

These systems encompasses are a pair of doors that the typically found in entries to facilities such as computer room. 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 unauthorised person follows an authorised person through secured entry.

Non-exposure of sensitive facilities

There should be no explicit indication such as presence of directional sign hinting the presence of facilities such as computer rooms.

Computer terminal locks

Controlled single entry point

A controlled single entry point is monitored by a receptionist. Multiple entry point increase the chances of unauthorised entry.

Alarm system

Linking alarm system to inactive entry point, motion detector, reverse flows of enter or exit only door can be used to avoid illegal entry.

Perimeter Fencing

Control of out of hours of employees

Employees who are out of office for a longer period of time should be monitored carefully.

Secured Report/Document Distribution cart

3.32.4 Audit Trail

All the activities taken in the system should be properly recorded. The following sorts of data must be kept -

- ◆ Action privileges requested
- ◆ Action privileges allowed
- ◆ Authentication information supplied
- ◆ Identity of the perspective user
- ◆ Number of logon attempts
- ◆ Resources requested
- ◆ Resources provided
- ◆ Start and finish time
- ◆ Terminal identifier

3.32.5 Audit and Evaluation techniques

Information Processing Facility (IPF) is used to gain an overall understanding and perception of the installation being reviewed. Much of the testing of physical safeguard can be visually observation of the safeguard. The documents to assist with this effort include emergency evaluation procedure, inspection, tags, fire suppression system test results and key lock logs.

The facility should include -

- ◆ Computer storage rooms
- ◆ Location of all communication equipment
- ◆ Location of all operator consoles
- ◆ Off-site backup storage facility
- ◆ Printer rooms
- ◆ Tape library
- ◆ UPS

To do thorough testing, we have to look above the ceiling panels and below the raised floor in the computer operation center. Keen observation is done on smoke and water detector.

The following paths of physical entry should be evaluated for proper security-

- ◆ All entrance points
- ◆ Glass windows and walls
- ◆ Movable walls and modular cubicles
- ◆ Above suspended ceiling and beneath raised floors
- ◆ Ventilation systems

3.32.6 Role in Physical Access controls

Auditing physical access requires the auditor to review the physical access risk and controls. This involves the following -

- 1) Risk assessment** - The auditor must satisfy that the risk assessment procedure adequately covers periodically and timely assessment of all assets, physical access threats, vulnerabilities of safeguards.
- 2) Controls assessment** - The auditor based on the risk profile evaluate whether the physical access controls are in place and adequate or not.
- 3) Review of physical access controls** - It requires examination of relevant documentation such as the security policy and procedures.
- 4) Testing of controls** - The auditor should test physical access controls to satisfy that -
 - ◆ Tour of organizational facilities including outsourced and offsite facilities.
 - ◆ Physical inventory of computing equipment & support infrastructure
 - ◆ Interviewing personnel
 - ◆ Observation of safeguard and physical procedure. This would also include inspection of -

Core computing facilities	Computer storage rooms
Communication closet	Backup and off site facilities
Printer rooms	Disposal yards and bins
Inventory of supplies and consumables	
 - ◆ Some special considerations involved the following -

All points of entry exit	Glass windows and walls
Moveable and modular cubicles	Ventilation/AC ducts
False ceiling and flooring panels	
 - ◆ Review of physical access procedures. Employee termination procedure etc.
 - ◆ Examination of physical access logs and reports.

3.33 Environment Control

- ◆ These controls deals with the external factors in the information system and preventive measures to overcome these conflicts.
- ◆ **From the perspective of environmental exposures and controls, information systems resources may be categorized as follows :**
 - i) Hardware and Media:** Includes Computing Equipment, Communication equipment, and Storage Media.

- ii) **IS Supporting Infrastructure or Facilities :** This typically includes the following:
 - ◆ Physical Premises, like Computer Rooms, Cabins, Server Rooms, Data Centre premises, Printer Rooms, Remote facilities and Storage Areas
 - ◆ Communication Closets
 - ◆ Cabling ducts
 - ◆ Power Source
 - ◆ Heating, Ventilation and Air Conditioning (HVAC)
- iii) **Documentation:** Physical and geographical documentation of computing facilities with emergency excavation plans and incident planning procedures.
- iv) **Supplies:** The third party maintenance procedures for say air conditioning, fire safety and civil contractors.
- v) **People:** The employees, contract employees, visitors, supervisors and third party maintenance personnel are to be made responsible and accountable for environmental controls.

3.33.1 Environment issues and exposures

Environmental exposures are primarily due to elements of nature. Some of the exposures are -

- ◆ Fire
- ◆ AC Failure
- ◆ Equipment failure
- ◆ Bomb attack
- ◆ Natural disasters – earthquake, volcano, hurricane etc.
- ◆ Power spike
- ◆ Electric shock
- ◆ Water damage

Some of the other issues are –

- ◆ Is the power supply remains within the manufacturer's specification?
- ◆ Are the AC, humidity and ventilation control systems protected against the effects of electricity rug?
- ◆ Is consumption of food beverages and tobacco products prohibited?
- ◆ Are backup media protected from damage due to variations of temperatures?
- ◆ Is the computer equipment kept free of dust, smoke and other pollutant?

3.33.2 Control for Environmental exposures

1. Water Detectors

In the computer room, water detector should be placed under the raised floor and near drain holes. A remedial action must be instantiated on hearing the alarm by notifying the specific individual and allotting the responsibility for investigating the cause.

2. Hand-held fire extinguishers

Fire extinguishers should be placed at the appropriate location throughout the area. They should be tagged for inspection.

3. Manual Fire alarm

Hand-pull alarms should be purposefully placed throughout the facility. The alarm should be linked to a monitored guard station.

4. Smoke Detectors

Smoke detectors are positioned at placed, and upon acceptance these detectors should produce an alarm that must be linked to a monitored station.

5. Fire Suppression system

These alarms are activated when extensive heat is generated de to fire. The system should be segmented so that fire in one part of a large facility does not activate the entire system. The fire suppression techniques are –

- a. Dry-pipe sprinkler systems
- b. Water based system
- c. Halon gas system

6. Strategically locating the computer room

The computer room should not be located in the basement.

7. Regular inspection by fire department
8. Fireproof walls, floor and ceilings
9. Electrical surge protectors
10. Un-interruptible Power Supply / Generator
11. Power leads from two Substations
12. Emergency Power-off switch

Two emergency power off switch one at computer room and other near but outside the computer room would serve the purpose. They should be easily accessible and yet secured from unauthorised people.

13. Wiring placed in electrical panels and conduit
14. Prohibition Against Eating
15. Fire resistant office furniture
16. Documented and tested emergency evacuation plans

3.33.3 Audit and evaluation techniques for environmental controls**1. Water and Smoke detectors**

The presence of water and smoke detector are verified on visiting the computer room. Also checks adequacy of power supply to these detectors.

2. Hand-held Fire Extinguishers

The presence of fire extinguishers in strategic locations throughout the facility is checked for.

3. Fire suppressions systems

Testing of suppressions systems becomes more expensive, hence reviewing documentation that has been inspected and tested within the last year ensures it.

4. Regular inspection by fire department

The person responsible for fire equipment maintenance is contacted and also the employees are queried, whether, fire department inspector has been invited.

5. Fire proof walls, floors and ceilings Surrounding the computer room

Identifies the fire rating of the walls surrounding the information processing facility are done. These walls should have at least a two-hour fire resistance rating.

6. Electrical surge protector

The presence of electrical surge protector for sensitive and expensive computer equipment is observed.

7. Power leads from two substation

Checking the use and replacement of redundant power lines into the information processing facility.

8. Fully Documented and tested business continuity plan**9. Wiring placed in electrical panels and conduit**

Checking of whether the wiring in the information processing facility is placed in the fire-resistant panels and conduit is done.

10. Documented and tested emergency evacuation plans

A direct interview of the employees is conducted to test whether the emergency plans are posted throughout the facilities.

11. Humidity/Temperature control

To visit on regular intervals and physically determine if temperature and humidity are adequate.

3.33.4 Role of auditor in environmental controls

- ❖ Audit of environmental controls should form a critical part of every IS audit plan. The IS auditor should satisfy that the overall controls assure safeguard the business against environmental risks.
- ❖ The critical factors that auditor should take into account while conducting his audit are:
 1. Audit planning and assessment
 2. Audit of technical controls

(a) Audit planning and assessment of risk

- ◆ 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 risks.
- ◆ The control assessment must ascertain that controls safeguard the organization against all acceptable risks are in place.
- ◆ The security policy of the organization should be reviewed to assess policies and procedures that safeguard the organization against environmental risks.
- ◆ Building plan and wiring plans need to be reviewed to determine the appropriateness of location of IPF.
- ◆ The IS auditor should relevant interview personnel to satisfy about employees' awareness of environment threats and controls.
- ◆ Administrative procedures such as preventive maintenance plans, incidents reporting and handling procedures need to be reviewed.

(b) Audit of technical controls

Audit of environmental controls requires the IS auditor to conduct physically inspection and observe practices.

- ◆ The IPF and the construction with regard to the type of material used for construction.
- ◆ The location of fire extinguishers, fire fighting equipment and refilling date of fire extinguishers.
- ◆ The presence of water & smoke detector, power supply arrangements.
- ◆ Emergency procedures, evacuation plans and marking of fire exits. If necessary, the IS auditor may also use a mock drill.
- ◆ Documents for compliance with legal and regulatory requirement with regard to fire safety equipment, external inspection
- ◆ Power source and conduct tests to assure the quality of power, and generators. Also the power supply interruptions must be checked.
- ◆ Environmental controls requirement such as air-conditioning, dehumidifiers, heaters, ionizers etc.
- ◆ Compliant logs and maintenance logs to assess if MTBF and MTTR (Mean Time To Recover).
- ◆ Activities in the IPF. Identify undesired activities such as smoking, consumption of eatable etc.

3.33.5 Documentation

As part of the audit procedure, the IS auditors should also document all findings. The working paper could include audit assessments, audit plans, audit procedures, questionnaires, interview sheets, inspection charts etc.

NEED FOR CONTROL AND AUDIT OF INFORMATION SYSTEMS: Factors influencing an organisation toward control and audit of computers and the impact of the information systems audit function on organisations are – • Organisational Costs of Data Loss • Incorrect Decision Making • Costs of Computer Abuse • Value of Computer Hardware, Software and Personnel • High Costs of Computed Error • Maintenance of Privacy • Controlled evolution of computer use • Information Systems Auditing • Asset Safeguarding Objectives • Data Integrity Objectives • System Effectiveness Objectives • System Efficiency Objectives	EFFECT OF COMPUTERS ON INTERNAL CONTROLS: 1. Change in the type and nature of internal controls: (RAM'S Personal Assistant) • <u>R</u>ecord keeping • <u>A</u>ccess to assets and records • <u>M</u>anagement supervision and review • <u>S</u>egregation of duties • <u>P</u>ersonnel • <u>A</u>uthorisation procedures 2. Internal controls used within an organisation comprise of the following five interrelated components: • Control environment • Risk assessment • Control activities • Information & communication • Monitoring	EFFECT OF COMPUTERS ON AUDIT 1. Changes to evidence collection: (DEVIL) • <u>D</u>ata retention and storage • Audit <u>E</u>vidence • Lack of <u>V</u>isible output • Lack of a <u>v</u>isible audit trail • Absence of <u>I</u>nput documents • <u>L</u>egal issues 2. Changes to Evidence Evaluation • System generated transactions • Systematic error
RESPONSIBILITY FOR CONTROLS • Long-range planning • Long range planning and IT department • Short range planning or tactical planning • Personnel management controls	THE IS AUDIT PROCESS • 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.	FUNCTIONS OF IS AUDITOR • Inadequate information security • Inefficient use of corporate resources, or poor governance • Ineffective IT strategies, policies and practices • IT-related frauds

CATEGORIES OF IS AUDITS • Systems and Applications • Information Processing Facilities • Systems Development • Management of IT and Enterprise Architecture • Telecommunications, Intranets and Extranets	STEPS IN INFORMATION TECHNOLOGY AUDIT: • Scoping and pre-audit survey • Planning and preparation • Fieldwork • Analysis • Reporting • Closure	COST EFFECTIVENESS OF CONTROL PROCEDURES: Implementing and operating controls in a system involves – • Initial set up cost • Executing cost • Correction costs • Failure cost • Maintenance costs
INFORMATION SYSTEMS CONTROL TECHNIQUES: The basic purpose of information system controls in an organisation is to ensure that the business objectives are achieved and undesired risk events are prevented or detected and corrected.	OBJECTIVE OF CONTROLS: The objective of control is to reduce or if possible eliminate the causes of the exposure to potential loss. Some categories of exposures are: • Errors or omissions • Improper authorizations and improper accountability • Inefficient activity Some of the critical control considerations in a computerized environment are: • Lack of management understanding of IS risks. • Absence or inadequate IS control framework. • Absence of or weak general controls and IS controls. • Lack of awareness and knowledge of IS risks. • Complexity of implementation of controls. The control objectives serve two main purposes: • Outline the policies of the organisation as laid down by the management. • A benchmark for evaluating whether control objectives are met.	

AUUDITOR'S CATEGORISATION OF CONTROLS: • Preventive Controls • Detective Control • Corrective Controls • Compensatory Controls	Classification of controls based on the nature of such controls with regard to the nature of IS resources to which they are applied: • Environmental Controls • Physical Access Controls • Logical Access Controls • IS Operational Controls • IS Management Controls • SDLC Controls	Category of controls is based on their functional nature/Components of Internal Control: • Internal Accounting Controls • Operational Controls • Administrative Controls
CONTROL TECHNIQUES: • Organisational Controls • Management Controls • Financial Control Techniques • Data Processing Environment Controls • Physical Access Controls • Logical Access Controls • SDLC (System Development Life Cycle) Controls • Business Continuity (BCP) Controls • Application Control Techniques	ORGANISATIONAL CONTROLS • Reporting responsibility and authority of each function, • Definition of responsibilities and objectives of each functions, • Policies and procedures, • Job descriptions, • Segregation of duties. MANAGEMENT CONTROLS • Responsibility • An official IT structure • An IT steering committee	FINANCIAL CONTROL TECHNIQUES: • Authorisation • Budgets • Cancellation of documents • Documentation • Dual control • Input/output verification • Safekeeping • Segregation of duties • Sequentially numbered documents • Supervisory review
AUDIT TRAILS – Objectives: (<u>DR. Audit</u>) • <u>D</u>etecting Unauthorised Access • <u>R</u>econstructing Events • <u>P</u>ersonal <u>A</u>ccountability	USER CONTROLS • Boundary Controls • Input Controls • Processing Controls • Output Controls • Database Controls	USER CONTROLS: ERROR IDENTIFICATION, CORRECTION AND RECOVERY CONTROLS Boundary control techniques are: • Cryptography • Passwords • Personal Identification Numbers (PIN) • Identification Cards

PRIME VISION / C.A. FINAL / ISCA / CONTROL OBJECTIVE

Input Controls: Factors affecting coding errors as follows: • Length of the code • Alphabetic numeric mix • Choice of characters • Mixing uppercase/lowercase fonts • Sequence of characters • Existence/Recovery Controls	Processing Controls: • Run-to-run totals • Reasonableness verification • Edit checks • Field initialization • Exception reports • Existence/Recovery Controls	Output Controls • Storage and logging of sensitive, critical forms • Logging of output program executions • Spooling/Queuing • Controls over printing • Report distribution and collection controls • Retention controls • Existence/Recovery Controls
Database Controls: The update controls are: • Sequence Check Transaction and Master Files • Ensure All Records on Files are processed • Process multiple transactions for a single record in the correct order • Maintain a suspense account	Database Controls: The Report controls are: • Standing Data • Print-Run-to Run control Totals • Print Suspense Account Entries • Existence/Recovery Controls	SYSTEM DEVELOPMENT AND ACQUISITION CONTROLS: • Strategic master plan • Project controls • Data processing schedule • System performance measurements • Post-implementation review
CONTROLS OVER THE SYSTEM DEVELOPMENT PHASES AND AUDITOR'S ROLE • Problem definition • Entry and feasibility assessment • Analysis of the existing system • Formulation of strategic requirements (system design) • Organisational and job design • Information processing systems design • Application software acquisition/selection process	CONTROL OVER SYSTEM AND PROGRAM CHANGES: • Management of the change process • Change management controls • System change controls • Program change controls • Authorisation controls • Documentation controls • Testing and quality controls	MANAGEMENT OF THE CHANGE PROCESS • Provide feedback to stakeholders • Prevents system disruptions • Accepted changeover to a new system • Helps users to adapt to new roles • Documentation and follow up on the recommended and implemented process changes • The proposed change need to be reviewed to identify potential conflicts with other systems.

PRIME VISION / C.A. FINAL / ISCA / CONTROL OBJECTIVE

QUALITY CONTROL • Establishment of a quality culture • Quality plans • Quality assurance responsibilities • Quality control practices • System development life cycle methodology • Program and system testing and documentation • Quality assurance reviews & reporting • Training and involvement of end-user and quality assurance personnel • Development of a quality assurance knowledge base • Benchmarking against industry norms	QUALITY CONTROL • Quality Reviews • Contract/Warrants • Service Level Agreements (SLA)	CONTROLS OVER SYSTEM IMPLEMENTATION • Procedures development • Conversion • User final acceptance testing: - Performance testing - Volume testing - Stress testing - Security testing - Clerical procedures checking - Back-up and recovery - Parallel operation
ACTIVITIES TO BE UNDERTAKEN IN PIR: • The main functionality of the operational system • System performance and operation • The development techniques and methodologies employed • Estimated time-scales and budgets • Changes to requirements • Set out findings, conclusions and recommendations in a report	AUDITOR'S ROLE/CONTROL CONSIDERATIONS: • Interview business users • Interview security, operations and maintenance staff • Determine whether the system's requirements have been met • Review system problem reports and change proposals • Confirm that adequate internal controls have been built into the system • Confirm that an adequate Service Level Agreement has been drawn up and implemented • Confirm that the system is being backed up in accordance with user requirements • Review the Business Case • Review trends in transaction throughput	CONTROL OVER DATA INTEGRITY, PRIVACY AND SECURITY – INFORMATION CLASSIFICATION: (TCP/IP) • <u>T</u>op Secret • <u>H</u>ighly <u>C</u>onfidential • <u>P</u>roprietary • <u>I</u>nternal use only • <u>P</u>ublic Documents

DATA INTEGRITY: 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 data processing program. (SID is on the POT) • <u>S</u>ource data control • <u>I</u>nput validation routines • On-line <u>D</u>ata Entry controls • Data <u>P</u>rocessing and storage controls • <u>O</u>utput controls • Data <u>T</u>ransmission controls	DATA INTEGRITY POLICIES • Virus-Signature Updating • Software Testing • Division of Environments • Version Zero Software • Offsite Backup Storage • Quarter-End and Year-End Backups • Disaster Recovery	DATA SECURITY Data security encompasses the protection of data against accidental or intentional disclosure to unauthorised persons as well as the prevention of unauthorised unauthorised modification and deletion of the data.
SECURITY CONCEPTS AND TECHNIQUES CRYPTOSYSTEMS A cryptosystem refers to a suite of algorithms needed to implement a particular form of encryption and decryption.	DATA ENCRYPTION STANDARD (DES): The DES is a cipher (a method for encrypting information) which has enjoyed widespread use internationally. It is a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information.	PUBLIC KEY INFRASTRUCTURE (PKI): 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 used to create an electronic identifier caller a digital signature that uniquely identifies the holder of the private key and can only be authenticated with the corresponding public key.

FIREWALLS Types of Firewalls: (A SIP) • <u>A</u>pplication-Level Firewalls • Proxy <u>S</u>erver Firewalls • Stateful <u>I</u>nspection Firewalls • <u>P</u>acket Filter Firewalls	HACKING: Ways in which a hacker can hack- • NetBIOS • ICMP 'Ping' (Internet Control Message Protocol) • FTP (File Transfer Protocol) • RPC statd • HTTP	Virus: A virus is a program (usually destructive) that attaches itself to a legitimate program to penetrate the operating system. Anti-virus Software: • Scanners • Active Monitor and Heuristic Scanner • Integrity Checkers
LOGICAL ACCESS CONTROLS • Logical access controls restrict users to authorised 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: (D BOOT) • <u>D</u>ial-up Ports • <u>B</u>atch Job Processing • <u>O</u>nline Terminals • <u>O</u>perator Console • <u>T</u>elecommunication Network	LOGICAL ACCESS ISSUES AND EXPOSURES: • Access control software • Application software • Data • Data dictionary/directory • Dial-up lines • Libraries • Logging files • Operator systems exists • Password library • Procedure libraries • Telecommunication lines • Temporary disk files

ISSUES AND REVELATIONS RELATED TO LOGICAL ACCESS: 1. <u>Technical Exposures:</u> (<u>Worms Destroyed D Horse by Throwing Bombs</u>) • <u>Worms</u> • <u>Data Diddling</u> • <u>Rounding Down</u> • <u>Trojan Horse</u> • <u>Salami Techniques</u> • <u>Bombs: Time Bomb & Logic Bomb</u>	2. <u>Asynchronous Attacks:</u> (<u>Pig Ltd.</u>) • <u>Piggybacking:</u> • <u>Data Leakage</u> • <u>Wire-Tapping</u> • <u>Denial of Service</u>	3. <u>Computer Crime Exposures:</u> (<u>Free DISCS</u>) • <u>Financial Loss</u> • <u>Legal Repercussions</u> • <u>Disclosure of Confidential, Sensitive or Embarrassing Information</u> • <u>Industrial Espionage/Blackmail</u> • <u>Sabotage</u> • <u>Loss of Credibility/Competitive Edge</u> • <u>Spoofing</u>
LOGICAL ACCESS CONTROL ACROSS THE SYSTEM • User access management - User registration - Privilege management - User password management - Review of user access rights • User responsibilities - Password use - Unattended user equipment • Network access control - Policy on use of network services - Enforced path - Segregation of networks - Network connection and routing control - Security of network services	• Operating system access control - Automated terminal identification - Terminal log-on procedures - User identification & authentication - Password management system - Use of system utilities - Duress alarm to safeguard users - Terminal time out - Limitation of connection time • Application and monitoring system access control - Information access restriction - Sensitive system isolation - Event logging - Monitor system use - Clock synchronization • Mobile computing - Mobile computing	ROLE OF AN IS AUDITOR IN EVALUATING LOGICAL ACCESS CONTROLS: • Reviewing the relevant documents pertaining to logical facilities • The potential access paths into the system • Deficiencies or redundancies • To verify test controls over access paths to determine its effective functioning • Evaluate the access control mechanism, analyse the test results and verify whether the control objectives has been achieved • Compare security policies and practices of other organisations

PHYSICAL ACCESS CONTROLS: PHYSICAL ACCESS ISSUES AND EXPOSURES- • 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	ACCESS CONTROL MECHANISMS • Identification – the users have to identify themselves, thereby indicating their intend to request the usage of system resources. • Authentication – the users must authenticate themselves and the mechanism must authenticate itself. • Authorisation – the users request for specific resources, their need for those resources and their areas of usage of these resources. - Ticket oriented approach - List-oriented approach	PHYSICAL ACCESS CONTROLS 1. Locks on Doors • Cipher locks • Bolting Door Locks • Electronic Door Locks • Biometric Door Locks 2. Physical identification medium Personal Identification Numbers (PIN) • Plastic Cards • Cryptographic Control • Identification Badges 3. Logging on utilities • Manual Logging • Electronic Logging 4. Other means of controlling Physical Access like: Video Cameras, Security Guards, Controlled Visitor Access, etc.
ROLE OF IS AUDITOR IN PHYSICAL ACCESS CONTROLS: • Risk assessment • Controls assessment • Planning for review of physical access controls • Testing of controls	ENVIRONMENTAL CONTROLS: ENVIRONMENTAL ISSUES AND EXPOSURES: • Fire • Natural disasters • Power spike • Air conditioning failure • Electrical shock • Equipment failure • Water damage/flooding • Bomb threat/attack	

CONTROLS FOR ENVIRONMENTAL EXPOSURES/AUDIT AND EVALUATION TECHNIQUES FOR ENVIRONMENTAL CONTROLS: • Hand-Held Fire Extinguishers • Manual Fire Alarms • Fire Suppression Systems: - Dry-Pipe sprinkling systems - Water based systems - Halon systems • Regular Inspection by Fire Department • Water Detectors • Smoke Detectors • Strategically Locating the Computer Room • Fireproof Walls, Floors and Ceilings surrounding the Computer Room • Electrical Surge Protectors • Uninterruptible Power Supply (UPS)/Generator • Power Leads from Two Substations • Emergency Power-Off Switch • Wiring Placed in Electrical Panels and Conduit • Prohibitions against Eating, Drinking and Smoking within the Information Processing Facility • Documented and Tested Emergency Evacuation Plans		
---	--	--
