Managerial Controls and their Categories

- Controls over the managerial functions that must be performed
    - to ensure development, implementation, operation and maintenance of information systems

Top Management and Information System Management Controls

- Controls adapted by the management –
    - To ensure that the information system function correctly and
    - Meet the strategic business objectives
- Top Management is responsible for preparing a master plan for the organisation
- Major functions a senior manager must perform are as follows
    - Planning
    - Organising
    - Leading
    - Controlling

Planning	Preparing the plan involves the following • Recognising the opportunities and problems confronting the organisation-where IT and IS can be used • Identifying Resources needed to provide required IT and IS • Formulating Strategies and tactics for acquiring the needed resources Types of Plans • Strategic Plan:- Long run plan, next 3-5 years is covered • Operation Plan:- Short plan, next 1-3 years Steering Committee • Consist of the representatives from all areas of business and IT personnel • Steering Committee to assume overall responsibility for activities of Information System function
Organising	There should be a prescribed IT structure with documented roles and responsibilities and agreed job descriptions • Resourcing the Information System Function:- Acquire the resources required to accomplish the goals and objectives set in the information systems plan • Staffing the Information System Function:- involves o Acquisition of Information Systems Personnel o Development of Information System Personnel o Termination of Information System Personnel
Leading	Motivating, guiding and communicating with personnel • Motivating and Leading the Information System Personnel:- Many theories exist but no one best way • Communicating with IS personnel:- Effective communications are essential for promoting good relations
Controlling	Comparing the actual performance with planned performance • Overall Control of IS function:- How much should be spent on

	the IS function and the value for the money received by the organisation • Control of IS Activities:-Top management to control the activities on the basis of policies and procedures • Control over Information System Services:- Each services-estimates to be made of expected benefits and resource consumption

System Development Management Controls

Activities dealing with the System Development controls in IT setup are as follows

- System Authorisation activities
- User Specification activities
- Technical Design activities
- Internal Auditor Participation
- Program Testing
- User Test and Acceptance Procedures

System Authorisation activities	• All systems to be authorised to ensure economic justification and feasibility • New system request to be submitted In written form by users to system professionals
User Specification activities	User to create a specification document describing the logical needs that must be satisfied by the system
Technical Design activities	• Translating the user specifications • Scope of these activities involve-system analysis, general system design, feasibility analysis and detailed system design
Internal Auditor Participation	Auditor should become involved at the inception of SDLC process to make suggestions regarding system requirements
Program Testing	• Program Modules to be thoroughly tested before implementing • Results of tests to be compared with pre-determined results to identify programming and logic errors
User Test and Acceptance Procedure	• Individual modules to be tested as unified whole. • Test team comprising the user personnel, system professional and internal audit personnel to subject system to rigorous testing

Programming Management Controls

- Major phase within the system development life cycle –Primary objective is to produce/acquire or implement high quality programs
- Phases in Program Development Life Cycle are

- Planning:- Techniques like PERT, Gantt Charts to be used to monitor progress against plan
- Control:- Two purpose of this phase are-
  - Task progress in software life cycle phases to be monitored against plan and corrective action to be taken and
  - Control over software development, acquisition and implantation to be exercised
- Design:- Systematic approach to program design is adopted
- Coding:- Programmer to choose a module implementation and integration strategy , a coding and documentation strategy
- Testing:- Three types of testing
  - Unit Testing:- Focuses on individual program modules
  - Integration Testing:- Focus on the groups of program modules
  - Whole of Program Testing:- Focus on the whole program
- Operation and Maintenance:-establishes the formal mechanisms to monitor the status of operational programs so maintenance needs can be identified
  - Repair Maintenance:- Program errors are corrected
  - Adaptive Maintenance:- Program modified to meet changing user requirements
  - Perfective Maintenance:- Program is tuned to decrease the resource consumption

Data Resource Management Controls

- Data is a critical resource to be managed properly
- Better users to be able to share data and data to be available when needed, in the form and in the location where it is needed
- Controls to be exercised over by appointing senior, trustworthy personnel and maintaining and monitoring logs of the data administrators and database administrators activities
- Control activities in maintaining integrity of database is
  - Definition Controls
  - Existence/backup controls
  - Access Controls
  - Update Controls
  - Concurrency Controls
  - Quality Controls

Definition Controls	To ensure database corresponds and complies with the definition standards
Existence/Backup Controls	• Ensure existence of database • Backup refers to making copies of data- to be used to restore the original data after data loss • Various back-up strategies are:-

	○ Dual recording of data:- two complete copies maintained ○ Periodic Dumping of data:- into a backup storage medium, e.g. removable disk ○ Logging input transactions:- logging input data transactions causing change to database ○ Logging changes to data:- copying a record each time changed by update
Access Controls	Prevent unauthorised viewing, retrieving, computing or destroying the entity's data-this is ne through User access Controls and data encryption
Update Controls	Restriction on update of database • Permitting only data addition of database • Allowing users to change or delete existing data
Concurrency Controls	Provide solutions to data integrity problems-when the two update processes access the same data item at the same time
Quality Controls	Ensure the accuracy, completeness and consistency of data maintained in the database

Quality Assurance Management Controls

It is concerned with ensuring that the

- Information systems produced –achieve certain quality goals
- Development, implementation , operation and maintenance of information system comply with a set of quality standards
- Reasons for the emergence of Quality Assurance in many organisations are as follows
    - Organisations-Producing safety critical systems and users more demanding in terms of quality of software
    - Organisations undertaking more ambitious projects when they build software
    - Users are becoming more demanding in terms of expectations
    - Organisations becoming more concerned about the liabilities
    - Poor quality controls lead to missed deadlines and dissatisfied users and customers
    - Improving information System quality- a part of improving the quality of goods and services being sold
- Quality assurance personnel to work to improve the quality of information system produced. Implemented, operated and maintained. They are to ensure
    - Quality goals are established and understood by all stakeholders
    - Compliance occurs with the standards that are in place

Security Management Controls

Information Security Managers are responsible for ensuring that the information system assets classified under Personnel, Hardware, Facilities, Documentation, Supplies, Data, Application Software and System software are secure.

Threat identification:- a threat is some event or action that can lead to a loss. During threat identification phase, security administrators attempt to remove out all the threats that can result in information system assets being lost, destroyed or damaged

Major Security threats and their control measures

Threat	Controls
Fire	Well-designed, reliable fire protection systems
Water	Facilities to be designed and sited to mitigate losses
Energy variations	Voltage regulators, circuit breakers and uninterruptible power supply
Structural damage	BCP. DRP facilities to be adapted
Pollution	Regular cleaning of facilities and equipment
Unauthorised intrusion	Physical access controls
Viruses and Worms	Controls to prevent use of virus infected programs
Misuse of software, data and services	Code of conduct to govern the actions of IS employees
Hackers	Strong Logical Access controls to mitigate losses from the activities of hackers

When the disaster strikes the last resort controls adopted are –A Disaster Recovery Plan (DRP) and Insurance

DRP:-Comprehensive DRP plan comprise of the four parts- Emergency Plan, Backup Plan, Recovery Plan and a test plan. Plan lays down the policies,guidelines and procedures for all IS Personnel

Insurance Cover:- Must be able to replace the information system assets and cover the extra cost associated with the restoring normal operations

Operations Management Controls

Operations Management typically performs controls over the functions as below:-

- Computer Operations
- Network Operations
- Data Preparation and Entry
- Production Control
- File Library
- Documentation and Program Library

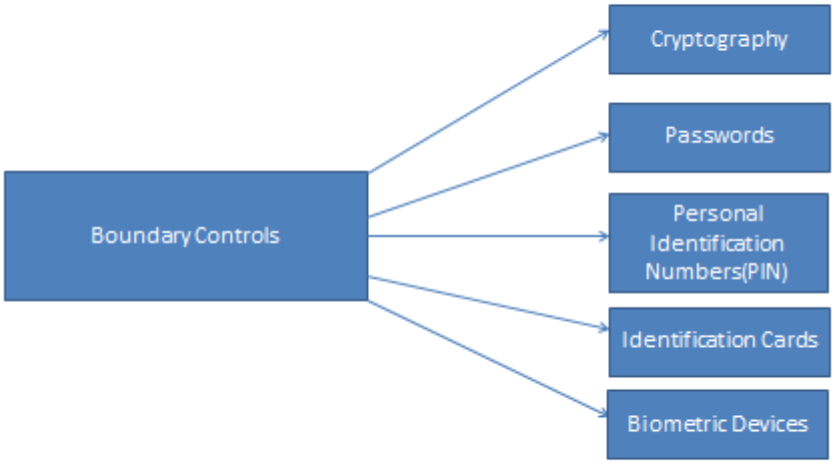
- Helpdesk/Technical Support
- Capacity Planning and Performance Monitoring
- Management of outsourced operations

Computer Operations	Controls over the computer operations govern the activities that directly support the day to day execution of the either test or production systems. Three types of controls under this- Operation Controls(what human operators or automated operation facilities must perform) , Scheduling Controls(how jobs are to be scheduled on a hardware/software platform) and Maintenance Controls (how hardware is to be maintained)
Network Operations	Proper functioning of network operations and monitoring performance of network communication channels, network devices, network programs and files
Data Preparation and Entry	Facilities to be designed to promote speed and accuracy
Production Control	Receipt and dispatch of input and output, job-scheduling, management of service level agreement with users
File Library	Includes management of organisations machine readable storage media like magnetic tape, cartridges and optical disks
Documentation and Program Library	Documentation librarians ensure that the documentation is stored securely –only authorised personnel gain access to documentation
Help Desk/Technical Support	Assist end users to employ end –user hardware and software such as microcomputers, spread sheet packages
Capacity Planning and Performance Monitoring	Regular Performance Monitoring enables the identification of resource deficiencies
Management of Outsourced operations	Responsibility for carrying out the day to day monitoring of the outsourcing contract

Application Controls and their categories

- Application system controls are undertaken to accomplish reliable information processing cycles that perform the processes across the enterprise
- Different application controls are as follows
    - Boundary Controls
    - Input Controls
    - Communication Controls
    - Processing Controls
    - Database Controls
    - Output Controls

Boundary Controls



Cryptography:- deals with programs for transforming the data into cipher text, a person not having the authentication will not be able to access the same

Passwords:- User identification by authentication mechanism with personal characteristics like name, birth date, employee code, function, designation or combination of these

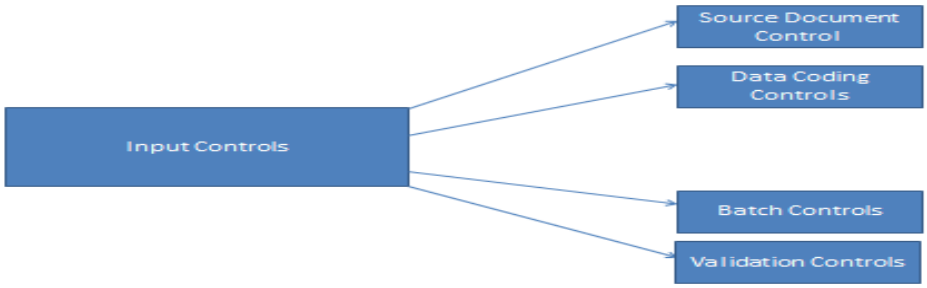
Personal Identification Number:- PIN is similar to password assigned to a user

Identification Cards:- store information required in authentication process

Biometric Devices:- Thumb and or finger impression, eye retina etc, are also used as boundary control techniques

Input Controls

- Ensure the accuracy and completeness of data and instruction input into an application system



Source Document Controls

Systems using physical source documents to initiate transactions need to exercise careful controls .Organisation to implement control procedures as

- Use Pre-numbered source documents(Unique sequential no. in each document)
- Use Source Documents in sequence (Adequate physical security at the user site)
- Periodically audit source documents (Missing documents to be identified

Data Coding Controls

Two types of errors can corrupt a data code and cause processing errors

- Transcription Errors –Fall into three categories
  - Addition Errors:- Extra digit is added to the code
  - Truncation Errors:- When a digit or character is removed from the code
  - Substitution Errors:- replacement of one digit in code with another
- Transposition Errors:-
  - Single Transposition Errors:- Two adjacent digits are reversed
  - Multiple Transposition Errors:- Non-adjacent digits are transposed

Batch Controls

Grouping together transactions that bear some type of relationship to each other Two types of batches occur

- Physical Controls:- Groups of transactions that constitute a physical unit. E.g source documents may be obtained via mail,assembled into batches, spiked and tied together
- Logical Controls:- Group of transactions bound together on some logical basis

Validation Controls

Input Validation controls are intended to detect errors in the transaction data before the data are processed

Communication Controls

Three major exposures that arise in communication system are

- Transmission impairments:- difference between data send and received
- Component failure:- data can be lost or corrupted
- Hostile party could seek to subvert data transmitted through the subsystem

Physical Component Controls

Transmission Media	Physical path along which a signal can be transmitted between buyer and seller. It is of two types • Guided Media:- Twisted pair, coaxial cable • Unguided Media:- satellite microwave, radio frequency and infrared
Communication Lines	Reliability can be improved by choosing a private(leased) communication line than a public communication line
Modem	Increases the speed at which data can be transmitted over a communication line
Port Protection Devices	Used to migrate exposures associated with dial up access to a computer system
Multiplexers and concentrators	Allow the band width or capacity of a communication line to be used more effectively

Line Error Control

Whenever data is transmitted over a communication line, it can be received in error be because of attenuation distortion (reduction of the amplitude of a signal) or noise

Flow Controls

Two nodes in a network can differ in terms of the rate at which they can send, receive and process data

Link Controls

Managing the links between two nodes in a network

Topological Controls

A communication network topology specifies the location of nodes within a network

Channel Access Controls

Two different nodes in a network can compete to use a communication channel. Whenever the possibility of contention for the channel exists, some type of channel access control technique must be used

Internetworking Controls

Connecting two or more communication networks together to allow the users of one network to communicate with the users of other networks

Three types of devices used to connect sub networks are

- Bridge:- Bridge connects similar LAN's (one token ring network to another token ring network)
- Router:- Most routers connect a LAN (like the one in your home or office) to a WAN (like the cable system running your cable modem) by interfacing

a broadband modem to the network within the enterprise, small office, or home.

- Gateway: - In a workplace, the gateway is the computer that routes traffic from a workstation to the outside network that is serving up the Web pages. For basic Internet connections at home, the gateway is the Internet Service Provider that gives you access to the entire Internet.

Processing Controls

Processing subsystem is responsible for computing, sorting, classifying and summarising data

Processor Controls – Controls that can be used to reduce expected losses from errors and irregularities associated with central processors

Database controls

Protecting the integrity of the database

Output Controls

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

INFORMATION TECHNOLOGY GENERAL CONTROLS

- Basic Policies and procedures that ensure that
  - an organisation's information systems are properly safeguarded,
  - application programs and data are secure,
  - computerised operations can be recovered in case of unexpected interruptions
- Most Common ITGC's are as follows:-
  - Logical access controls over infrastructure, applications and data
  - System Development Life Cycle Controls
  - Program Change Management Controls
  - Data Centre physical security controls
  - System and data backup and recovery controls
  - Computer operation controls

Controls over data integrity and security

- Classification of information and documents is essential
- Classification of information based on the sensitivity level are as follows
  - Top Secret:- High Sensitive information-Mergers and Acquisition
  - Highly Confidential:-If shared around the organisation would impede the organisation's operations. E.g.: Patient's Medical records
  - Proprietory:-Define a way in which an organisation operates. It is of use to authorised personnel only

- Internal Use only:- Information is not approved for the general circulation outside the organisation. E.g.-Minutes of meeting, Internal Project Reports
- Public Documents:- Information in public domain like annual reports, press-statements

Data Integrity

- Primary objective is to prevent, detect and correct errors in transactions as they flow through different stages
- There are six categories of integrity controls summarised as follows
  - Source Data Controls:- Pre numbered forms, review for authorisation
  - Input Validation routines:- Key data fields, limit, range
  - Online-data entry controls:- Redundant data checks, compatibility tests
  - Data processing and storage controls:-Reconciliation of the database totals with externally maintained tools
  - Output Controls:- System outputs confirm to organisational objectives
  - Data Transmission Controls:- Design network to handle peak processing, multiple communication paths
- Data Integrity Policies
  - Virus-Signature Updating:- automatically update the signatures when they are made available from the vendor through enabling of automatic updates
  - Software Testing:- All software must be tested in a suitable test environment
  - Division of environment:- Division of environment into Development, Test and Production
  - Offsite backup storage:- Offsite backups for backups older than one month
  - Quarter and year end backup:- must be done separately for accounting purposes
  - Disaster Recovery:- Comprehensive plan to ensure the continuity of business operations

Financial Controls

- Controls used by the System user over the source or transaction origin, documents before system input
- Financial control techniques are
  - Authorisation- obtaining authority to perform some act
  - Budgets:- estimates of the amount of time or money expected to be spent
  - Cancellation of documents:- Preventing the reuse by marking it
  - Dual Control:- Simultaneously access an asset. Two tellers in bank open depository vault together
  - Input/output Verification:- Comparing the information provided by a computer system to the input records
  - Safekeeping:-Physically securing assets, such as computer disks under lock and key

- Sequentially numbered documents:- pre-printed sequential numbers which enable detection of missing documents

Personal Computer Controls

- Risks are as follows
  - PCs are small in size and easy to connect and disconnect
  - Pen-drives can be easily transported
  - PC is single user oriented machine- no inherent data safeguards
  - Segregation of duties not possible
  - Operating staff may not be adequately trained
- Security measures
  - Physically locking the system
  - Proper logging of equipment shifting
  - Centralised purchase of hardware and software
  - Use of antimalware software

Cyber Frauds

Major reasons for increase in cyber frauds are as follows

- Failure of Internal Control System
- Failure of Organisations to update themselves
- Small fraudsters target the weakness in the system

Major Cyber Attacks

Some of the major Cyber Attacks are as follows

- Phishing
  - **Phishing** is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication
  - Phishing is typically carried out by email spoofing and it often directs users to enter personal information at a fake website, the look and feel of which are identical to the legitimate one and the only difference is the URL of the website in concern
- Network Scanning
  - Network scanning is a procedure for identifying active hosts on a network, either for the purpose of attacking them or for network security assessment.
- Virus/Malicious Code
  - A computer virus is a type of malicious software program ("malware") that, when executed, replicates itself by modifying other computer programs and inserting its own code
- Spam
  - Electronic spamming is the use of electronic messaging systems to send an unsolicited message (spam), especially advertising, as well as sending messages repeatedly on the same site.
- Website Compromise /Malware Propagation

  - It includes website defacements. Hosting malware or websites in an unauthorised manner
- Others
  - Crackers:- are hackers with malicious intentions
  - Eavesdropping:- Eavesdropping is secretly listening to the private conversation of others without their consent
  - E-Mail Forgery:-Sending e-mail messages that look as if someone else sent it is termed as E-Mail forgery
  - E-Mail threats:- Sending a threatening message to try and get recipient to do something
  - Scavenging:- Gaining access to confidential information by searching corporate records
- Impact of Cyber Frauds on Enterprises
  - Financial Loss
  - Legal Repercussions
  - Loss of Credibility or competitive edge
  - Disclosure of confidential, sensitive or embarrassing information
- Techniques to commit Cyber frauds
  - Hacking:-unauthorised access and use of computer systems
  - Cracking:-Crackers are hackers with malicious intentions
  - Data Diddling
  - Data leakage:-unauthorised copying
  - Denial of Service attack:-Series of actions preventing access to software system
  - Internet Terrorism:- use of internet to disrupt e commerce and destroy communications
  - Logic time bombs:- lies idle until special circumstances
  - Masquerading or Impersonation:- pretending to be an authorised users
  - Password cracking:-steals file containing valid password
  - Piggybacking:- tapping into telecommunication line and latching on
  - Round down:- computer rounds all the interest calculations and the remaining fraction is placed in account run by perpetrator
  - Scavenging or dumpster diving:- In the IT world, dumpster diving refers to using various methods to get information about a technology user. In general, dumpster diving involves searching through trash or garbage looking for something useful.
  - Social engineering: - Gradually the hacker gains the trust of the target and then uses that trust to get access to sensitive information like password or bank account details**.**
  - Super Zapping:- Using software that bypasses normal security constraints to allow unauthorized access to data.
  - Trap Door:- Perpetrator enters in the system using a back door that bypasses normal system control and perpetrates fraud