CHAPTER 3

CA AKHIL MITTAL

CONTROL OBJECTIVES

E-MAIL : caakhil24.srcc@gmail.com

CHAPTER 3

CONTROLS OBJECTIVES

1) INFORMATION SYSTEM CONTROL:

- Information technology covers all key aspects of business processes of the organisation & has on impact on its strategic & competitive advantage.

- Control is defined as: Policies, Procedures, practices & enterprise structure that are designed to provide reasonable assurance that objectives are accomplished.

2) NEED FOR CONTROL & AUDIT OF INFORMATION SYSTEM:

Following are the factors which influence the organisation control & audit of the computers:

CODE TO REMEMBER: C.V.A.A.S. - - D.E.E. - - Mc.D.

(Chaminda Vaas Sister (Dee) in McDonald)

1.Cost of data loss:

- **Data is critical resources for an organisation,**
- **for its processes & ability to adapt in the changing environment.**

2.Value of Computer hardware, Software & Personnel:

- **These are critical resources of the organisation having impact on the organisation,**
- **& such proper control to be fixed on these resources.**

3.Computer **A**buse:

- **Unauthorised access to computers, viruses, unauthorised physical access can lead to destruction of the assets, hence required proper control.**

4.Auditing of information system :

- **It is the process of focusing on the asset safeguard & data integrity.**

5.Safeguard of assets:

- **The information system assets** must be **protected** by a system of **INTERNAL CONTROLS** from unauthorised access.

6.Data Integrity objectives:

- **Integrity of data depends on the value of the information.**
- Importance to maintain data integrity depends on:
  - **VALUE OF INFORMATION**
  - **EXTENT OF ACCESS TO INFORMATION**
  - **VALUE OF DATA TO BUSINESS**

7.Efficiency / effectiveness of system:

- **Effectiveness:** evaluated by **Auditing the characteristics & objective of system.**
- **Efficiency:** To optimise the **use of various information system resources.**

8.Error by computer:

- **In this technological environment,** one error during the process/ entry,
- **Can cause great damage** since it relates to **critical business processes.**

9.Maintenance of Privacy:

- **Data collected** in respect of an individual on **medical, educational etc.**
- With the use of computers it might be possible that **a person may access to** these information **without proper channel. [Unauthorised Access].**

10. Controlled evaluation of computer use:

- **Excess use & dependency on the computers may be destructive.**
- **It is not possible to guarantee the success of the process** with the use of the technology. **As such** there must be controlled computer use.

11. Decision making (faulty):

- Management & operational **controls** taken by the managers **involves detection, investigation & correction of out-of-control processes.**
- **For effective & successful decisions it is imperative that** management uses **correct data.**

3) EFFECT OF COMPUTERS ON INTERNAL CONTROL:

The internal controls within enterprises in **a computerised environment** cover the **following major areas:**

A. Personnel:

-- Whether staff is trustworthy or not.

-- Whether the personnel knows what are their objectives & if they have requisite skill to do.

B. **Segregation of duties:**

-- Segregation means **various stages in the process of a transaction** are split among people.

-- Within a computerised environment, the staffs **know the interrelationship** between the source of data, how it is processed & distribution & use of the outputs.

C. **Authorisation procedures:**

-- To ensure that **transactions are approved.**

-- **In on-line** transaction system, **written evidences of individual** data entry authorisation

D. **Record Keeping:**

-- Controls over **protection & storage of documents, transaction details & audit trail** etc

E. **Access to assets & records:**

-- Clients financial information is more prone to **unauthorised access.** Increased use of the networking facilities **increases the risk of unauthorised access.**

-- As such proper controls are needed to protect the critical information by way **of physical & logical controls.**

F. **Management supervisions & review:**

-- Management supervisions & review helps **in detecting ERROR & FRAUD** on regularly basis.

G. **Concentration of programs & data:**

-- Transactions, programs & data files may be stored in **computer readable form.**

-- In the absence of appropriate controls over this programs from **unauthorised access**

4) EFFECT OF COMPUTERS ON AUDIT:

To evaluate as to whether the business processes activities are recorded as per standards. To do the same, **2 basic functions** carried out to examine these changes are:

CHANGES TO EVIDENCE COLLECTION

Changes in the audit trail may lead to difficulty for the financial auditor **in gathering sufficient,** appropriate audit evidences to **validate** the figures in the client's financial statements.

If client uses computerised financial system, some audit trial may exist in machine readable form. As such **auditor** has to use specialised audit tools.

CODE TO REMEMBER: D.R. - L.A.L.A.

A. Absence of input **D**ocuments:

- Transactions may be entered into computer without proper documents.
- E.g. Input of telephone orders into telesales system.
- EDI (**Electronic Data Interchange**) will result in **LESS PAPERWORK.**

B. **R**etention & storage of data:

- Client's storage capabilities may restrict the amount of historical data,
- The same can be **stored ON-LINE** for easy access to all the users.
- If client has insufficient data retention, auditor is not able to get view of reporting processes of the business.

C. **L**ack of visible output:

- Transaction processing may not produce a **HARD COPY** i.e. printed record.
- In absence of physical records, **auditor has to access electronic data records** of the client's computer.

D. **A**utomatic transaction generation:

- Certain transactions may be generated automatically by the computer system.
- As such these transactions are not supported by documents & formal way **i.e. signature of manager, supervisor etc.**
- For example, **depreciation is charged automatically by the system.** If I would relate it with tax computation **(COMPUTAX)** , u remember that we just put the **opening, addition & deletion amount** of assets, & in computation sheet we get the amount of **depreciation as computed by the system.**

E. **L**egal Issues:

- Most of the organisation is making use **of EDI** for their business purposes.
- However at time of making contracts, it is difficult to establish the terms of the contracts **such as WHERE IT IS MADE, WHAT ARE PARTIES TO CONTRACTS** etc.
- These legal issues may differ from country to country & even state to state.

F. **A**udit trial lacks:

- Audit trial in a computerised system lacks visible audit trial.
- As such auditor is bound to follow **various audit approach** such as audit around the computers.
- Absence of audit trial makes the work of auditor **CUMBERSOME.**

CHANGES TO EVIDENCE EVALUATION

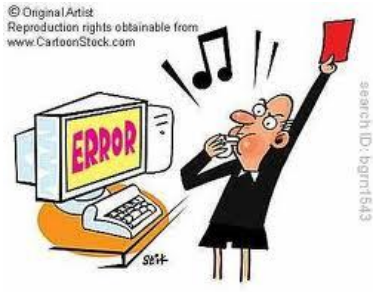
Evaluation of the audit trial aims at tracing the consequences of **control strength & weaknesses through the system.**

As such it is possible to identify **periodic & deterministic errors.**

SYSTEM GENERATED TRANSACTIONS

- Financial systems have the ability to **initiate, approve & record financial transactions.**
- EDI system **helps the organisation to provide faster processing** without the manual intervention.

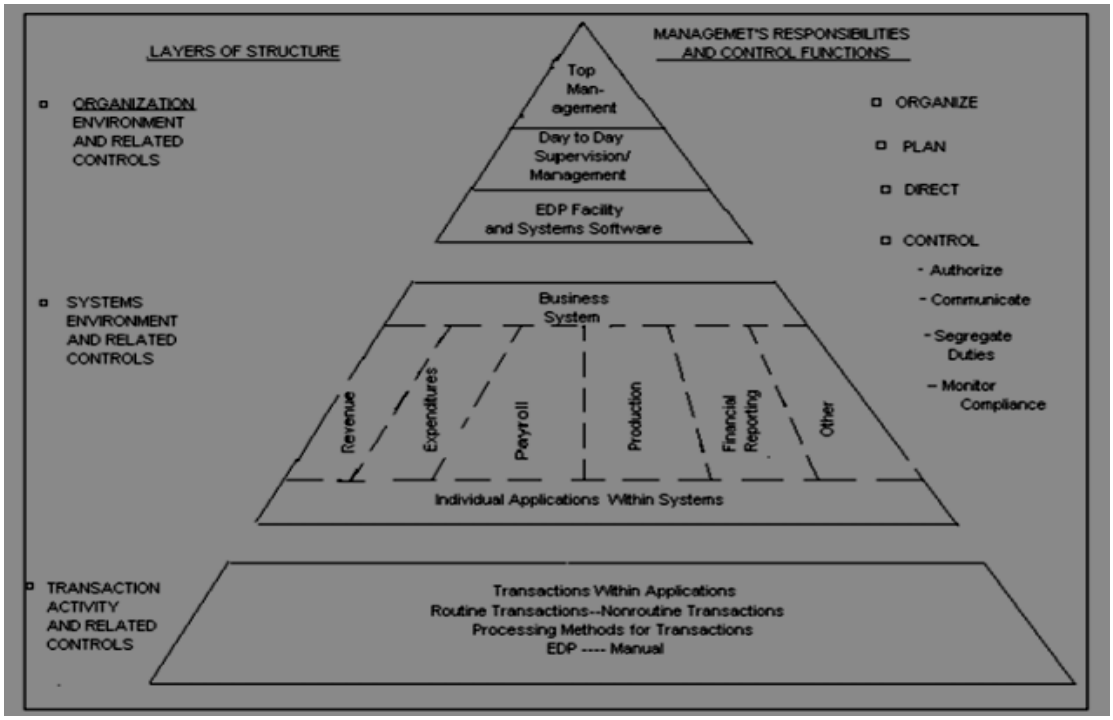
SYSTEMATIC ERRORS



- Computers are **designed** to carry out processing on continuous basis.
- It may not possible that with **same inputs,** every time **same output** is obtained.

5) RESPONSIBILITY FOR CONTROLS:

- **MANAGEMENT** is responsible for **establishing & maintaining controls.**
- Management should **consistently apply the INTERNAL CONTROLS** standards to meet the organisational objectives.
- Number of management level depends upon company **size & organisation structure.**



LONG RANGE PLANNING:

INCLUDES: Documenting goals & objectives which are as under:

-- Revenue & expenses expenditure.

-- Time allowance & target areas

Long range planning & IT department: Information system managers must take measures to:

-- Develop & implement cost effective controls.

--Assess the adequacy of internal control in operation.

--Identify needed improvement.

Short range planning or tactical planning:

Functions & activities performed **every day** are established to **meet the LONG RANGE GOALS**:

PERSONNEL MANAGEMENT CONTROLS:

This involves activities & functions to **accomplish the administration of individuals, salary & benefit cost.** Control techniques are:

- **JOB DESCRIPTAION:**
  -- Measurement control to communicate management requirement.
  -- Provides standard of PERFOAMNCE MEASUREMENT.

- **SALARY & BENEFIT BUDGET:**
  -- Identify COST FACTORS & evolve a strategic plan,
  -- for new products & services.

- **RECRUTING STANDARDS & BUDGET:**
  -- Requires TECNHICAL training & experience to develop & maintain,
  -- operational efficiency.

- **JOB PERFORMANCE EVALUATION:**
  -- To counsel & motivate employees to maintain,
  -- quality of system design.

- **SCREENING & SECURITY STANDARD:**
  -- Screening & credit reports are preventive control measures,
  -- with applicable labour laws & regulations.

6) THE IS AUDIT PROCESS:

Audit of **IS environment** includes the assessment of the:

- Internal controls within IS environment to **assure, validity, reliability & security information.**
- Efficiency & effectiveness of the **IS environment** in economic terms.

7) RESPONSIBILITY OF IS AUDITOR:

Following is the set of skill that an auditor must possess:

Must possess knowledge of: **1.** **B**usiness operations, practices

B.I.T.S.

2. **I**T strategies, policy & procedure control

3. Professional **T**echnical qualifications & certifications

4. Professional **S**tandards, best practices of IT control

Understanding of: **1.** Technical & manual controls relating to business continuity

2. Information Risks & Controls.

8) FUNCTIONS OF IS AUDITOR:

IT auditor should review risks relating to **IT SYSTEM** and processes, some of them:

- ☯ Inadequate Information security
  - ■ **Out of date antivirus controls, open system without password.**
- ☯ Inefficient use of corporate resources.
  - ■ **Huge spending on unnecessary IT projects like** storage devices, printing.
- ☯ Ineffective IT strategies, policies & practices.
  - ■ **Lack of policies for use of Information & communication Technology.**
- ☯ IT related frauds.
  - ■ **Includes hacking.**

9) CATEGORIES OF IS AUDITS:

CODE TO REMEMBER: S.I.S.-I.T.

caakhil24.srcc@gmail.com

A. System & applications:

i. To verify that system & applications are appropriate & efficient.
ii. Ensuring valid, reliable, timely input & outputs at all levels of system's activity.

B. Information processing Facilities:

i. To verify that processing facility is controlled to ensure,
ii. Accurate, reliable, timely processing of applications under disruptive conditions.

C. Systems Development:

i. To verify that systems under development meet objective of the organisation & to ensure,
ii. Those systems are developed in accordance with accepted standards of entity.

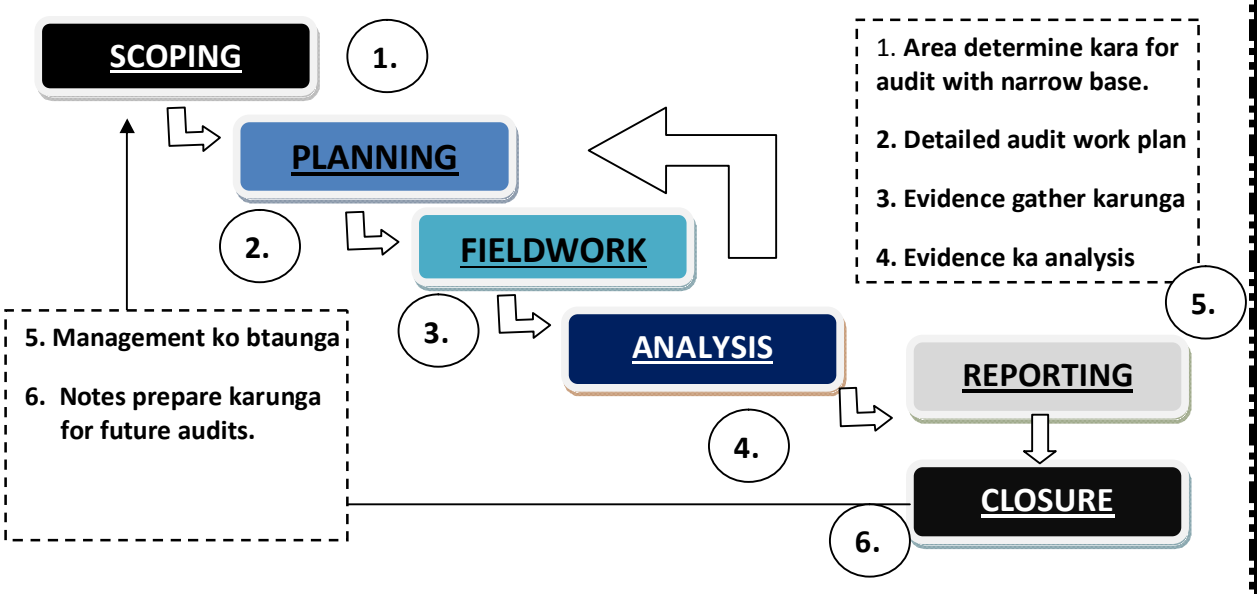
D. IT & Enterprise Architecture management:

i. That IT management has developed ORGANISATIONAL STRUCTURE & PROCEDURES,
ii. To ensure that a controlled & efficient environment for information processing.

E. Telecommunication, Intranet & Extranet:

i. To verify that controls are in place of the CLIENT server & on networking connecting CLIENTS & SERVERS.

10) STEPS IN INFROMATION TECHNOLOGY AUDIT:



Now explaining each of the steps in detail:

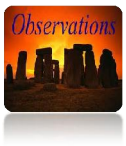
1. SCOPING

1. Auditor determines main AREA of focus based normally on some form of RISK BASED ASSESSMENT.

2. Information sources are :


WEB BROWSING

PREVIOUS AUDIT REPORT



OBSERVATIONS

PRE AUDIT REVIEW

2. PLANNING

1. Here scope of audit is **BROKEN** into **GREATER LEVELS** of details, **involving** generation of **AN AUDIT WORK PLAN.**

3. FIELDWORK

1. Gathering **EVIDENCES** by interviewing **STAFF, MANAGER,** reviewing documents, data, observing processes.

4. ANALYSIS

1. Steps involve **sorting out & reviewing all types of evidences gathered.** Techniques of the analysis:

   SWOT: **S**trength **W**eakness **O**pportunities **T**hreats

   PEST: **P**olitical, **E**conomic, **S**ocial & **T**echnological

5. REPORTING

1. Reporting to management is done after the data is gathered & analysed

6. CLOSURE

1. Involves **PREPARING NOTES** for future audits & follow up of the actions that the management promised to undertake in respect of the previous reports.

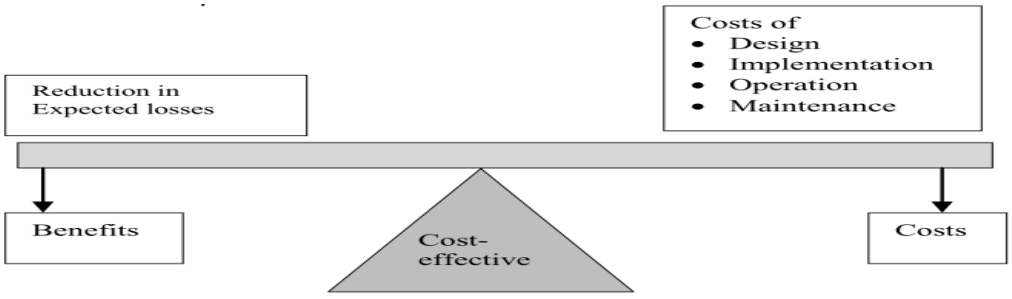
I am not explaining the following topics in this chapter:

1. **AUDIT STANDARDS** (You will study the same in Audit)
2. **ISO 27001** (Same is explained in chapter 8 of ISCA)
3. **ITIL** IT Infrastructure Library (Same is explained in chapter 8)
4. **COBIT** (Same is explained in chapter 8)

11) COST EFFECTIVENESS OF CONTROL PROCEDURES :

- Before implementing any internal control, it is imperative to do **cost & benefit analysis.** It is necessary to ascertain whether these controls are not disrupting the operations.

  Therefore, the **objective of designing an INTERNAL CONTROL SYSTEM** is to provide **reasonable assurance** that **control problems** don't take place.



Implementing and operating controls **in a system involves the following 5 costs:**

I am here by trying to link the points:

Initial cost	executing cost	correction cost	failure cost	Maintenance cost
Cost control Design karne ki cost starting mein	Design karne ke baad, i implemented. Uski cost	Error hui usko thik karne ki cost	Control error detect nhi kar paya uski cost	Control ki working thik rhe uski cost

- BENEFIT OF CONTROL PROCEDURE = EXPECTED LOSS WITH CONTROLS - EXPECTED LOSS WITHOUT CONTROLS

12) INFORMATION SYSTEMS CONTROL TECHNIQUE :

- **PURPOSE:** To ensure that **business objectives are achieved & undesired risks are prevented.**

- This is achieved by **designing information control framework** which comprises **policies, procedures, practices & organisation structure.**

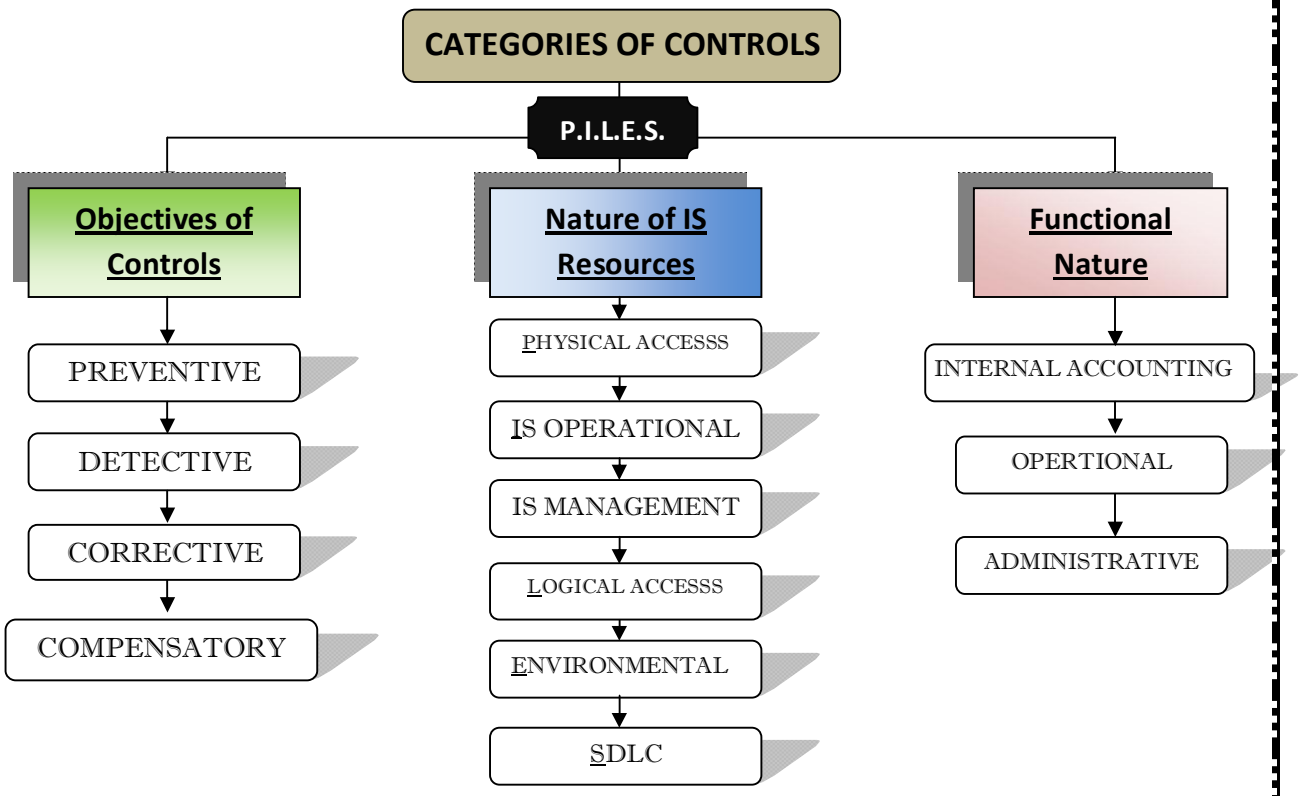
- **OBJECTIVES OF CONTROLS:**
  Objective of controls is to REDUCE/ELIMINATE causes of the exposure to **potential loss.**

- **CONTROL OBJECTIVE:**

  "A STATEMENT OF DESIRED RESULT TO BE ACHIEVED BY IMPLEMENTING CONTROL PROCEDURES IN PARTICULAR IT PROCESS OR ACTIVITY".

OBJECTIVE ***of control objectives***

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



caakhil24.srcc@gmail.com

Now explaining each of the controls in detail:

OBJECTIVES OF CONTROLS

TYPE OF CONTROL	CHARACTERISTIC	EXAMPLES
PREVENTIVE CONTROL 	-- Understanding vulnerabilities of assets -- Understanding probable THREATS -- Provision of necessary controls	-- Segregation Of duties -- Access Control -- Firewalls, Antivirus software
DETECTIVE CONTROL 	--Detecting Errors, omissions, malicious act etc --Clear understanding of lawful activities & report deviation -- Surprise Checks by supervisor	--Error message over tape labels. --Periodic report of the performance with variance -- Internal Audit functions
CORRECTIVE CONTROL	--Minimise impact of the THREAT --Identify the CAUSE of problems --Correct error arising from a problem --Getting feedback from detective & preventive control	--Backup procedures. --Rerun procedures --Contingency Planning
COMPENSATORY CONTROL	--Designed to REDUCE probability of threats. --Implemented where organisation is not able to have appropriate CONTROLS. --Compensatory measures to be adopted to reduce probability of threats	

ANOTHER CLASSIFICATION OF CONTROLS **based on NATURE of such controls is as under:**

NATURE OF IS RESOURCES

TYPE OF CONTROL	CHARACTERISTIC	EXAMPLES
PHYSICAL ACCESS CONTROL 	-- Controls relating to PHYSICAL SECURITY of the tangible IS resources & intangible resources.	-- Access control Doors -- Security Guard -- Door Alarm
IS OPERTIONAL CONTROL	-- Controls relating to IS operations, administration & its management.	-- Helpdesk Operations -- IS Infrastructure mgmt.
IS MANAGEMENT CONTROL	-- Controls relating IS management, policies, procedures, standards etc	-- Monitoring of IS operations -- Steering Committee
LOGICAL ACCESS CONTROL 	-- Controls relating to logical access to information resources.	-- Networking Control --Application boundary controls
ENVIRONMENTAL CONTROL 	-- Controls relating for HOUSING IT resources	-- Smoke Detection -- Fire extinguisher -- Power, air conditioning
SDLC CONTROL	-- Controls relating to planning, design, development, testing etc	

FUNCTIONAL NATURE

TYPE OF CONTROL	CHARACTERISTIC
INTERNAL ACCOUNTING CONTROLS	-- Controls relating to PHYSICAL SECURITY of the tangible IS resources & intangible resources.

caakhil24.srcc@gmail.com

OPERATIONAL CONTROLS	--**Deals with DAY TO DAY** operations, **functions & activities** to assure that operational activities **are contributing to the business objectives.**
ADMINISTRATIVE CONTROLS	-- **Concerned with ensuring EFFICIENCY & COMLIANCE with management policies.**

13) ORGANISATIONAL CONTROL:

- Enterprise control **concerned with DECISION MAKING** processes.
- Companies with **large data processing facilities at SEPERATE LOCATION** & combining it as **A SINGLE BUSINESS UNIT** is difficult process.
- **Organisational Control** technique includes **documentation of:**
  - Reporting responsibilities & authority of each function
  - Definition of responsibilities & objective of each function
  - Policies & Procedures
  - Job description
  - Segregation of duties

(i) RESPONSIBILITIES & OBJECTIVES:

A. Each IS function must be **clearly defined & documented.**

B. This includes **system software/development, application programming etc.**

C. Managers of each group is responsible for optimum utilisation of IS resources. These responsibilities includes:

- Providing information to senior management on IS resources.
- Planning for **expansion of IS resources.**
- Controlling the **use of IS resources.**
- Implementing activities & functions that support **accomplishment of the company's strategic plan.**

(ii) POLICIES, STANDARDS, PROCEDURE & PRACTICES:

A. These are **standards & instructions** that all **IS personnel** must follow **while performing their duties.**

B. Documented instructions **for filling out a standard changes request, justification of the cost of the changes** etc.

C. Documented policies should exist in **IS** for:

- Use of IS resources.
- Physical Security
- Data Security
- On-line security etc.

(iii) JOB DESCRIPTION:

A. These communicate management's specific expectation for job performance.

B. All jobs must have **a current, documented JOB DESCRIPTION** readily available to the employees.

C. Job description **establishes responsibilities & accountability** of the employee's actions.

(iv) SEGREGATION OF DUTY:

A. Common control technique **aimed at separating conflicting job duties.**

B. By such separation **work of one is checked** by the person.

C. Examples are:

- **IS Audit.**
- **Computer Hardware operations.**
- **System Analyst functions.**

14) MANAGEMENT CONTROL:

- Controls adopted by the management of an enterprise **are to ensure that information system function correctly.**
- Scope of control here includes **framing high level policies, procedures.**
- The control shall include:

- **Responsibility:** Senior management people responsible for IS within organisational structure.
- **Official IT structure:** There should be prescribed organisational structure with all knowing their responsibilities.
- **IT steering committee:** Comprise of user representative areas of the business & IT personnel.

15) FINANCIAL CONTROL TECHNIQUES:

CODE TO REMEMBER: A.B.$C^{2.}$D.^{2} – S.N.O.R.

A. AUTHORIZATION:

- This entails **obtaining the AUTHORITY** to perform some act.

B. BUDGET:

- This shows **THE AMOUNT OF TIME/MONEY** expected to be **SPENT** during a period.
- The budget has to be **COMPARED** with the actual performance to ascertain **deviation.**

C. CANCELLATION OF DOCUMENTS:

- This makes a documents **NOT READY FOR REUSE.`**
- Example: **Marks of "PAID OR OROCESSED"** on the invoices.

D. CONTROL (DUAL):

- This entails having **2 people** simultaneously access **ASSETS.**
- Example: **ATM** machines are emptied/filled with money **in presence of 2 people.**

E. DOCUMENTATION:

- This includes **WRITTEN OR TYPED** explanation of actions taken on **SPECIFIC TRANSACTIONS.**

F. DUTIES SEGREGATION:

- This entails **assigning SIMIALR FUNCTIONS** to separate people to provide reasonable **ASSURANCE** against **FRAUD.**

G. SAFEKEEPING:

- This entails **PHYSICALLY ASSETS,** such as **computer disks, desk drawer, file cabinet storeroom etc.**

H. NUMBERING DOCUMENTS:

- These are **working documents** with the **PRE-PRINTED** sequential numbers, **which helps in detection of MISSING DOCUMENTS.**

I. OUTPUT/INPUT VERIFICATION:

- This entails comparing **INFORMATION** provided by a **COMPUTER SYSTEM** to input documents.

J. REVIEW:

- This refers to **REVIEW DF SEPCIFIC WOTK BY A SUPERVISOR.**
- It requires a **MARK ON THE DOCUMENTS** depicting that supervisor has handled the documents at least once.

16) CONTROLS IN NUT SHELL:

I. Data processing Environment Controls:

-- These controls are **hardware & software** related.

II. Physical Access Control:

-- These controls are personnel; hardware & software related.

III. Logical Access Control:

-- These controls are **software related** & includes procedures exercised in IS software.

IV. SDLC controls:

-- Controls in SDLC involves **specifying activities that should occur in each system of SDLC**

V. Business Continuity Plan Controls:

-- These controls relate to have an **OPERATIONAL & TESTED IT** continuity plan.

-- These controls includes: **alternative procedures, backup, recovery plans etc.**

VI. Application control techniques:

-- These include **programmatic routines within the APPLICATION PROGRAM CODE.**

17) AUDIT TRAILS:

- **AUDIT TRAILS**: Are logs that can be designed to record activity at the **system, application & user levels.**

- Audit trails provide an **IMPORTANT DETECTIVE CONTROL** to accomplish **security policy objectives.**

- Accounting audit trail **shows the SOURCE & NATURE OF DATA & PROCESSES** that update the **DATABASE.**

- Following are audit trail objectives:

A. ***DECTECTING UNAUTHORISED ACCESS:***

-- Involves **real time detection.**

-- Objective is to **protect the system from outsider who is attempting to breach security controls.**

-- **REAL TIME AUDIT** is used to report on **changes in system performance** that in certain case may indicate any sort of **virus infestation.**

B. ***RECONSTRUCTION OF EVENTS:***

-- **Audit analysis** can be used **to reconstruct the steps** that led to **system failures, security violations** etc,

C. ***PERSONAL ACCOUNATBILITY:***

-- **Audit trail** can be used **to monitor user activity** at the lowest level of details.

-- **This** is rather **preventive control** that can be used to **influence behaviour.**

18) USERS CONTROL:

Some of the user controls are:

I. BOUNDARY CONTROL:

- Major controls of boundary system are **access control mechanism.**
- The access control **mechanism** involves **3 steps:**
  - Identification
  - Authentication
  - Authorisation
- User can provide **3 classes of input** information for authentication process & gain access control to his required resources.

CLASS OF INFORMATION	TYPES OF INPUTS
Personal Information	Name, birth, account number, PIN
Personal Characteristic	Fingerprint, hand size, signature
Personal Objects	Identification cards, key, badge

CYRPTOGRAPHY

- Deals with the **programs** for **transforming DATA into CODES.**
- *CYRPTOGRAPHIC TECHNIQUE :*

  ENCRYPTS

  a. **Data {Clear Text}** into **cryptograms {Cipher Text}**

  b. **Factors:** Time & cost involved in **DECIPHER** the cipher text by **CRYPT-ANLAYST.**

PASSWORD

- Passwords **can be used as** BOUNDRAY ACCESS CONTROLS.
- User can easily protect their information by using passwords.
- Following things to be kept in mind: **frequent changes in password, minimum password length** etc.

PERSONAL IDENTIFICATION NUMBER [PIN]

- Passwords **can also be used as** BOUNDRAY ACCESS CONTROLS.
- This number is provided to a user **by an institution based on USER CHARECTERISTICS.**
- However PIN is exposed to certain vulnerabilities while **issuance, delivery, transmission, storage** etc.

IDENTIFICATION CARDS

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

II. INPUT CONTROL:

- Are responsible for **ensuring & completeness of the data & instructions** input into an **application system.**
- Controls are being implemented on **INPUT** since **HUMAN INTERVENTION** is required involving **considerable time, as such prone TO ERROR & FRAUDS.**
- **Data CODES** are used to **give unique identity.**
- Auditor must verify **the QUALITY of CODING SYSTEM** & analysing the impact on **integrity & accurateness of data.**

III. PROCESSING CONTROL:

- Data processing control **perform VALIDATION CHECK** to identify errors during **processing of data.**
- Ensure **completeness & accuracy** of the data being processed.
- Processing controls are enforced **through DATABASE MANAGEMENT SYSTEM.**

☯ Some of the data processing controls: **CODE TO REMEMBER: R. - V.E.E.R.**

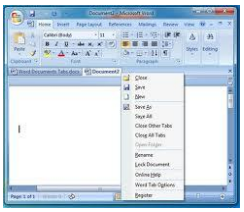
1. **R**UN-TO-RUN TOTALS:
   - This help in **verifying data** that goes through **different stages.**
   - A specific record can be used **to maintain control total.** For example **invoice amount** ₹ **1,50,000.00** & additional invoice is of **20,000.00**, then total sales value will be OF ₹ **1,70,000.00.**
2. **V**ERIFICATION:
   - 2 or more **fields** can be compared & cross verified **to ensure their correctness.**
   - For example, **statutory % of provident fund** can be calculated on the **gross pay** to verify the deduction is accurate.
3. **E**DIT CHECKS:
   - It is similar to **data validation controls** can be used **at the time of processing stage** to verify **accuracy & completeness of DATA.**
4. **E**XCEPTION REPORTS:
   - This are **generated to IDENTIFY ERRORS** in data processed.
   - Such report helps in ascertaining **that why a particular transaction** is not processed **or** what is the **error in PROCESSING THE TRANSACTIONS.**
5. **R**ECOVERY CONTROLS:
   - Recovery controls **enables a system to be recovered if FAILURE** is **TEMPROARY AND LOCALISED.**

IV. OUTPUT CONTROL:

☯ Ensure that the **data delivered to users will be PRESENTED,FORMATTED** and **DELIVERED** in a consistent and secured manner.

☯ Output can be in any form:

PRINTED DATA REPORT



WORD DOCUMENT

FLOPPY DISK OR CD-ROM

☯ Some of the output controls:

CODE TO REMEMBER: M.R.S. - .E.P.S.

1. MONITORING OF OUTPUT PROGRAM EXECUTION:

- When program are executed for **OUTPUT OF DATA,** it should be logged & monitored.
- Without such control, **CONFIDENTIALITY** will be at stake.

2. RETENTION CONTROL:

- It considers the **DURATION FOR WHICH** output should be retained before destroying.
- **RETENTION PERIOD** depends on following factors:
  - ✠ **Need of the output.**
  - ✠ **Use of the output.**
  - ✠ **Legislative Requirement.**

3. STORAGE & LOGGONG OF CRITICAL FORMS:

- Pre printed **stationery** should be **STORED** securely to ,
- Prevent **UNAUTHORISED DESTRUCTION / REMOVAL & USAGE.**

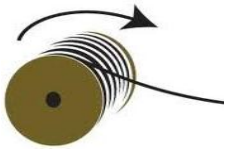
4. EXISTENCE CONTROL:

- This control needed to **RECOVER OUTPUT** in the event that is LOST
- If output is **written to a SPOOL/FILES** has been kept, then **recovery & new generation is EASY & STRAIGHT FORWARD.**

5. PRINTING CONTROL:

- It should be **ENSURED** that **unauthorised disclosure of INFORMATION** printed is **PREVENTED.**
- Restriction must be placed **on the workstation** that is used or printing.

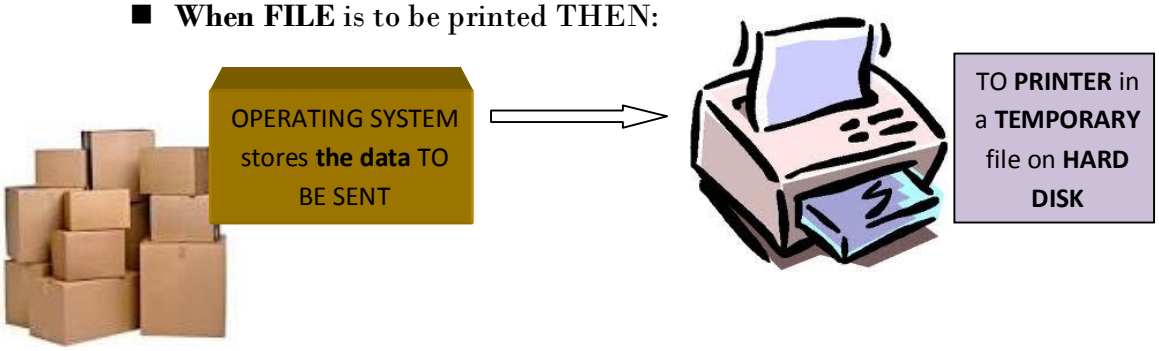
6. SPOOLING/QUEUING:



"SPOOL"

"Simultaneous Peripherals Operations Online"

- This is used **to ensure that USER IS ABLE TO** work continuously,
- Even before **the print operation is COMPLETED.**
- **When FILE** is to be printed THEN:



- Then this file is **sent to printer as soon as PRINTER** is ready to accept the data.

V. DATABASE CONTROL:

☯ Protecting the **INTEGRITY OF A DATABASE,** when application software act as an **INTERFACE** between **the USERS & DATABASE** are called:

UPDATE CONTROLS REPORT CONTROLS

☯ Some of the UPDATE CONTROLS:

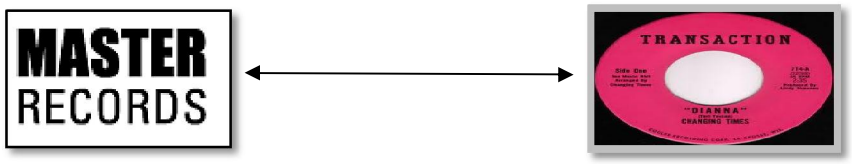
CODE TO REMEMBER: P.M. - C.P.

Prime **M**inister in **C**onnaught **P**lace

1. Processing of records:

- While processing TRANSACTION file records mapped to respective MASTER FILES, end-of-file of transaction files with respect to end-of-file master file **IS TO ENSURED.** It simply means that all files are processed.

2. Maintain a suspense Account:

- 

When there is mismatch between the MASTER RECORD & TRANSACTION RECORDS due to **failure in the corresponding RECORD ENTRY,** then these **transactions** are **MAINTAINED** in a suspense account.

3. Checking of transactions & master files:

- To maintain INTEGRITY, INSERTION OR DELETION **of records in the master file, as such**
- There must Be SYNCHRONIZATION of processing BETWEEN MASTER AND TRANSACTION FILES.

4. Process multiple transactions for single record:

- Multiple transactions can **occur based on SINGLE MASTER RECORD**
- For instance, **DISPATCH REPORT** of product to **VARIOUS CENTRES.**

☯Some of the REPORT CONTROLS:

CODE TO REMEMBER: P - E.P.S.

1. Print Run-to-Run control totals:

- Run-to –run control helps in **identi**fying errors or irregularities.

2. Existence Controls:

- Backup & recovery **strategies encompass CONTROLS required to RESTORE** *FAILURE* in a database.
- Recovery strategies involves:

ROLL FORWARD: Current state database form previous version

ROLL BACK: Previous state database form current version

3. Print suspense Account entries:

- The suspense entries are to be **periodically monitored with the respective ERROR FILES** & action taken on time.

4. Standing Data:

- Application program uses **many internal tables i.e.** GROSS PAY CALCULATION, BANK INTEREST **etc.**
- **Any changes in THESE TABLES** may adversely affect on **organisation basic functions.**
- **So there should be PROPER MONITORING** of internal tables.

19) SYSTEM DEVELOPMENT & ACQUISTION CONTROL:

*To effectively govern the **development, acquisition, implementation & maintenance** of Information system, it is **rather imperative** to have **formal, time tested** proven methodologies.*

Methodology** should contain **appropriate** controls **for:

- ❑ Management Reviews & approval,
- ❑ User Involvement,
- ❑ Analysis, design, testing, implementation & conversion.
- ❑ Methodologies should enable the management to **trace the source of the input till their destination.**

CONTROLS OVER THE SYSTEM DEVELOPMENT PHASES & AUDITOR'S ROLE

A. SDLC **defines the agenda that stakeholders** (*management, users, programmers)* **must address**

B. Quality of the system that to be developed **depends on** how well the **stakeholders grip**(catch up) **with these issues.**

To have effective control over the system development, there is imperative need to start from scratch i.e. from beginning. It involves the following steps:

1. PROBLEM DEFINITION:

- In this phase, **stakeholders make attempt to understand the nature of problem.**
- **Information system requirement** can be conceived **through a FORMAL PROCESS** system planning.

CONTROLS

- Need for information system in preview of business requirement.
- Support & priority for information system.
- Level of acceptance for change among stakeholders.
- Investigation & strategy by which need for system is justified.

AUDITOR'S ROLE

- Whether STAKEHOLDERS have reached agreement on problems.
- Understanding of threats to ASSET safeguarding, data integrity etc.

2. MANAGEMENT OF THE CHANGE PROCESS :

- Management of the change **process RUNS parallel** to all **SDLC** phases.

CONTROLS

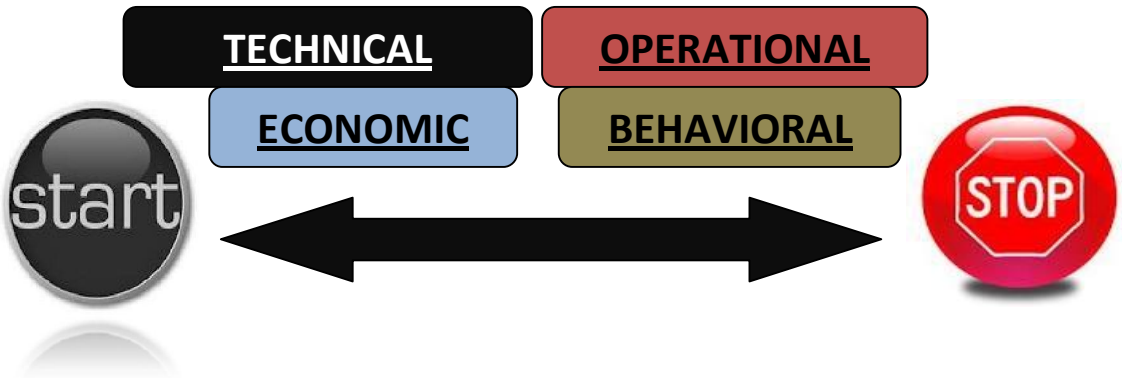
- Involves addressing matters **such as budgeting, reporting, checkpoints, decision making etc.**
- Preparing organisation **for unrestricted changes** by **training, feedback etc.**
- **Complete CHANGEOVER** to the new system.
- Help users **to adapt to their NEW ROLES** by providing positive feedback.

AUDITOR'S ROLE

- To evaluate quality of decision making.
- If the new system **is SMALL,** then change management can be done **IN-HOUSE** with less material concerns.
- If the new system **is LARGE,** then it will have **high level of requirement & TECHNOLOGOICAL** uncertainty.

3. ENTRY & FEASIBILTY ASSESSMENT:

- The specific technique used to evaluate the feasibility of systems.



SYSTEM DEVELOPMENT PROCESS

CONTROLS

- **TECHNICAL:** Can technology be acquired, developed to support **proposed** project.
- **OPERATIONAL:** Can system be designed **to process inputs & give required output.**
- **ECONOMIC:** The proposed system is **deemed feasible** if **BENEFIT > COST.**
- **BEHAVIORAL:** Can system improve **the quality of work life.**

AUDITOR'S ROLE

- Behavioral impact on the users that arise in **new system.**
- Material loss **incurred as a result of** development, implementation, operations or maintenance of system.

4. ANALYSIS OF EXISTING SYSTEM:

- Before designing a system, **it is imperative to UNDERSTAND** the existing system.
- The analysis includes:
  - **Study of existing organisational history, structure & culture.**
  - **Study of existing information flows.**

CONTROLS

- Study of history of system in organisation gives idea of:
  - ✓ Types of useful systems.
  - ✓ Issues that are remained unaddressed over a period of time.
- Study of existing information is done **through formal methodologies.**
- These methodologies include **structured analysis, prototyping and agile models.**

caakhil24.srcc@gmail.com

AUDITOR'S ROLE

- Need to study **aspects of present organisational structure.**
- Evaluating the **quality of methodologies** used.
- Usage of **high quality** tools in analysis.

5. SYSTEN DESIGN:

- **SRS** (System Requirement Specification) **document identifies the deficiencies** in the existing system.

CONTROLS

- Align business requirement with the **management's objectives, user's goal.**

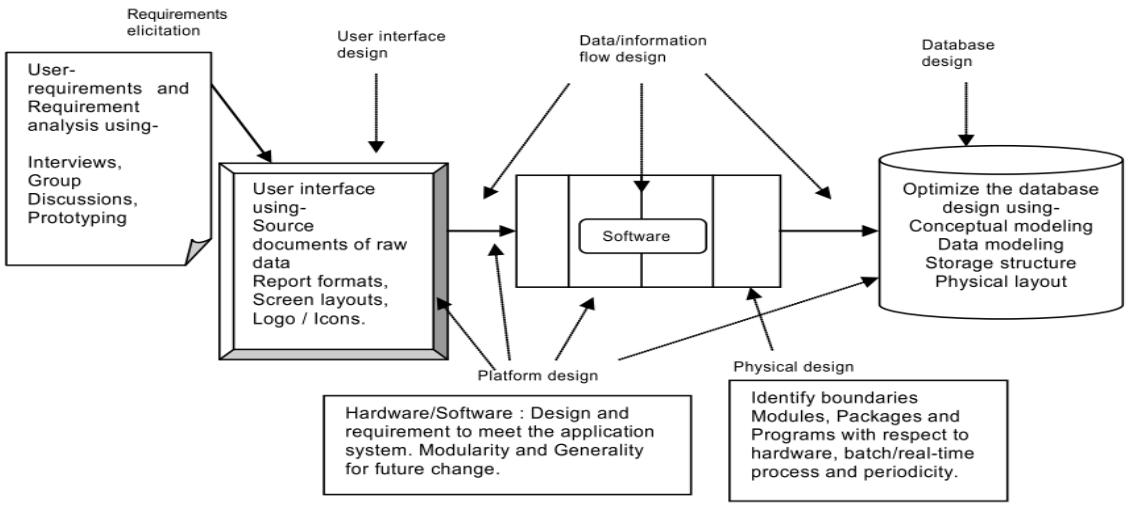
AUDITOR'S ROLE

CODE TO REMEMBER: **F.B.S**

- **F**easibility of the **system –designed proposed.**
- To assess **B**ehavioral **impact on the USERS** within the proposed system.
- Evaluate quality of **S**RS **design work.**

6. ORGANIATIONAL & JOB DESIGN:

- Reliability of the controls designed into system **are evaluated to MEET STRATEGIC** requirements of the proposed system.



caakhil24.srcc@gmail.com

AUDITOR'S ROLE

CODE TO REMEMBER: **D.A.C.U**

- **D**atabase structure & cost of the data model is to be evaluated.
- **A**ppropriateness of the requirement strategies in the scope of **stakeholder.**
- **C**apturing of all the data/information flow **by the SYSTEM DESIGN.**
- **U**ser interface designing quality to be developed by following **best design practices.**

7. INFORMATION PROCESSING SYSTENS DESIGN:

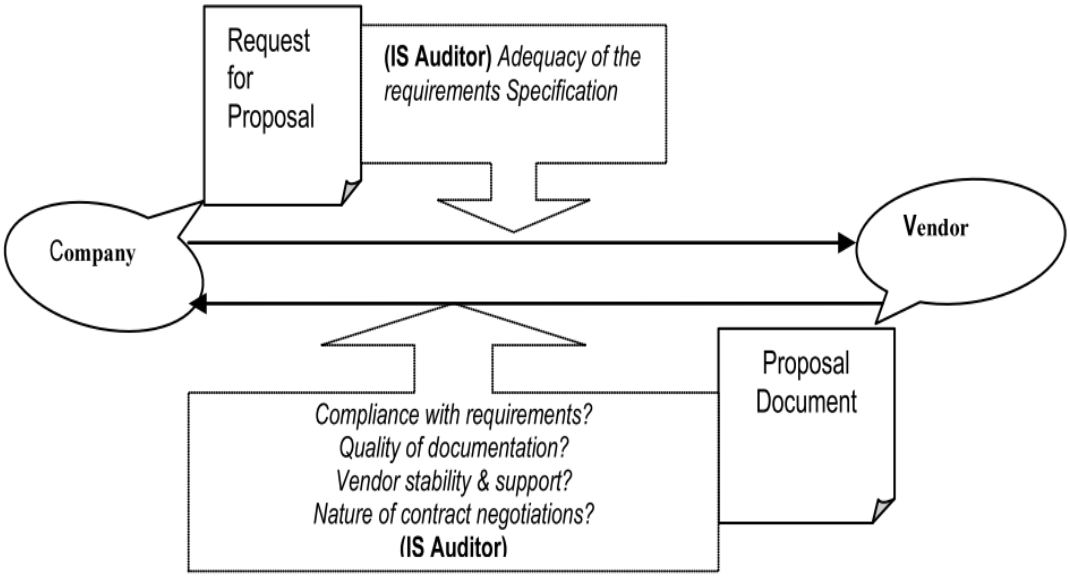
- Once information flow & processing within a **system is IDENTIFIED & DESIGNED,** application software may be **ACQUIRED OR IN-HOUSE.**

CONTROLS

CODE TO REMEMBER: **V.-M.R.F.**

- **V**endor evaluation process consider the following:
  - ✓ **C**ost benefits of the hardware / software.
  - ✓ **M**odifications of the **application software.**
  - ✓ **S**tability of the supplier company.
  - ✓ **S**upplier's ability to provide support.

  CODE TO REMEMBER: **C.M.S^2**
- **M**eeting of the business & system goals by the **INFORMATION & SYTEM REQUIREMENTS.**
- Detailed **R**equest for Proposal (RFP), documents needs to specify the ACCEPTABLE **requirements.**
- **F**easibility analysis **to define The CONSTRAINTS** foe each alternative system.



AUDITOR'S ROLE

CODE TO REMEMBER:**R.C.-D.I.L.**

- **R**isk highlighting by the auditor before CONTRACT is signed.
- **C**riteria for PRE-QUALIFICATION of vendors & sufficient documentation available to justify final selection of vendor.
- Ensure that **D**ecision to acquire software has undergone thorough **FEASIBILITY STUDY, VENDOR EVALUATION** etc.
- **I**nformation collection by the auditor through his **own source on VENDOR VIABILITY, SERVICE RECORDS** etc.
- **L**egal scrutiny of the contract before it was signed.

CONTROLS OVER SYSTEM & PROGRAM CHANGES

1. MANAGEMENT OF THE CHANGE PROCESS :

- Management of the change **process RUNS parallel** to all **SDLC** phases.
- For complex components of the system, **needs WELL DEFINED, TESTED, PLANNED, CORDINATED change management.**

Change process involves the following tasks:

- Provide **feedback** to the system stakeholders.
- Prevent system **disruption** which may result in **business loss**
- **Accepted CHANGEOVER** to the new system.
- Help users **to adapt to their NEW ROLES.**
- Documentation & Follow up of **recommended process changes.**

2. SYSTEM CHANGE CONTROL :

Involves addressing matters ***such as budgeting, reporting, checkpoints, decision making etc.***

Change-facilitation deals with the following activities:

- Preparing organisation **for unrestricted changes** by **training, feedback etc.**
- **Complete CHANGEOVER** to the new system.
- Help users **to adapt to their NEW ROLES** by providing positive feedback.

AUDITOR'S ROLE

CODE TO REMEMBER:**R.C.-D.I.L.**

- To evaluate quality of decision making.
- If the new system **is SMALL,** then change management can be done **IN-HOUSE** with less material concerns.
- If the new system **is LARGE,** then it will have **high level of requirement & TECHNOLOGOICAL** uncertainty.

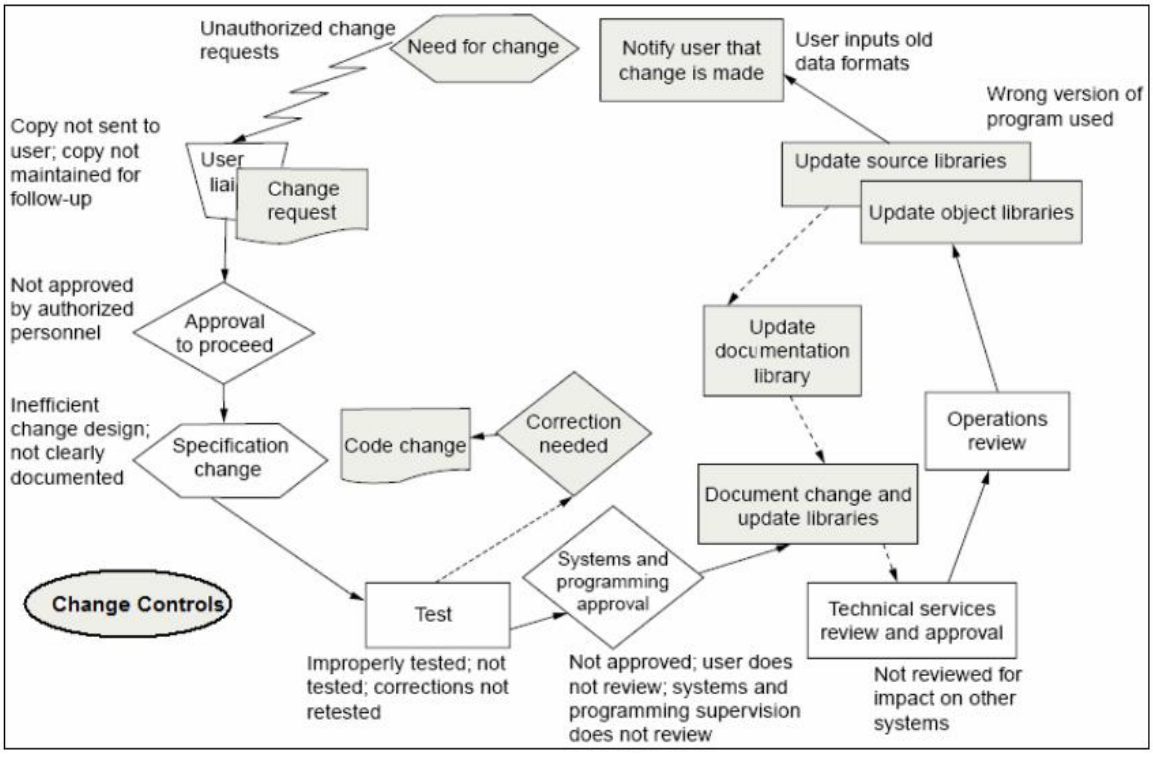
CHANGE CONTROL aims at **addressing the problems** which are not detected during the **system design or testing. The RISKS** the change control processes **deals with:**

CODE TO REMEMBER: **F.R.A.U.D.**

A. **F**ailure of system due to **errors, omissions etc.**
B. **R**epeated Errors.
C. **A**buse to company system or data.
D. **U**nauthorised Changes
E. **D**ata loss due to **errors, omissions etc.**

3. PROGRAM CHANGE CONTROL:

- Application software programs are **designed to support specific business operation.**
- It ensures that **only authorised programs & modifications** are implemented.
- Standardised policies & procedures **ensure** that all programs & their modifications are **properly authorised, tested & approved.**



caakhil24.srcc@gmail.com

AUDITOR'S ROLE

CODE TO REMEMBER: **B.U.T. - F.M.**

- **B**ackups of the system's data and programs.
- **U**pdated technology inventory of all hardware, software & services.
- **T**acking of program changes are to be accounted.
- **F**ormal handover process so that authorised person is involved in the **software testing & updation processes.**
- **M**aintenance of software program code libraries.

4. AUTHORISATION CONTROL:

AUTHORISATION CONTROL ensures all **information & data is authorised by MANAGEMENT.**

AUDITOR'S ROLE

CODE TO REMEMBER: **R.I.T.A.**

- **R**esponsibilities assignment & authorisation to those involved in the change & monitor their work.
- **I**dentification **BYEPASSES** of data validation & edit checks.
- **T**acking of program changes are to be accounted.
- **A**uthorised modifications should be there in case of manual authorisation is there.

5. DOCUMENT CONTROL:

- Need for **recording all REQUESTS FOR CHANGE (RFC).**
- Request for changes in **both HARDWARE & SOFTWARE** resources of the system **to be LOGGED.**

DOCUMENTATION CONTAINS DESCRIPTION OF **hardware, software, policies, standards, procedures.** A user instruction **manual document** defines **responsibilities & actions:**

A.

INPUTS CONTROLS THAT IDENTIFY ALL DATA ENTERING THE PROCESSING CYCLE

PROCESSING CONTROLS INFORMATION THAT INCLUDES EDITS, ERROR, AUDIT TRIALS ETC

OUTPUT CONTROLS THAT DEFINES HOW TO VERIFY THE CORRECTNESS OF THE REPORTS

B.

1. Narrative description of the system.
2. Detailed flowchart of all processes.
3. Detailed document flowchart.
4. A list of approvals required on each **INPUT DOCUMENTS**.
5. A COPY of each report produced by the system with description of its purpose.
6. A system recovery section.

AUDITOR'S ROLE

CODE TO REMEMBER: **T.P. - I - P.O.D.**

Test **P**erformance of **I-POD**

*Assessing documentation involves **evaluating the changes**. To **understand** document flow, certain background information has to be obtained. The **AUDITOR** need to obtain the following documents:*

1. **T**itle of the computer product.
2. **P**urpose of the product system name & identification number.
3. **I**mplementation date of the system.
4. **P**rocessing type & frequency.
5. **O**rigin point of all each source document.
6. **D**estination of each copy of the source document & action applied to each copy. **[action = filed + audited + entered in computer]**

6. TESTING CONTROL:

- In this phase, **design & specifications** should be subject to **quality review.**
- **& c**ontinues **during the SYSTEM DEVELOPMENT & acceptance testing** phases of SDLC.

PURPOSE OF TESTING: Computer system s are tested to prove that **system perform up to users satisfaction.**

PERSONNEL INVOLVED: Includes **DEVELOPERS, OPERATION STAFF, END UESR, AUDITORS, SYSTEM ADMINISTRATORS, SECURITY PERSONNEL**

OBJECTIVE OF TESTING: Ensure that **DELIVERED SYSTEM** is of adequate quality.

DURING TESTING PHASE:

- **System is tested to verify that IT WORKS AS INTENDED.**
- **Meets DESIGN SPECIFICATIONS.**

About the system

- **Overall strategy should be developed to define:**
  - Individual test events.
  - Roles & responsibilities.
  - Test Environment.
  - Problem reporting & tracking.

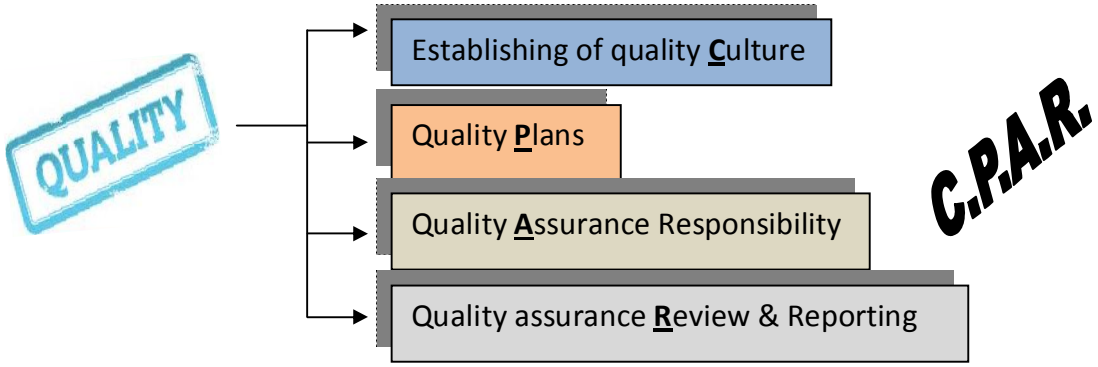
- **REGRESSION TESTING:** It is process whereby system is RE-TESTED to ensure that changes have not introduced any other problem.

7. QUALITY CONTROL:

- It is the process **THAT IMPACTS** the **EFFECTIVENESS, INTEGRITY & AVAILABILITY OF INFORMATION SYSTEM.**

- It describes the **controls over the IT process** of managing quality meeting the business requirements.

- **Quality control encompasses the following:**



caakhil24.srcc@gmail.com

System Development Life Cycle Methodologies

Development of a **quality Knowledge Base**

QUALITY STANDARDS:

(i) CMII: Capability Maturity Model Integration.

- Is a framework for organizing & accessing maturity level of IT processes for software development.

(ii) 9000 Quality management & Quality Assurance Standard(ISO):

- Defines quality control as "OPERATIONAL TECHNIQUES & ACTVITIES THAT ARE USED TO FULFIL QUALITY REQUIREMENT."

QUALITY REVIEW:

Quality review covers **NON-COMPUTER TESTING ACTIVITIES.**

I AM NOT EXPLAINING THE FOLLOWING POINTS:

1. **Auditor's role**
2. **Copyright Violation**
3. **Contracts & Warranties**
4. **Service Level agreements**

CONTROLS OVER SYSTEM IMPLEMENTATION

Final steps to implement the system include CONVERSION, DOCUMENTATION, and TRAINING & SUPPORT.

Following are the activities involved during the IMPLEMENTATION STAGE:

A. PROCEDURE DEVELOPMENT:

- Covers **WHO, WHAT, WHEN, WHERE & HOW** i.e.
- Of the **IMPLEMETATION PROCESS.**
- Design of the procedures **must match the JOB RESPONSIBILITY** of users.

Auditor is to assess following in designing phase documentation:

- Quality of procedure design as per **SRS specifications of system.**
- Change Management Policies **are implemented & followed.**
- Approach followed in **TESTING & IMPLEMENTATION of change**
- **Quality of procedure DOCUMENTATION, SYSTEM MANUALS** etc.

Conversion activities

CODE TO REMEMBER: **P.C. - M.E.E.**

1. **P**rocedures for correcting & converting data into new application.
2. **C**leansing of the data before conversion.
3. **M**ethods to access the ACCURACY of conversion.
4. **E**xception report designing showing the UNCONVERTED DATA.
5. **E**stablishing responsibility for verifying & signing off & overall conversion by the SYSTEM OWNER.

AUDITOR'S ROLE

- Has DATA CONVERSION PLAN been drawn up?
- Does the Data conversion Plan:

CODE TO REMEMBER: **A - B.A.S.I.C.S.**

--**A**llocate staff to each task & defining roles & responsibilities.

--**B**ackup & recovery procedures to be defined **for converted data on NEW system**

--**A**udit trail preservation after the conversion.

--**S**eparation of roles between **who TRANSFER DATA & VERIFY IT.**

-- **I**nbuilt software if any, **that has been developed to support DATA conversion task**

--**C**riteria defined or not for **IDENTIFYING & RESOLVING** problems on quality of the existing data.

--**S**trategy of data conversion has been described or not.

B. USER FINAL ACCEPTANCE TESTING:

- It is perfumed in a **secured environment,**
- Where **both SOURCE & EXECUTABLE** codes are **PROTECTED.**
- It means any change to the system will not take place **until it goes through STANDARD SYSTEM MAINTENANCE PROCESS.**
- **ACCEPTANCE TESTING** to be undertaken by:

SUPPORTED BY



USERS | IT STAFF | EXPERT CONSULTANT

ACCEPTANCE TEST PLAN INCLUDES:

- PERFORMANCE TESTING
- VOULME TESTING
- STRESS TESTING
- SECURITY TESTING
- BACK UP & RECOVERY
- CLERICAL PROCEDURES CHECKING

AUDITOR'S ROLE

The auditor has to ensure that both DEVELOPERS & USERS have thoroughly tested the system to ENSURE that it:

CODE TO REMEMBER: **B.C.A. - N.E.A.T.**

-- **B**uilt in controls **possessed by system** to provide r**easonable** assurance of **proper operation.**

-- **C**orrective action taken by the management if **level of testing doesn't meet the required standards.**

-- **A**llocate adequate resources in **terms of manpower, time & equipment.**

-- **N**eed of the **users & management is fulfilled.**

-- **E**nd user involvement in the **design & execution of acceptance testing programme.**

-- **A**dequate **audit trail** of changes maintained.

-- **T**est plan (Acceptance) covers all the aspects of the **user requirements specifications**

C. USER TRAINING:

- User training is critical for the **efficient & effective IMPLEMENTATION** of a system.

- It involves the following training:

MANAGERS TRAINING

Manager's training **an overview & application system.**

USERS TRAINING

Involves how to **use software, enter the DATA,** generates output

CONTROLS OVER SYSTEM MAINTENANCE

Maintenance of the system can be undertaken under **THREE** categories:

- Corrective maintenance
- Adaptive maintenance
- Perfective maintenance

AUDITOR'S ROLE

The auditor has to evaluate the EFFECTIVENESS & EFFICIENCY of the system maintenance processes:

CODE TO REMEMBER: **R.T.D. - P.M.T.**

Re**T**ire**D** **PMT** teacher need maintenance

-- **R**atio of **actual maintenance cost PER APPLICATION.**

-- **T**ime to deliver **change request.**

-- **D**ivergence instance from the **standard procedures.**

-- **P**roduction problems **per application & respective maintenance charges.**

-- **M**odules which **are returned to development due to ERRORS discovered.**

-- **T**ime **elapsed to ANALYZE & FIX PROBLEMS.**

2. PERFORMANCE MEASUREMENT:

Performance measurement is **dependent on the business strategy & objectives of the management.** The factors for measurement involve:

- Value delivered by the IT system,
- Ratio to the cost to IT to the per unit business function.
- Responsive time of the system for a new change.
- Ongoing **cost of the system** to maintain its effectiveness.

Performance measurement includes:

- **THROUGHPUT :** Output per unit of time
- **UTILIZATION :** **P**ercentage of time the system is being used productivity

POST IMPLEMENTATION REVIEW

PIR *is done to determine if the* ***ANTICIPATED BENEFITS*** *are achieved. PIR helps in:*

- Controlling project development activities.
- Encourages accurate **INITIAL COST & BENEFITS.**

A. PIR *is done in order to meet the following objectives:*

1. Business objectives : **Delivered within**


WITHIN BUDGETS & DEADLINE

2. User expectations :
   - Good Response Time
   - Required Output produced
   - User Friendly
   - Reliable

CODE TO REMEMBER
T.O.U.R.

3. Technical requirements:
   - Capable of expansion
   - Operate easily
   - Interface with other system
   - Low running cost

CODE TO REMEMBER
C.O.I.L.

B. PIR team:

***PIR** team consists of the following:*

Other **external support to assist in:**

1. Evaluating delivery of technical &
2. Specialised Functions

C. PIR team activities:

***PIR** team should undertake the following activities. Review of:*

CODE TO REMEMBER: **F. - C.O.D.E.**

1. **F**unctionality of the **operational system.**
2. **C**hanges to requirement, their need, authorisation in accordance with the **change & configuration management standards.**
3. **O**peration & performance of the system.
4. **D**evelopment Techniques & methodologies employed.
5. **E**stimated time scales & budgets & identify reasons for **variation.**

AUDITOR'S ROLE

Following issues are to be considered while judging the EFFECTIVENESS of the PIR.

The auditor must INTERVIEW OR REVIEW:

caakhil24.srcc@gmail.com

■ BUSINESS USERS:

- ❖ Interview business users in,
- ❖ Each **functional areas covered by the system.**
- ❖ & assess their **satisfaction with the system.**

■ SECURITY:

- ❖ Interview security, operations, maintenance staff,
- ❖ In respect of their responsibilities.

■ USERS REQUIREMENT SPECIFICATIONS:

- ❖ Determine whether **system's requirements** have been met or not.
- ❖ Identify the **reasons for not providing the requirement on time.**

■ SYSTEM PROBLEM REPORTS:

- ❖ Review **system problem report, & change proposals** to establish the nature of problems.

■ INTERNAL CONTROL SYSTEM:

- ❖ **Confirm** that **adequate INTERNAL CONTROL has been built into the system & they are operated correctly.**

CONTROL OVER DATA INTEGRITY, PRIVACY & SECURITY

INFORMATION CLASSIFICATION

Classification of information has been already mentioned in chapter-5. I am hereby just giving a glimpse of the names:

- TOP SECRET
- HIGHLY CONFIDENTIAL
- PROPRIETARY
- INTERNAL USE
- PUBLIC DOCUMENTS.

DATA INTEGRITY

Data integrity control techniques **aim to PREVENT, DETECT & CORRECT ERRORS** in transactions as they flow through **various stages of data processing program.**

Analysing data integrity involves evaluating the critical procedures:

1. VIRUS detection & elimination.
2. Data integrity controls ensures that information has not been altered.

DATA INTEGRITY

Reflects **accuracy, correctness, validity & currency of the data**

There are 6 categories of data integrity controls:

CONTROL CATEGORY	THREATS/ RISKS	CONTROLS
SOURCE DATA CONTROL 	-- Invalid Data -- Incomplete data input	D-VAN -- Forms Design. -- Check digit Verification -- Authorisation Review -- Sequentially Numbered documents.
INPUT VALIDATION ROUTINES 	--Invalid or inaccurate data in computer – processed transaction files	-- Identifying the errors & correcting them. -- Such checking on timely basis. -- Prepare SUMMARY ERROR REPORT.
ON-LINE DATA ENTRY CONTROLS 	--Invalid or inaccurate transaction input entered through ONLINE terminals	--User ID's & passwords --Compatibility tests --Transaction Log maintained by the system
DATA PROCESSING & STORAGE CONTROLS 	--Incomplete or inaccurate data in computer – processed master files	--Policies & procedures in respect of : D-AUS - Data security - Audit Trails - Use of file labels - Storage personnel

OUTPUT CONTROL	-- **Incomplete/inaccurate computer output**	--**Procedures to ensure:** - That system outputs conform to organisation's integrity. - Proper **distribution** of the **output**. - Protection of **confidential information**.
DATA TRANSMISSION CONTROL	-- **Unauthorised access to data transmitted**	--**Monitor network to:** - Detect week points. - Backup components. - Multiple communication paths between networks

DATA INTEGRITY POLICIES

CODE TO REMEMBER: **V.D.** - **B.O.S.E.**

1. VIRUS SIGNATURE SOFTWARE:

- It must be updated immediately,
- When they are available from the vendor.

2. DISASTER RECOVERY:

- Comprehensive **disaster recovery plan** must be,
- Used to ensure **continuity of business.**

3. BACKUP:

- **Quarter or year end backup** must be done separately,
- From the normal schedule for **accounting purpose.**

4. OFFSITE BACKUP:

- Backup Older than **1 month** must be sent **offsite** for permanent storage.

5. SOFTWARE TESTING:

- All software must be tested in a,
- **Suitable environment** before **installation** on production system.

6. ENVIRONMENT DIVISION:

- Division of **environment into DEVELOPMENT, TEST & PRODUCTION** is required for critical systems.

SECURITY CONCEPT & TECHNIQUES

Following are the security techniques:

A. CRYPTOSYTEM:

- Refers to **SUITE OF ALGORITHM** needed to implement particular form of **encryption & decryption.**

- It consists of 3 algorithms:
  1 – Key generation
  2 – Encryption
  3 – Decryption

CIPHER is often used to refer a **PAIR OF ALGORITHM**

B. DATA ENCRYPTION STANDARDS:

- It is **mathematical algorithm** for **encrypting** (enciphering) & **decrypting** (deciphering) **binary coded information.**

- ENCRYPTING → **Converts data into an UNINTELLIGIBLE FORM**

- DECRYPTING → **Converts data back into its ORIGINAL FORM**

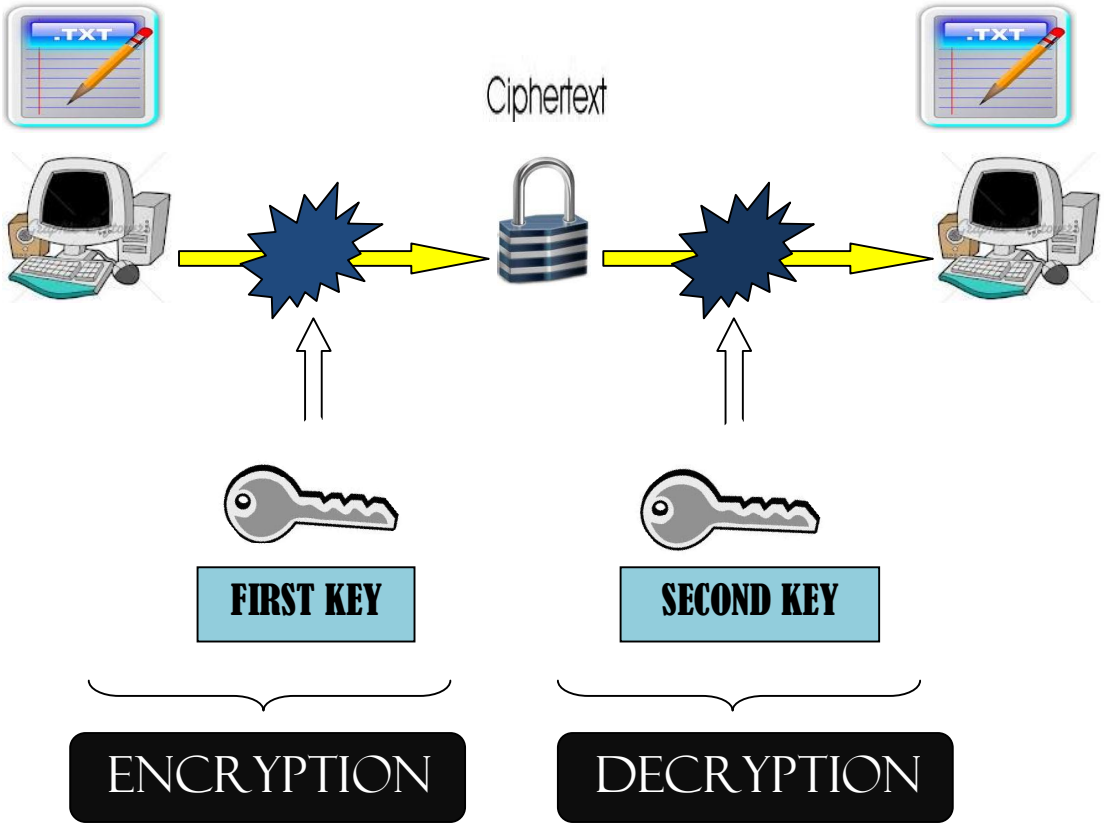
caakhil24.srcc@gmail.com

C. PUBLIC KEY INFRASRTUCTURE:

- PKI can provide **for authentication,** data integrity, **system software, policies, procedures & standards.**
- This system is based on **public key cryptography** in which user has a key **pair –**

A unique electronic value → PUBLIC KEY

A mathematically related → PRIVATE KEY



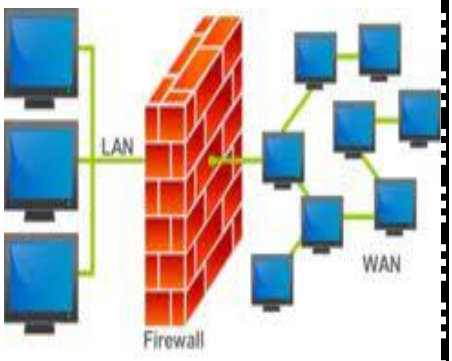
caakhil24.srcc@gmail.com

DATA SECURITY & PUBLIC NETWORK

One of the major considerations for an organisation in respect of networking system is **"How to provide a LOW COST, SECURE ELECTRONIC NETWORK"**.

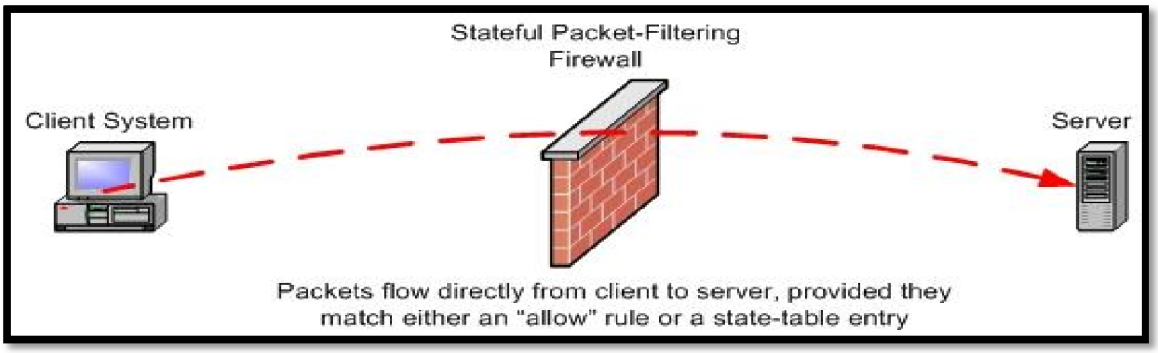
Solution to this problem is "VIRTUAL PRIVATE NETWORK". **Here "tunnels" are created over the** regular internet lines-connections" **that can be easily used by anyone at lower cost.**

A. FIREWALLS:



- **It is collection of components i.e. computer, routers, software.**
- That **mediates** access between **different security domains.**
- 4 types of firewalls:

PACKET FILTER FIREWALLS



- It evaluates **the headers of each** incoming & Outgoing packets,
- **To ensure that it has VALID INTERNAL ADDRESS,** originated from a **permitted external address CONNECTS** to authorised protocol.

caakhil24.srcc@gmail.com

- **If the PACKET** doesn't match **with the PRE-DETERMINED** policy for allowed traffic, than the **firewall** will **DROP THE PACKET.**

- **PACKET FILTER** don't analyse the content of the packets.

- ***Here are some of the weakness in packet filter firewall:***

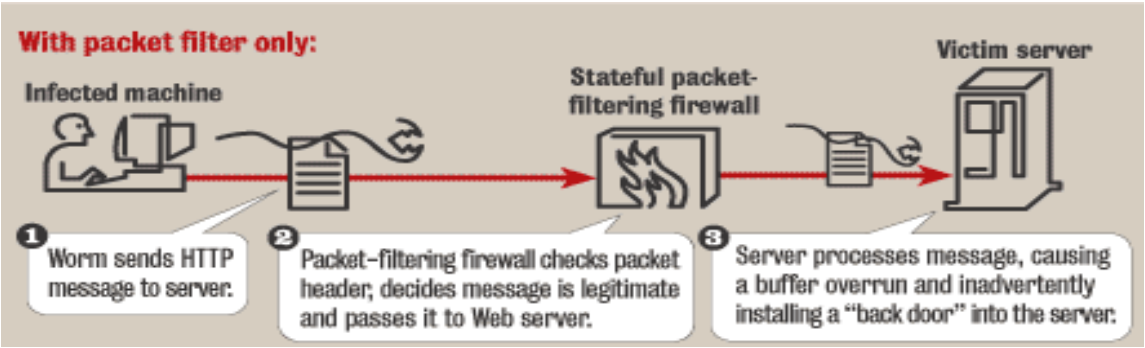
Unable to prevent attack that exploits application-specific vulnerabilities because of non-EXAMINING **of** contents of packets.

It doesn't support ADVANCED UERS AUTHENTICATIONSCHEME.

Firewalls are generally vulnerable to ATTACKS & EXPLOITATION.

Firewalls are easy to MISCONFIGURE.

STATEFULL INSPECTION FIREWALLS

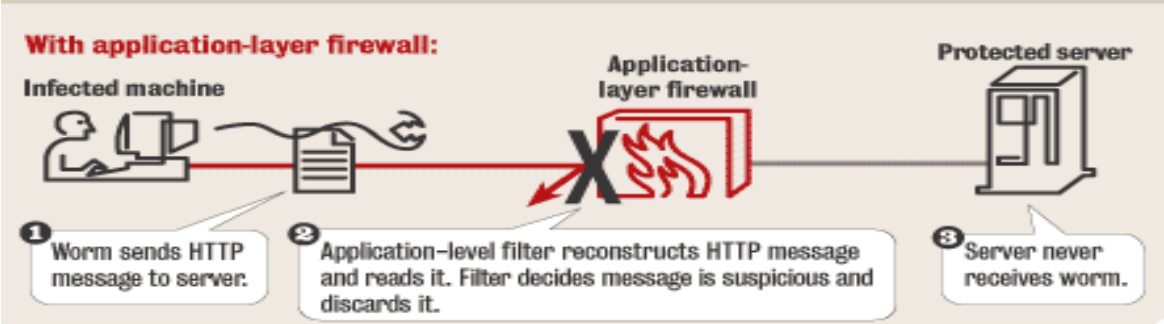


- **These are packet filter that** MONITOR **that state of TCP connection.**
- When a connection is **established the FIREWALL** adds connection **information to the table.**
- The firewall can refer to **this connection in future.**

PROXY SERVER FIREWALLS

- **Proxy server** act as **an intermediary between INTERNAL & EXTERNAL** IP address **& block direct access to the INTERNAL NETWORK.**
- Proxy server provides **another layer of access control** by segregating the **flow of Internet traffic.**
- ***PROXY SERVERS*** are capable of **filtering for potential malicious code & application specific commands.**

APPLICATION LEVEL FIREWALLS



- It performs **application level screening,** including
- The filtering capabilities of packet filter firewall + With Additional VALIDATION of the packet content based on the application
- Application firewall **examines EACH PACKET after the initial connection is established for specific application.**

UNAUTHORISED INTRUSION

*It is the **attempt to monitor & possibly prevent attempts to intrude in the system & network resources of the organisation.***

WHAT TYPE OF INTRUSION DETECTION SYSTEMS?

Intrusion detection system falls into **2 categories:**

1. **Network Based System:**

NATURE	WORKING
1. **This type of system are** placed on the NETWORK,	1. They examine the network traffic.
2. **Nearby the system or systems being monitor.**	2. Determine whether it falls within acceptable boundaries.

2. **Host Based System:**

NATURE	WORKING
1. **This type of system actually runs** on **system being monitored.**	1. **They examine the system to determine whether the activity on the system is acceptable.**

HACKING

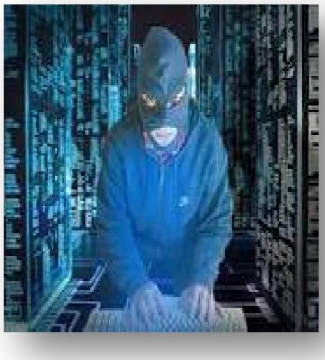
HACKING is an act of ***penetrating computer systems*** **gain KNOWLEDGE about the system & how it works.**

NOW WILL DISCUSS THE VARIOUS TERMINOLOGY OF THE HACKING

A. HACKERS:

HACKERS is someone who is enthusiastic about the computer programming & all things related to technical working.

B. CRACKERS:



CRACKERS are people who try to gain unauthorised access to computers.

C. DAMAGE CAUSE BY THE HACKERS:

- ***Hackers can see what you doing on your computer.***
- ***Hackers can write NEW, DELETE and EDIT files.***
- ***Hackers can install programs on your system without your knowledge which can be used to steal information.***

D. HOW DO HACKERS HACK:

Ways by which hackers can hack**:**

CODE TO REMEMBER: R.H.-N.I.F.

Right **H**and mein K**NIF**e

1. **R**PC.STATD:
   - This is a problem **specific to LINUX & UNIX.**
   - There is problem of unchecked buffer overflow problem.
   - Data exceeds the memory, **as such hackers could WRITE** bits of program code **into memory.**

2. **H**TTP:
   - It means **"HYPERTEXT TRANSFER PROTOCOL".**
   - There is **bug** in this software called an **"UNCHECKED BUFFER OVERFLOW".**
   - If user makes **request** for a file on web, part of request go into memory that contain program code, **through which hacker can run program he want on the server**.

3. **N**ETBIOS:
   - This kind of hack **exploits a BUG** in Window9x.
   - It is used on **local area network.**

4. **I**CMP PING:

- It is main protocol that makes **internet** work.
- "**PING**" is command **that can be sent to a computer using ICMP.**
- **A computer will respond back,** telling that computer exists. If the computer doesn't have adequate firewall, **hacker can easily hack.**

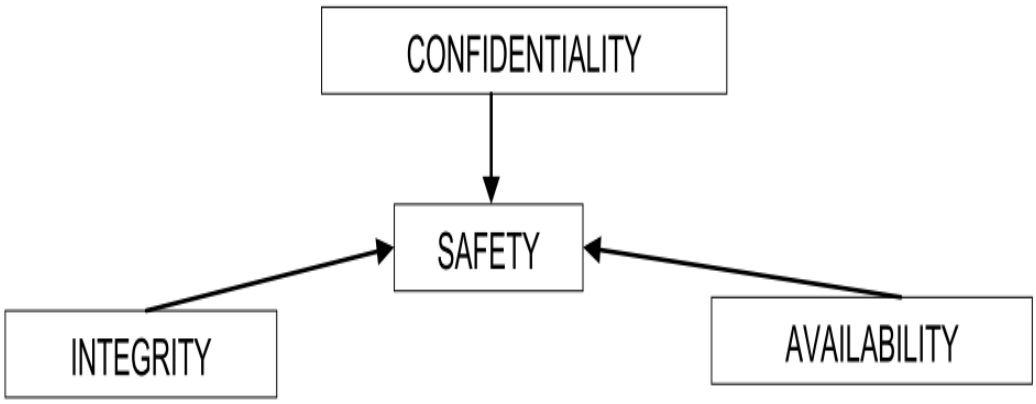
5. **F**TP (**FILE TRANSFER PROTOCOL**):

- It is **standard internet protocol,** which can be sued to **download files** from website.
- FTP requires some **form of authentication** for access of private files such as:

  -- **Doly Trojan** -- **Fore** -- **Blade Runner**

AUDITOR'S ROLE

Focus of the IS auditor is to examine ALL FACTORS *that adversely affect* ***the CONFIDENTIALITY, INTEGRITY & AVAILABILITY*** *of the information.*



DATA PRIVACY

DATA PRIVACY REFERS to the **EVOLVING RELATIONSHIP** between **technology & legal right,** in collection & sharing of **data.**

The most common sources of data that are affected by DATA PRIVACY issues are:

■ Health information	■ Genetic Information
■ Criminal Justice	■ Location Information
■ Financial Information	

A. DATA PRIVACY POLICIES:

Following are the data privacy policies: **Code to Remember: I.-D^2.E.E.**

1. **I**nformation sharing: Corporate customer information shall not be shared with anyone.
2. **D**ata backup Encryption: All data backup must be **encrypted.**
3. **D**ata Access: Access to information, hard copy **must be restricted to some individuals.**
4. **E**xtranet Connection Encryption: All extranet connections must use **encryption** to protect privacy of information.
5. **E**-mail Monitoring: All **e-mail must** be monitored.

CONTROLLING AGAINST VIRUSES & OTHER DESTRUCTIVE PROGRAMS

Following are the antivirus software, used to protect data from viruses & also prevent their propagation & harm:

1. **SCANNERS:**
   - These scanners look for sequence of **bit patterns** called **virus signatures** which are characteristic of **virus code.**
   - They check **memory, disks, and system files** to find matching **bit patterns.**
   - It is therefore necessary to **update the scanner with the data.**

2. **ACTIVE MONITOR & HEURISTIC SCANNER:**
   - This look for **critical interrupt calls & operating system functions,** depicting virus actions.

3. **INTEGRITY CHECKERS:**
   - These **detect unauthorised changes** to system files.
   - This requires s**tock of all files** on the system, & compute a binary **check data called "CYCLIC REDUNDANCY CHECK (CRC)".**
   - When program is called for execution, **software** computes **CRC** again & checks with the parameters.

RECOMMENDED POLICY & PROCEDURE CONTROLS

Following are the recommended policies & procedures

VIRUS RELATED POLICIES

H	Reporting & incident handling procedure to **H**andle virus.
A	Security policy **A**ddress the virus threats, vulnerabilities etc
T	Anti-virus **awareness** & **T**raining on symptoms of attacks.

HARDWARE / SOFTWARE RELATED POLICIES

Code to remember: I A.M. A.KHIL

1. Hardware **I**nstallation & related component to be verified.
2. All terminals must have **RATED ANTI-VIRUS** software installed
3. External **M**edia like **disks, CDs', tapes** must be avoided.
4. All new software acquisition should follow a controlled procedure of **centralised A**cquisition & testing for virus.

NETWORK RELATED POLICIES

Network access to internet should be strictly preferable to stand alone computers

Network should be **protected** by means of **FIREWALL** that can prevent unknown virus

LOGICAL ACCESS CONTROL

These controls are designed to designate WHO or WHAT to have access to a SPECIFIC SYSTEM RESOURCES & type of transactions & functions.

Assessing logical access controls involves evaluating the FOLLOWING critical procedures:

- Logical access control restricts the **unauthorized access to system.**
- There are logical controls over the **network access.**
- Controls implemented **to protect the integrity of the application.**

Here we will discuss some of the logical path access:

1. Online Terminals:

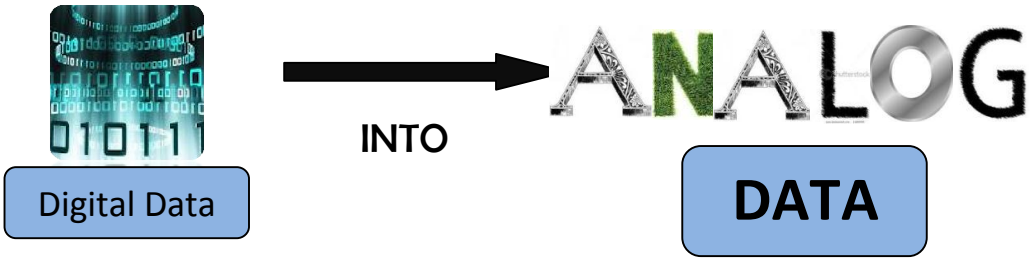
- To access on line terminals, a user has to provide,
- **a valid LOGIN-ID & password.**

2. Batch Job Processing :

- Here all **jobs are processed** in a **BATCH.** These batches are processed on **regular interval.**
- The **jobs are accumulated** and sent in **batches.** In accumulation process, it might be possible that **unwanted access** may threat the **integrity** of the data.
- To avoid this, **access to be granted to authorized persons.**

3. Dial up ports:

- **Dial up port** connects remotely to other network via communication media.
- **MODEM =** convert



- Modem can be used to connect with other through **terminal & telephone lines.**

4. Telecommunication Network:

- In this network, **a number of computer terminals, personal computers** etc are **host computers,** through **network or telephone lines.**
- Each of these routes has to be protected by means **of security procedures:**

Access controls mechanism should provide security to the following applications:

Access Control Software	*Application Software*
Data	*Data Dictionary*
Libraries	*Logging Files*

Issues & revelation relating to logical access:

*Logical access controls are used to increase the **organization's potential** for the losses that result due to **exposures** that may lead to shut down of the system.*

*Some of the exposures that an entity's system is o**pen to:***

TECHNICAL EXPOSUERS

It includes UNAUTHORISED IMPLEMENTATION & MODIFICATION of DATA & SOFTWARE.

I. DATA DIDDLING:

- Data diddling involves **change of data** before **or** as they entered in system.
- **Limited** technical knowledge is required **to diddle data.**

II. BOMBS:

- Bomb is a piece **of BAD CODE** deliberately planned by an insider.
- This bomb explodes or cause damage when **condition of explosion** gets fulfilled.
- Bombs are generally of 2 types:

TIME BOMB

- It causes disruption **of computer, system modification of data etc,** on a **particular DATE & TIME** for which it is developed.
- The **COMPUTER CLOCK** initiate it

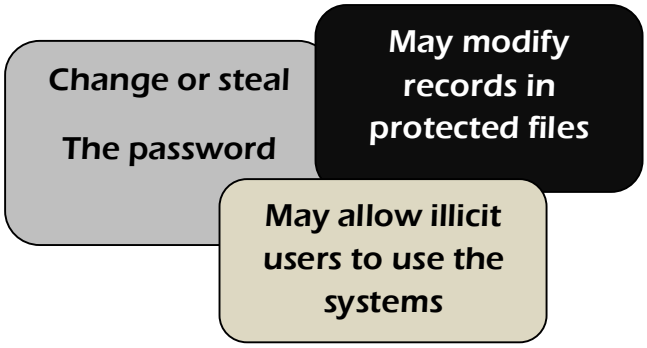
LOGIC BOMB

- It is **combination of EVENTS.**
- For instance
  "If a file name **Akhil** is changed, then content will be **permanently deleted.**"

III. TROJAN HORSE:

- These are **program hidden under AUTHORISED PROGRAM.**
- It is **ILLICIT (ILLEGAL)** coding contained in **a legal program.**
- **It doesn't copy itself to** another machine.

- **TROJAN MAY RESULT IN:**



IV. WORMS:

- WORM copies itself **to another machine on the network.**
- Worms **are stand alone programs,** & can be easily detected.
- Worms **doesn't harm or cause damage to the** system, **BUT ONLY COPIES** itself in a **computer network.**

V. ROUNDING DOWN:

- Refers to **ROUNDING OF SMALL FRACTIONS,**
- of a **denomination** & **transferring fractions to AUTHORISED** account.

VI. SALAMI TECHNIQUES:

- Involves **slicing of small amounts** of money **from computerised transactions.**
- For example **Rs. 21,45,526.95** is being **written as Rs. 21,45,526.**

VII. TRAP DOORS:

- It allows **insertion of SPECIFIC LOGICS,** such as program interrupts **that permits a review of the data.**
- **It also permits insertion of UNAUTHORISED LOGIC.**

COMPUTER CRIME EXPOSUERS

Computer systems are used to steal money, goods, software or corporate information. Some of the side effects of these computer crimes are as follows:

1. FINANCIAL LOSES:
   - It covers **loss of electronic funds,**
   - Or increase in **expenditure towards repair of** damaged electronic components.
2. LEGAL REPERCUSSION:
   - An entity has to adhere various **human rights** policies.
   - Organisation is **exposed to LAWSUITS** from investors in case of non-compliance of rules.
   - Auditor must take **legal view** before reviewing the issues related to it.
3. LOSS OF CREDIBILITY:
   - Credibility is the **ESSENCE** of any business to **maintain its competitive edge in market.**
   - This credibility will be shattered **resulting in loss to the business & prestige.**
4. BLACKMAIL:
   - The perpetrator **(One who designs)** can obtain money from the organisation by **threatening & exploiting the SECURITY VIOLATION.**

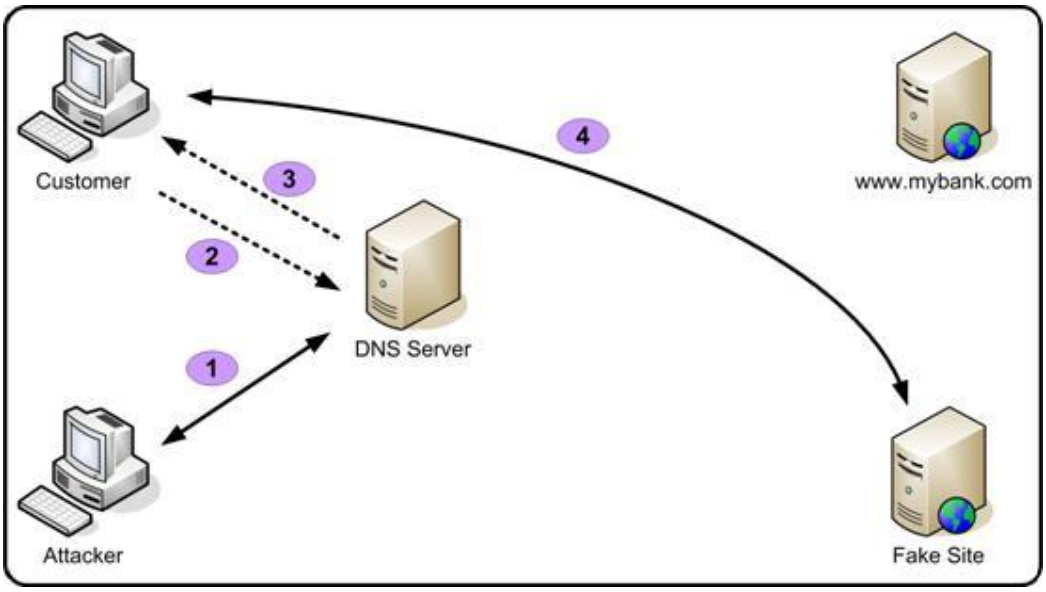
5. **DISCLOSURE OF INFORMATION:**

- This event involves **disclosure of sensitive, confidential** information.
- Such practice can **spoil the REPUTATION** of the organisation.

6. **SABOTAGE:**

- People who are not interested in **financial gain,** also want to spoil the credibility of the organisation.
- This is due to reason of **DISLIKE** for the organisation.

7. **SPOOFING:**



1. **The attacker targets the DNS service used by the customer**
2. **The customer queries the DNS server**
3. **The DNS responds to the customer query– not the real IP address**
4. **The Customer then connects to the host, expecting it to be www.mybank.com, but in fact reaching the attackers fake site.**

- **It involves FORGING ONE'S SOURCE ADDRESS.**

- Spoofing is when an attacker pretends to be someone else in order gain access to restricted resources or steal information.
- One machine is used to **IMPERSONATE** (To assume character of) the other in spoofing technique.
- For example, **a penetrator makes the USER think that he/she is connected to operating system.**

ASYNCHRONOUS ATTACKS

Here data can be moved asynchronously across the telecommunication lines. There are many forms of ***Asynchronous attacks:***

1. **DATA LEAKAGE:**
   - Data leakage involves **dumping files to papers OR stealing computer reports & tape.**

2. **WIRE-TAPPING:**
   - This involves **SPYING INFORMATION** being transmitted over the telecommunication network.

3. **PIGGYBACKING:**
   - This is an **act of following an AUTHORISED person through**
     A SECURED DOOR
     OR
     ATTACHING TO AUTHORISED
     TELECOMMUNICATION LINK
   - This involves **intercepting communication** between OPERATING SYSTEM & USERS.

4. SHUT DOWN OF COMPUTERS :

- This is **initiated** through **terminals or microcomputers** that are **directly or indirectly** connected to the computers.
- These security measures will function **if appropriate access control** on the logging. In case of **overloading** some system proved to be vulnerable & **shut themselves**.
- **HACKERS** use this technique to **SHUT DOWN** computer system over internet.

PHYSICAL & ENVIRONMENTAL CONTROL

*Physical & environmental securities are the measures **taken to protect system, buildings, and related** infrastructure. This protection involves the following critical procedures:*

- *Data is protected from interception.*
- *Mobile & portable systems are protected.*
- *Physical security controls are commensurate with risk of physical damage.*

LOGICAL ACCESS CONTROLS are implemented in order to protect the following type of ASSETS:

TYPES OF ASSET	SECURITY CONTROL
User Access Management **USER REGISTRATION** **PRIVILEGE MANAGEMENT**	■ Is the user registered to access the information? ■ Is de-registration process is followed? ■ **Privilege** access i.e. **one can access that data** which he uses in fulfilling his duties.

USER PASSWORD MANAGEMENT ***REVIEW OF USER ACCESS RIGHT***	■ Allocation, storage, revocation & reissue of password are **password management functions.** ■ User needs changes with time & as such **requires periodic** review of access right.
User Responsibilities ***PASSWORD USE*** ***USNATTENDED USER EQUIPMENTS***	*User awareness & responsibility is critical factor* ■ Use of **strong passwords** to maintain confidentiality. ■ User must ensure that no **equipment under their responsibility** is left **unprotected**
Network access control ***POLICY ON USE OF NETWORK SERVICES*** ***ENFORCED PATH*** ***SEGREGATION OF NETWORKS*** ***SECURITY OF NETWORK SERVICES***	*Internet puts an organization on stake, since one can access entity information easily:* ■ Selection of appropriate services & approval to access them is **part of the policy.** ■ Based on **risk assessment,** it is necessary to **specify path** connecting networks. ■ Based on **sensitive information,** it is necessary that some **network** to be isolated from the **internet service.** ■ Technique of **authentication & authorization** policy implemented across the **organization's network.**
Operating system access control	*Operating system helps application to use **various IS resources** & perform functions. If there is an unauthorized access, **operating system** is last*

AUTOMATED TERMINAL IDENTIFICATION ***TERMINAL LOG ON PROCEDURES*** ***USER IDENTIFICATION & AUTHENTICATION*** ***PASSWORD MANAGEMENT SYSTEM*** ***USE OF SYSTEM UTILITIES***	***barrier*** *to be* ***conquered*** *for unlimited access.* *It ensures that* ***a session could only be started*** *from* ***a particular location*** *or* ***computer terminal*** *It doesn't provide* ***unnecessary help*** *to provide information which may be misused by* ***intruder.*** *The user must* ***be identified*** *&* ***authenticated.*** *An operating system must have* ***selection of good passwords.*** ***System utilities*** *are the programs* ***that help to manage critical functions*** *of operating system.*
Application & monitoring system access control ***SENSITIVE SYSTEM ISOLATION*** ***EVENT LOGGING***	*A user is allowed to access the* ***information*** *for which he is authorised to access.* ***Controls*** *are implemented on the* ***access rights*** *of the users.* *Critical constitution of the* ***system,*** *if necessary must be run in* ***isolation.*** *It is necessary to* ***review if logging*** *is enabled.*
Mobile Computing	*Theft of* ***data*** *on the disk drives* ***is HIGH RISK FACTOR.*** *To protect the data,* ***information has to be encrypted & access identifications*** *i.e.* ***fingerprints, eye-iris, smart cards*** *etc*

AUDITOR'S ROLE

IS auditor has to keep in mind the following points while working with the logical access control mechanism:

Code to Remember: V - M.A.R.D.S.

1. **V**erifying test controls:
   - Verifying the test controls over access paths to determine effective functioning.

2. **M**echanism of access controls:
   - Auditor has to evaluate access control mechanism, analyse test results & other audit evidences.

3. **A**ccess path:
   - Potential access paths into SYSTEM must be evaluated by the auditor.

4. **R**edundancies identification:
   - Deficiencies or redundancies must be identified & evaluated.

5. **D**ocuments reviewing:
   - Reviewing the relevant documents & risk assessment techniques & understanding the security risks.

6. **S**ecurity policies comparison:
   - The auditor should compare **SECURITY POLICIES** of other organisation with policies of their organisation & access its adequacy

PHYSICAL ACCESS CONTROL

This section of my notes **deals with the LOSSES due to ACCIDENTS, INTENTIONAL VIOLATION OF ACCESS PATHS** etc.

It covers the flowing 3 areas of discussion

Now explaining each of the above said areas in detail:

1. Physical Access Issues & Exposures

Following points depicts the result *due to* intentional violation of access paths:

Code to Remember: U.B.I. - M.A.D.E.

1. **U**nauthenticated entry.
2. **B**lackmail
3. **I**nformation disclosure publicly.
4. **M**odification of semester equipment & information.
5. **A**buse of data processing resources.
6. **D**amage or theft of documents or equipments
7. **E**mbezzlement.

(a) POSSIBLE PERPETRATORS:

- Perpetrators may be because of employees who are:

❁ Discontented	❁ Interested outsider.
❁ Former Employees	❁ Threatened for disciplinary action
❁ On Strike	
❁ Terminated employee	❁ Addicted to gambling

- Facilities to be protected from **auditor point of view:**

❁ Computer Room	❁ Portable equipments
❁ Local Area Network	❁ Control Units
❁ Power sources	❁ Input/output control room
❁ Storage rooms	

(b) ACCESS CONTROL MECHANISM:

- It is associated with **identified, authorised** users & the resources they are allowed to access.
- The **mechanism** processes **user request in 3steps:**
  - ❖ ***Identification***
  - ❖ ***Authentication***
  - ❖ ***Authorisation***

(c) IDENTIFICATION & AUTHENTICATION:

- Users identify themselves **to access control mechanism** by providing information.
- To validate the user, **his entry is matched** with the **entry in the authentication file.**

(d) AUTHORISATION:

- There are 2 approaches to implement the authorisation module:

TICKET ORIENTED APPROACH

In this approach, **access control mechanism** assigns

USERS

Users are assigned **a TICKET** for each resources & element represents the **user privilege on the resources**

LIST ORIENTED APPROACH

Resource / User	File A	Editor	File B	Program
User P	Read	Enter		
User Q	Statistical Read only	Enter		Enter
User R		Enter	Append only	
User S		Enter		Read Resource Code only

Under this approach, **access control mechanism operates with the help of MATRIX.**

Taking the example, MR. P can only read **FILE A.** As such, mechanism is presented via **a column in the matrix.**

2. Physical Access Controls

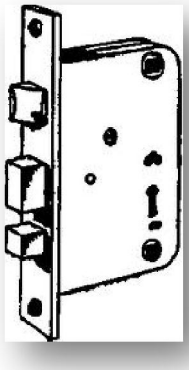
Physical access controls *are designed to protect the organisation* ***from UNAUTHORISED ACCESS.*** *Some of common access controls techniques are as follows:*

(a) Locks on Doors:

CIPHER LOCKS

- Cipher lock consists of **pushbutton** fixed near door.
- There are **10 numbered buttons** on the panel.
- To enter. **A person has to punch 4 DIGIT** sequence & door unlock for **a predetermined period.**

BOLTING DOOR LOCKS



- Special metal key is used **to gain entry,**
- When the lock is a **bolting door lock.**

ELECTRONIC DOOR LOCKS

- A magnetic **chip-based** plastics card key, may be
- Entered into **a sensor reader to gain access in system.**
- Thereafter the sensor read the code, **that is stored** within **card activates** the door locking mechanism.

BIOMETRIC DOOR LOCKS

- These locks are extremely secure, which uses individual's unique body features such as:
- **Retina, voice, fingerprints, signature** etc.
- **This type of security needed to protect sensitive information.**

(b) Physical Identification medium:

PERSONAL IDENTIFICATION NUMBERS

- A secret number is assigned to individual.
- Visitor is asked to **log on** by inserting card in device & enter their PIN for authentication.
- Example : **Cash withdrawal procedure from ATM**

PLASTIC CARDS

- These cards used **for identification purpose**.
- Control over this card ensures **authorised access** by the users.

IDENTIFICATION BADGES

- Can be **issued to personnel as well to visitors.**
- For easy identification, **badges** may be given different c**olours.**

(c) Logging on utilities:

MANUAL LOGGING

- Keeps the record of the visitors **including NAME, PURPOSE OF VISIT, PERSON TO SEE.**
- Any identification proof may also be asked for gaining the entry.

VISITORS' REGISTER

DATE	NAME	ADDRESS	INTRODUCED BY		
Jan 10 74	Gordon Wolfe	Head office	anne	3:30	3:45
Jan 15 74	Lloyd St clair	Can. Chemicals Corp	Neil	3:40	4:00
Jan 16 74	Mr. Shaun		Curtis	9:30	10:00
Jan 16 74	Mr. Shearington		Curtis	11:30	—
Jan 17 74	Walter Lucas	Tempisto Ind. Ltd.	O.B. Bishop	11:55	—
Jan 18 74	Hugh McMillan	Development Corp	Jule	9:40	
Jan 18 74	alex clunis	Fuller Brush Corp.	Neil	not in	
Jan 18 74	Clayton C Mifflin	Credit Bureau Chat	Dan	2:00	

(d) **Other means of controlling physical access:**

❖ Video Cameras	❖ Computer Terminal Locks
❖ Security Guards	❖ Alarm System
❖ Controlled Visitor Access	❖ Perimeter Fencing
❖ Bonded Personnel	❖ Secured Report
❖ Dead Man Doors	❖ Controlled single Entry Point

AUDITOR'S ROLE

IS auditor has to keep in mind the following points while working with the physical access control. Auditor has to form **an opinion on the effectiveness** of the physical access controls:

RISK ASSESSMENT	PARTICULARS
Risk Assessment	■ Auditor must satisfy himself that **risk assessment procedure** covers **periodic & timely assessment** of all assets.
Controls Assessment	■ Auditor based on **risk profile evaluates** whether the **physical access controls** are in place.
Planning for review of physical access controls	■ It requires **examination of relevant documentation.**
Testing Of Controls	■ Physical inventory of **equipments.** ■ **Interviewing personnel** can provide information **on awareness of procedures.** ■ Observation of **safeguards & physical access procedures.**

PHYSICAL ACCESS CONTROL

This section deals with **external factors** in **information system & preventive measures** to overcome these conflicts. Issues covered:

- ENVIRONMENTAL ISSUES & EXPOSURES
- AUDIT & EVALUATION TECHNIQUES FOR ENVIRONMENTAL CONTROLS.

Following are the information system resources:

1. HARDWARE & MEDIA:

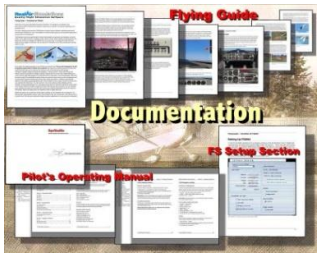
- Includes COMPUTER & COMMUINCATION EQUIPEMNTS,
- & STORAGE MEDIA

2. INFORMATION SYSTEMS SUPPORTING INFRASTRUCTURE:

- Includes the following

Physical premises	Communication Closet
Cabling Ducts	Power Source

3. DOCUMENTATION:



- Physical & geographical Documentation of,
- Computing facilities with emergency plans & incident planning procedure

4. SUPPLIES:

- Third party maintenance procedure,
- By the civil contractors whose entry & assess with respect to their scope of work assigned.

5. PEOPLE:

- Employees, contractor employees, visitors, third party personnel,
- Are to be made responsible/accountable for environmental controls.

3. Audit & Evaluation techniques for environmental Controls

A. WATER & SMOKE DETECTOR:

- ✓ Presence of water & smoke detector are to be,
- ✓ Verified by visiting the computer rooms.

B. HAND HELD FIRE EXTINGUISHER:

- ✓ Presence of fire extinguisher in strategic locations.
- ✓ Throughout the facility is checked for.

C. FIRE SUSPENSION SYSTEMS:

- ✓ Testing of **suppression systems,** & documenting that the system has been inspected **& tested.**

D. FIREPROOF WALLS, FLOORS ETC.

- ✓ Check the fire rating of the wall surrounding the information system facilities.

E. ELECTRICAL SURGE PROTECTOR:

- ✓ Here, **presence of** electrical surge **protectors** for **sensitive & expensive computer equipment** is observed.

F. WIRING PLACED IN ELECRTIC PANELS:

- ✓ Check whether **wiring in the information** facilities **is placed** in the fire resistant panel.

END OF THE CHAPTER

I EXPLAINED THOSE TOPICS WHICH ARE IMPORTANT AS PER ME. OTHER TOPICS I HAVE NOT EXPLAINED, IF NEEDED CONTACT ME AT E-MAIL ID