Date: 16 April 2021

VIRTUAL COACHING CLASSES
ORGANIZED BY BOS, ICAI

INTERMEDIATE LEVEL
PAPER 7A : ENTERPRISE INFORMATION SYSTEMS

Faculty: CA Rekha Uma Shiv

INFORMATION SYSTEM AND ITS COMPONENTS

DAY-1

SYSTEM

- A group of mutually related and cooperating elements.
- Having common goal.
- By taking inputs and producing outputs.
- It may contain several sub systems with sub goals all contributing to meet the overall system goal.

INFORMATION SYSTEM

- Refers to interaction between process and technology.
- The main aim and purpose of each Information System is to convert the data into information which is useful and meaningful.
- Accepts data as input from the user for a process that creates information as output .

INFORMATION SYSTEM MODEL

An Information System model comprises of :

1. **Input:** Data collected from an organization or from external environments. It's converted into suitable format required for processing.

2. **Process:** A process is a series of steps undertaken to achieve desired outcome or goal.
3. **Output:** Then information is stored for future use or communicated to user.

INPUT

(Business problems in the form of data, instructions, commands)

PROCESSING (Software, Programs, people, communication equipment, storage)

OUTPUT (Solution to problems in the form of reports, graphics, calculations, media)

User

CONTROL

(Decision Makers, Auto Control)

FEEDBACK

Components of Information System

PEOPLE

- People are the most important element in most Computer-based Information Systems.

- The people involved include **users of the system and information systems personnel**, including all the people who manage, run, program, and maintain the system.

COMPUTER SYSTEM – HARDWARE

- **Hardware** is the tangible portion of our computer systems;
- It basically consists of devices that perform the functions of input, processing, data storage and output activities of the computer.

HARDWARE

INPUT

a) Commands

b)Instructions

c) Texts

d)Image

e)Audio

f)Video

PROCESSING

a) Storage

b)Retrieval

c)Transformation

d) Deletion/ Updation / Alteration

OUTPUT

a) Textual

b) Graphical

c) Tactile

d) Audio

e)Video

DATA STORAGE

a) Internal Memory

b) Primary Memory

c) Secondary Memory

d) Virtual Memory

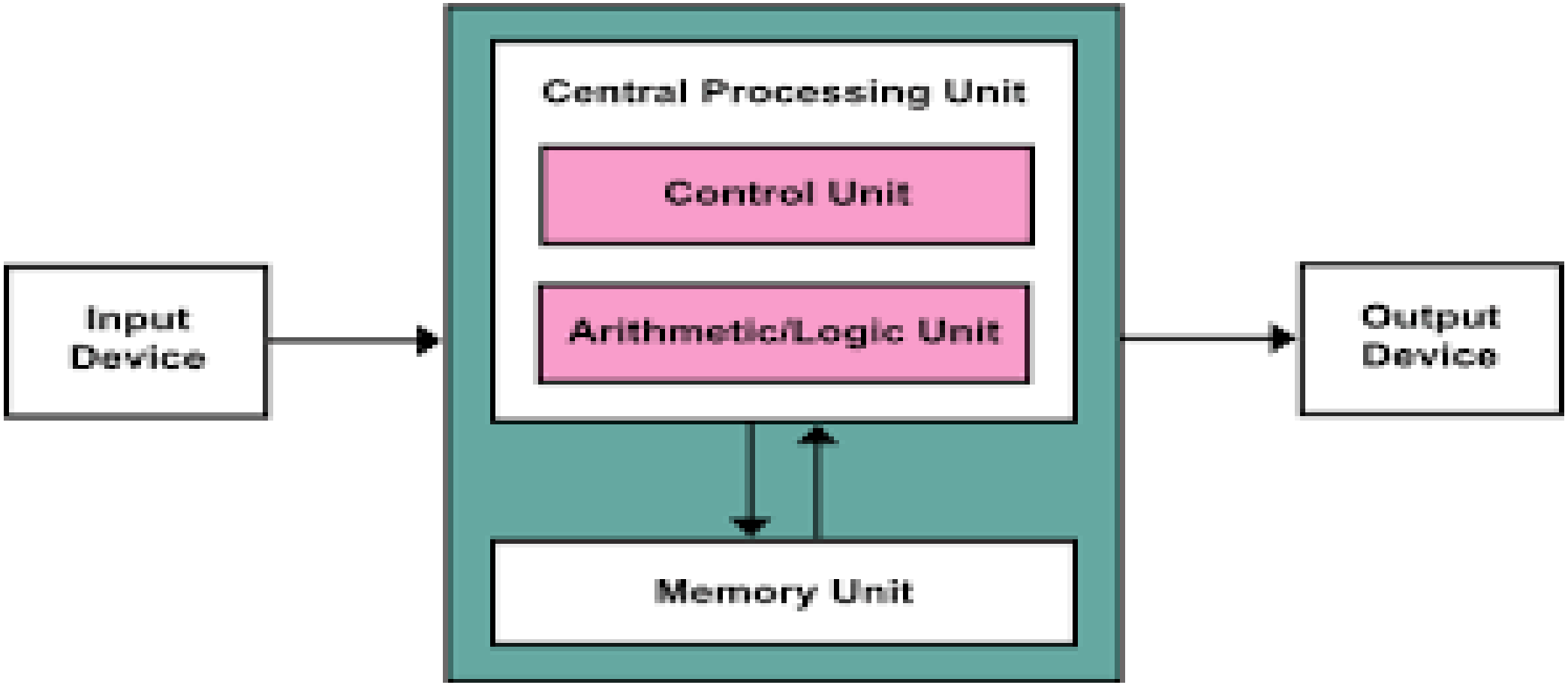
INPUT

- **Input Devices** are devices through which we interact with the systems.
- It include devices like Keyboard, Mouse, Touch pad, Scanners and Bar Code, MICR readers, Webcams, Microphone and Stylus/ Touch Screen.
- Keyboard helps us with text based input, Mouse helps us in position based input, Scanners & Webcams help in image based input and Microphone helps us in voice based input.

PROCESSING

- Includes the Central Processing Unit and the main memory.
- Its called brain of the computer .
- The Central Processing Unit /microprocessor interprets and executes the program instructions and coordinates how all the other hardware devices work together.
- The CPU is built on a small flake of silicon taking binary value of 1 or 0.

CPU



UNITS → Big & Way Big Bytes

- Byte a grouping of eight bits
  for instance --> 0110 0001
- **Kb** (kilobyte) about 1000 bytes
- **Mb** (megabyte) about one thousand Kb
  or one million bytes
- **Gb** (gigabyte) about one thousand Mb
  or one billion bytes
- **Tb** (terabyte) is about one thousand Gb
  or one trillion bytes

OUTPUT DEVICES

- Output devices are devices through which system responds.
- Provide output to decision makers at all levels in an enterprise to solve business problems.
- Output may be in in visual, audio or digital forms.
- Common output devices include monitors (LCD/CRT),printers ,speakers etc.

TYPES OF OUTPUT

- **Textual output** comprises of characters - words, sentences, and paragraphs.
- **Graphical outputs** are digital representations of non-text information - drawings, charts, photographs, and animation.
- **Tactile output** such as raised line drawings may be useful for some individuals who are blind.
- **Audio output** is any music, speech, or any other sound.
- **Video output** consists of images played back at speeds to provide the appearance of full motion.

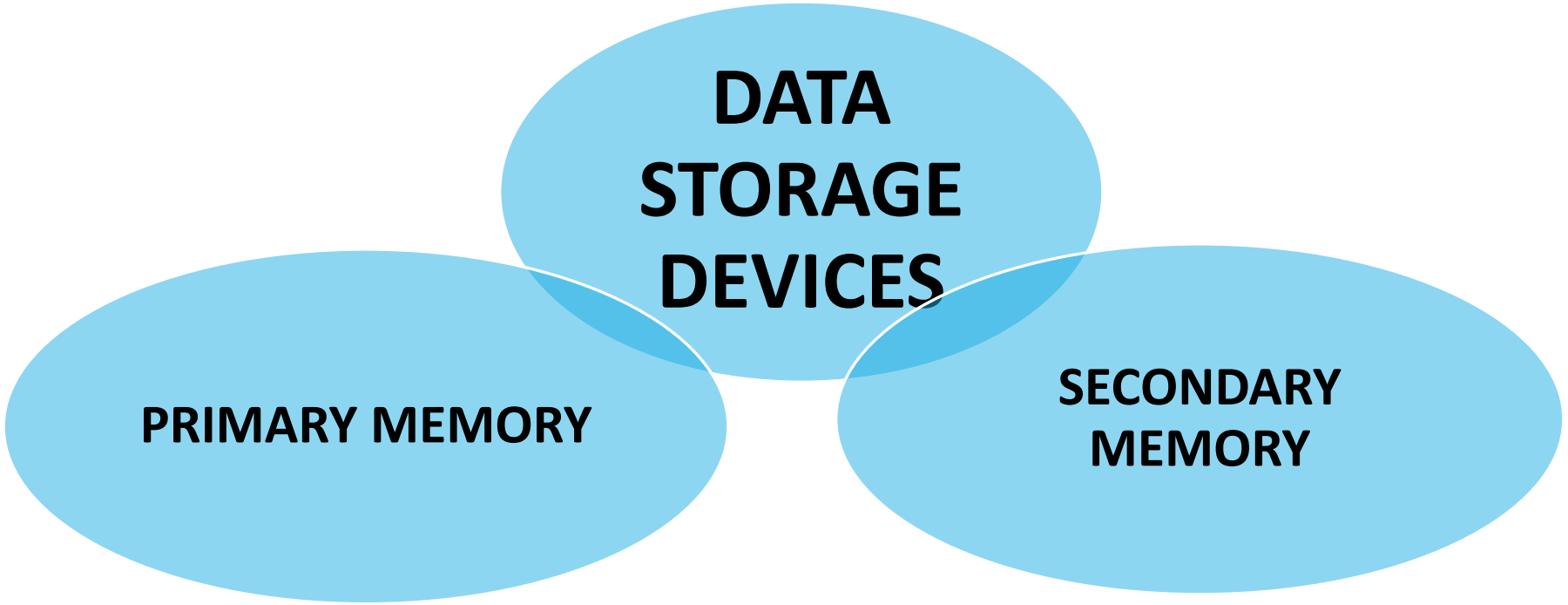
MCQ Time !

Q. The people who use the information system in Xybo Computec include:

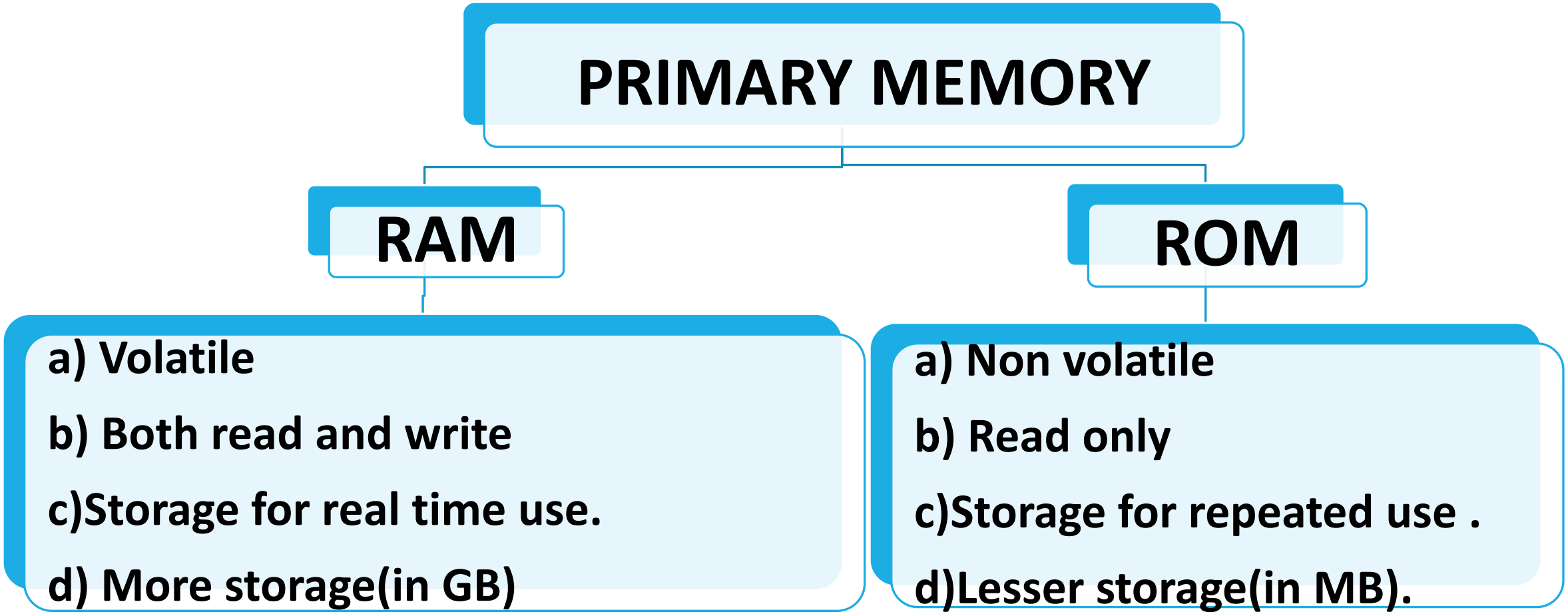
a) Management
b) Information systems personnel
c) Developers and testers
d) All of the above

DATA STORAGE DEVICES

- Refers to the memory where data and programs are stored.

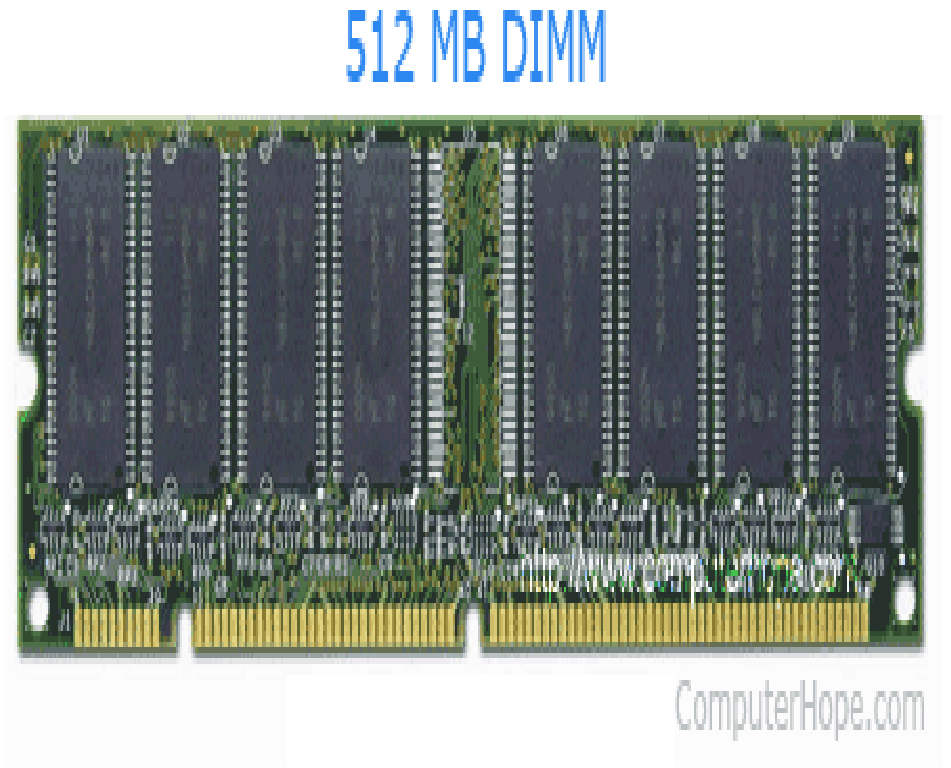


PRIMARY/MAIN MEMORY



ROM Example

RAM Example



SECONDARY MEMORY

- CPU refers to the main memory for execution of programs, but these main memories are volatile in nature and small in storage capacity.
- The secondary memories are available in bigger sizes; thus programs and data can be stored on secondary memories.

Contd..

The features of secondary memory devices are :

a)Non-volatility

b)Greater capacity

c)Greater economy

d)Slow speed

SECONDARY MEMORY EXAMPLES


Flash


Floppy Disk


Zip Disk


CD + RW

CD + R


DVD + RW


DVD + R


Storage Tape


Smart Media


Removable Hard – Drive

Micro Drive


Memory Stick


Smart Cards


Online Storage Site


PC Card

MCQ Time !

Q. During festive seasons the external hard disk is often given as a complimentary product along with high end systems. Which of the following is not an advantage of the said complementary product compared to the system memory?

a) Non-volatility

b) Greater capacity

c) Greater economy

d) Greater speed

PROCESSOR REGISTERS

- **Processor Registers:** Registers are internal memory within CPU, which are very fast and very small.

CACHE MEMORY

- **Cache Memory:** To bridge the huge speed differences between Registers and Primary Memory, we have cache memory.
- Cache is a smaller, faster memory, which stores copies of the data from the most frequently used main memory locations.
- Processor/Registers can access it more rapidly than main memory.

MCQ Time !

Q. Which among the following is a smaller, faster memory, which stores copies of the data from the most frequently used main memory locations ?

a) Primary Memory

b) Virtual Memory

c) Cache memory

d) Secondary Memory

DATA

- Raw fact
- Unprocessed bits and pieces of information with no context.
- It can either be quantitative or qualitative.
- Once data is processed , it is converted to meaningful information.
- This information can be used for decision making and analysis.

DATABASE

A set of logically inter-related organized collection of data.

DATABASE MANAGEMENT SYSTEMS (DBMS)

- DBMS may be defined as a software that aid in organizing, controlling and using the data needed by the application program.
- Provide the facility to create and maintain a well-organized database.
- Examples - Oracle, MySQL, SQL Servers and DB2

Various operations that can be performed on these files are as follows:

- **ADDING** new files to database,
- **DELETING** existing files from database,
- **INSERTING** data in existing files,
- **MODIFYING** data in existing files,
- **DELETING** data in existing files, and
- **RETRIEVING OR QUERYING** data from existing files.

DATABASE MODEL

- Type of data model
- Determines the logical structure of a database
- Determines in which manner data can be stored, organized and manipulated.

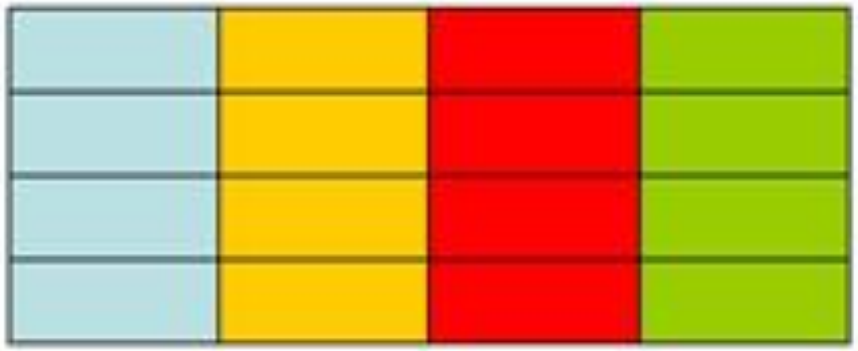
HIERARCHY OF DATABASE

- **Database:** This is a collection of Files/Tables.
- **File or Table:** This is a collection of Records. It is also referred as Entity.
- **Record:** This is a collection of Fields.
- **Field:** This is a collection of Characters, defining a relevant attribute of Table instance.
- **Characters:** These are a collection of Bits.

- The field is the basic unit of data in a database. A field stores a single piece of information of a particular data type:

- Fields are combined to form records:

- A set of records with the same fields are collected together in a table:



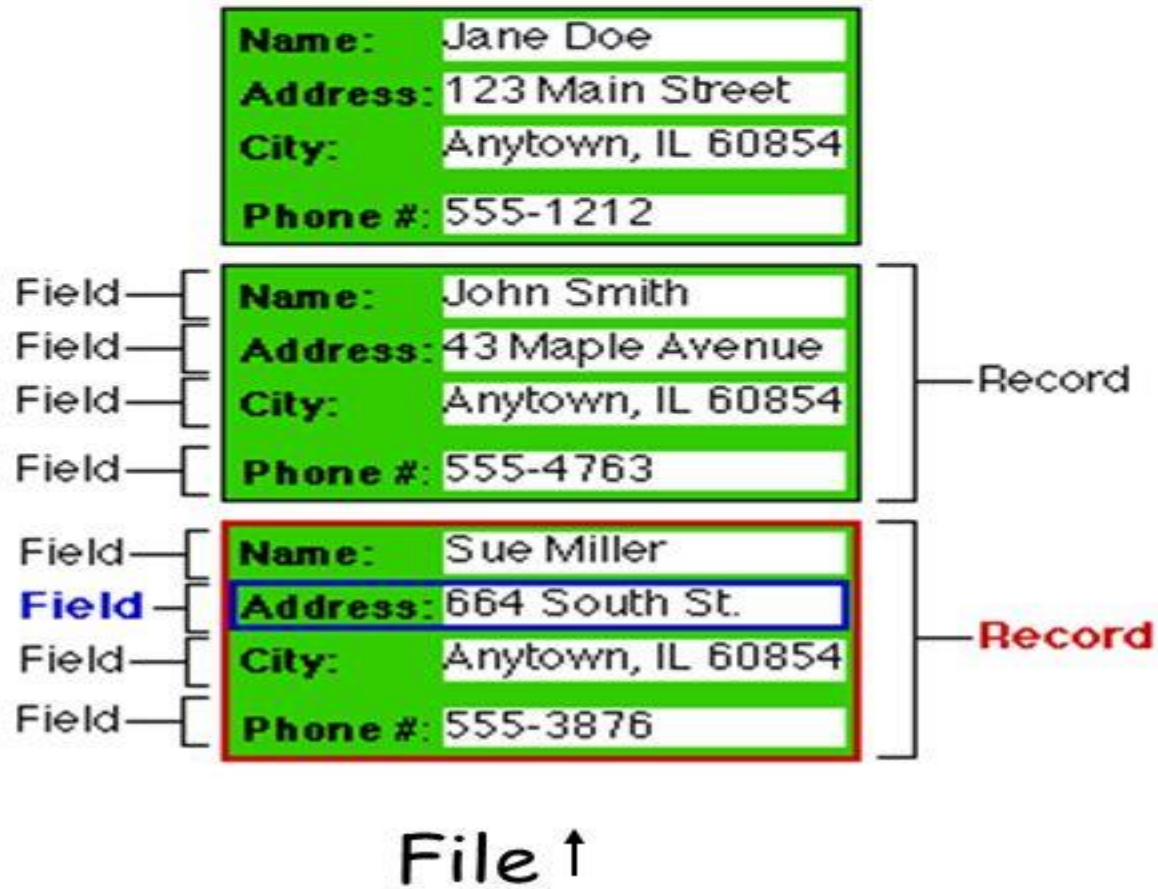
Basics of a Database

Databases are made up of

-files

-records

-fields

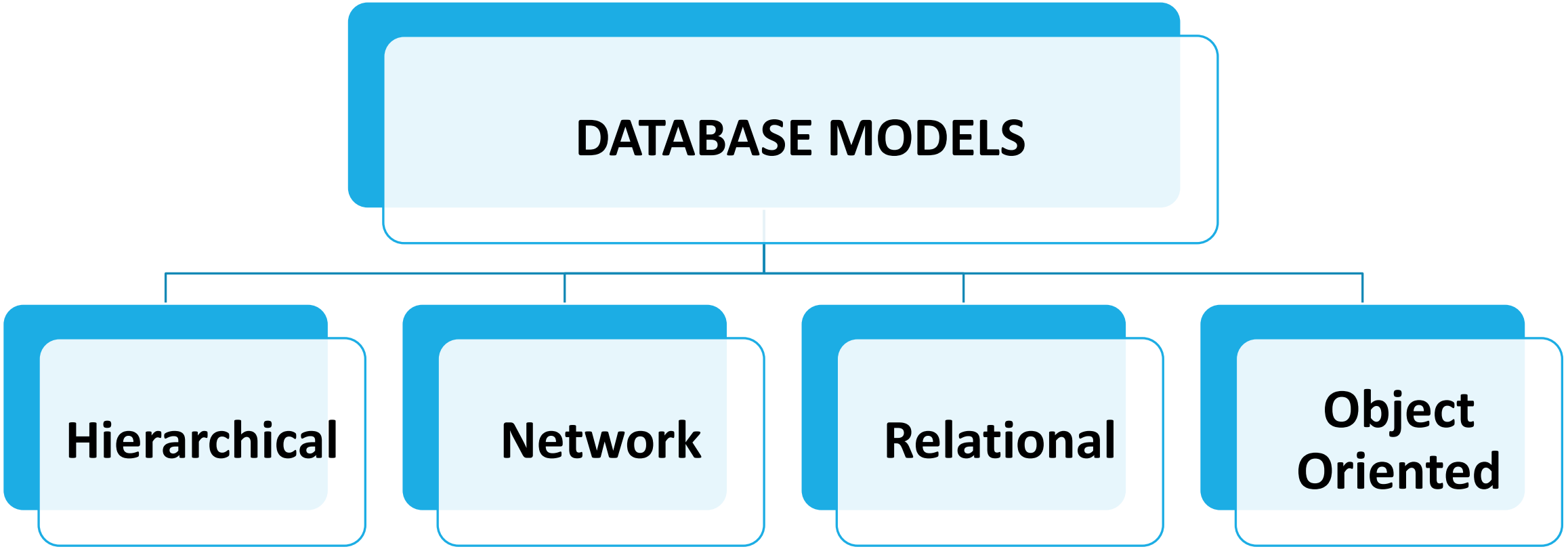


ADVANTAGES

- Permitting Data Sharing
- Minimizing Data Redundancy.
- User-friendly
- Improved security
- Integrity can be maintained

DISADVANTAGES

- Expensive
- Security



HIERARCHICAL DATABASE MODEL

- Records (Nodes) are logically organized into a inverted tree pattern.
- Follows a parent child relationship.
- The top record in the hierarchy that “own” other records is called Parent or Root Record which may have one or more child records

Contd..

- No child record may have more than one parent record.
- Hierarchical data structure implements **one-to-one** and **one-to-many relationships**

ILLUSTRATION

Employee table

EmpNo	First Name	Last Name	Dept. Num
100	Mahwish	Faki	10-L
101	Hamadh	Hashim	10-L
102	darshan	Ar	20-B
103	Chaaya	Sandakelum	20-B

Computer table

Serial Num	Type	User EmpNo
3009734-4	Computer	100
3-23-283742	Monitor	100
2-22-723423	Monitor	100
232342	Printer	100

OBJECT ORIENTED DATA BASE MODEL

- Modeled in terms of objects and their interactions.
- An **Object- Oriented Database** provides a mechanism to store complex data such as images, audio and video, etc.
- An object-oriented database (also referred to as Object-Oriented Database Management System or OODBMS) is a set of objects.

Contd..

- In these databases, the data is modeled and created as objects.
- OODBMS helps programmers make objects which are an independently functioning application or program, assigned with a specific task or role to perform

MCQ Time!

Q. IBM Information Management system which used a hierarchical database model was previously used by Finsys Systems. Which type of relationship is not supported by such database model?

a) One to one

b) Many to one

c) One to many

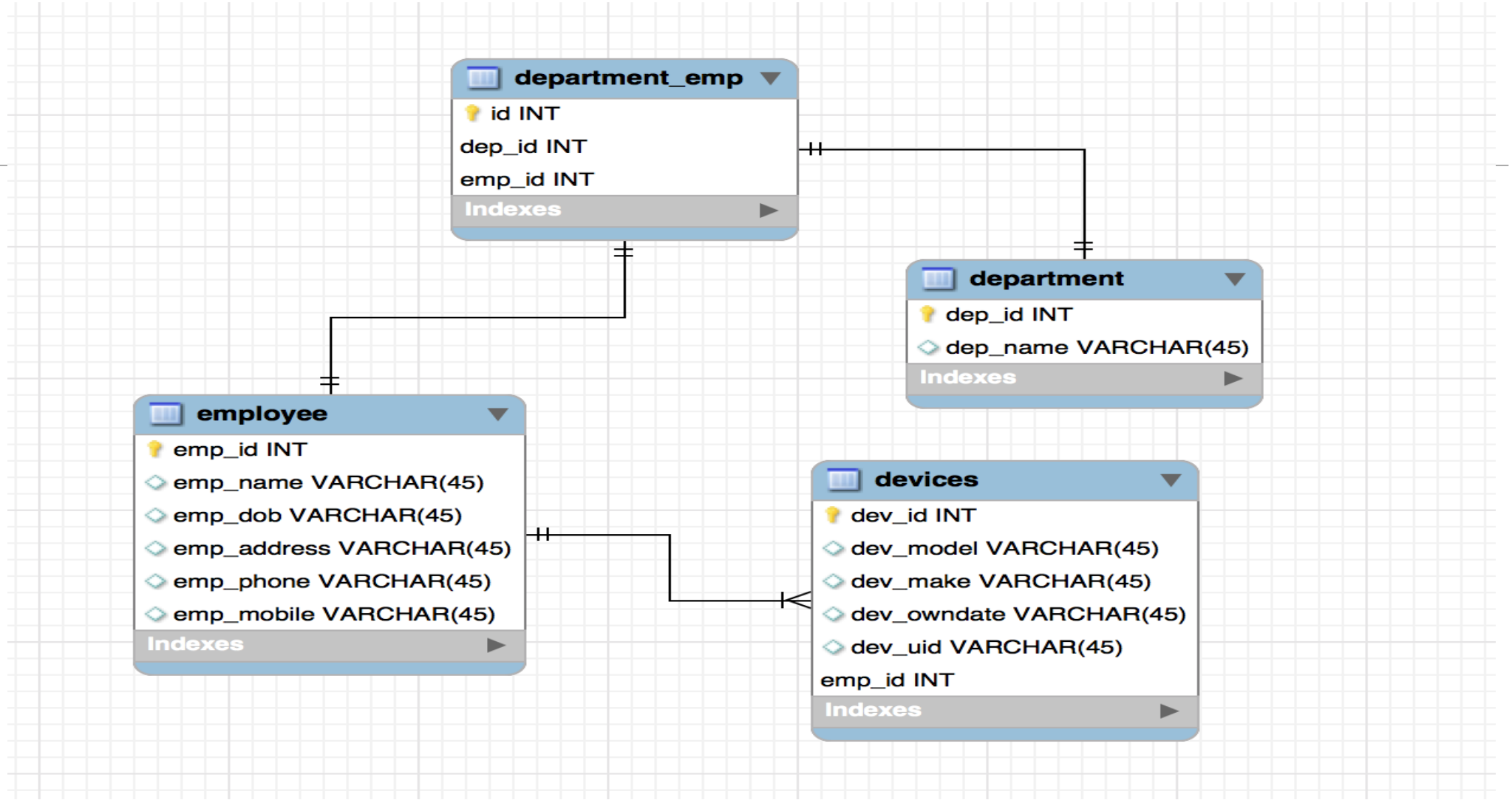
d) None of the above

RELATIONAL DATABASE MODEL

- This model organizes data into one or more Tables.
- A table is a collection of records and fields.
- A unique key identifies each row called as primary key.
- Keys are commonly used to join or combine data from two or more tables.

Contd..

- **Relations:** A relation is a table with columns and rows.
- **Attributes:** The named columns of the relation are called attributes (fields); and
- **Domains:** It is the set of values the attributes can take.



MCQ Time!

Q. Which among the following database models makes use of independently functioning application or program, to perform specific task ?

a) Relational database models

b) Network database Model

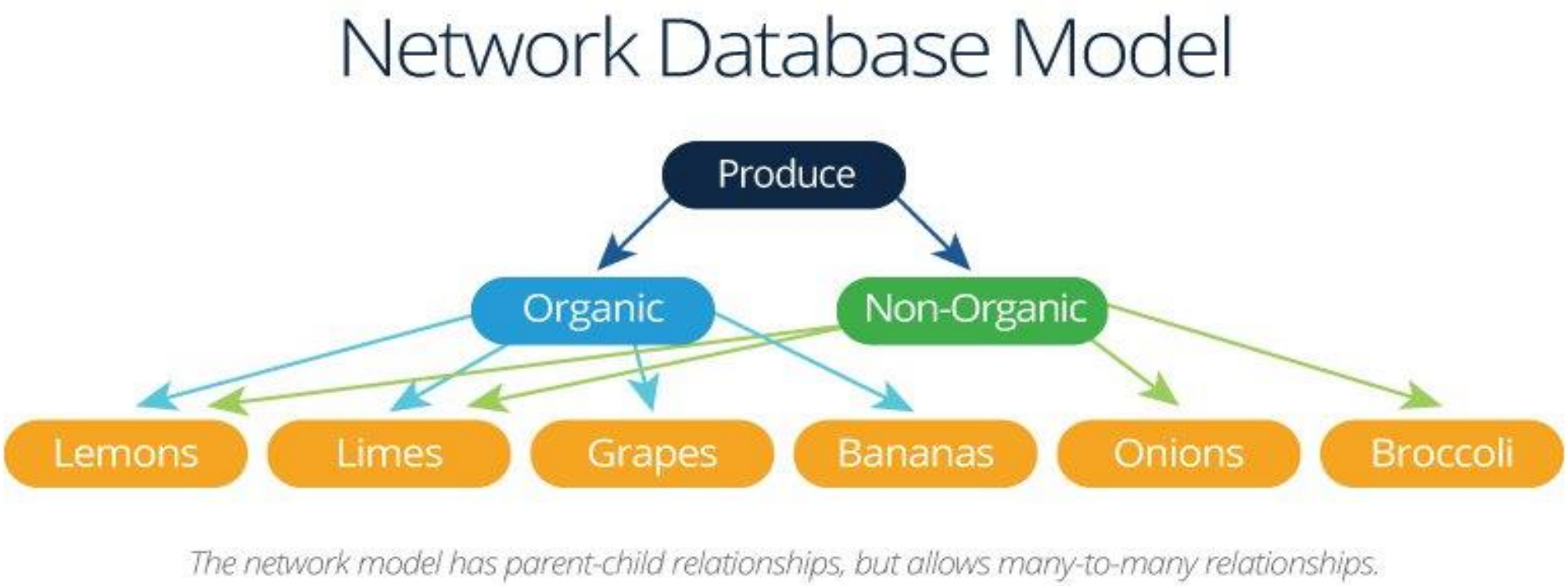
c) Hierarchical Model

d) Object Database Model

NETWORK DATABASE MODEL

- The network model is a variation of the hierarchical model
- Here , the branches can be connected to multiple nodes.
- A network database structure views all records in sets.
- Each set is composed of an owner record and one or more member records.
- Allows the network model to implement the many-to-one and the many-to-many relationship types.

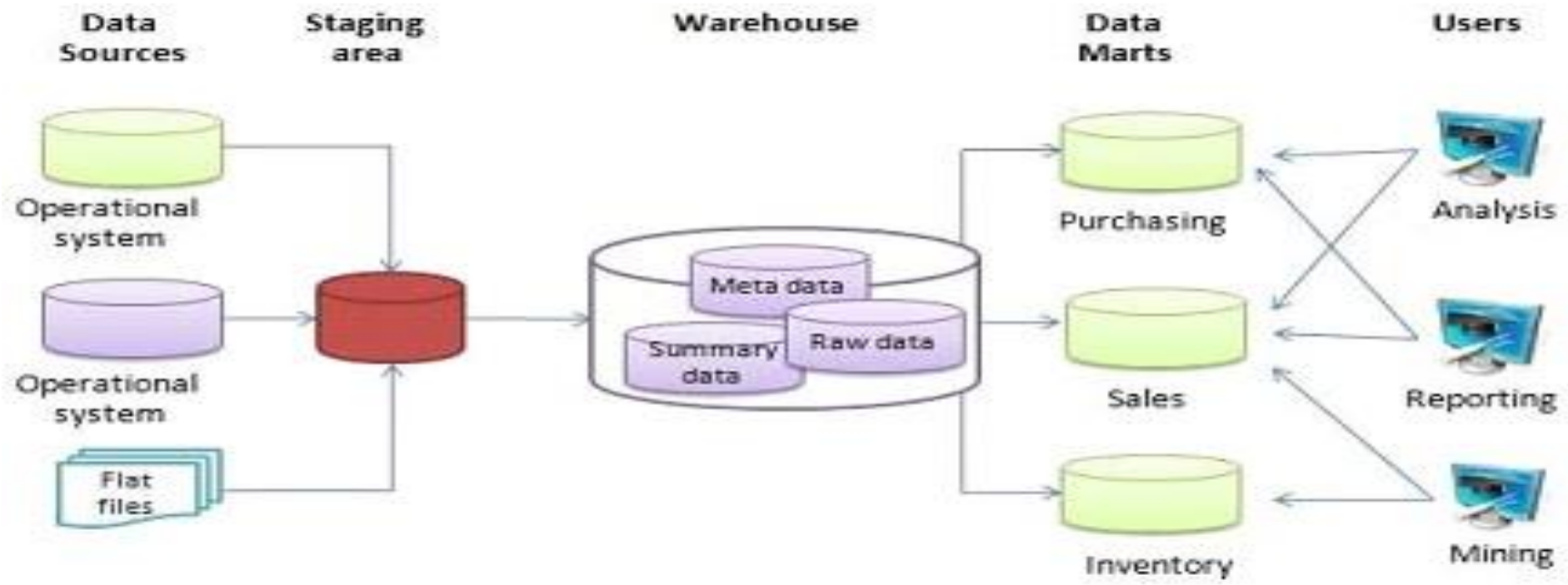
ILLUSTRATION



WHAT IS A DATAWAREHOUSE ?

- Huge repository of data.
- Information systems used for storing historical data.
- Pulls data from different sources within an organization.
- Mainly used for analysis and reporting purposes.
- Assists in business decision making.

ILLUSTRATION



DIFFERENCE BETWEEN A DATABASE AND DATAWAREHOUSE

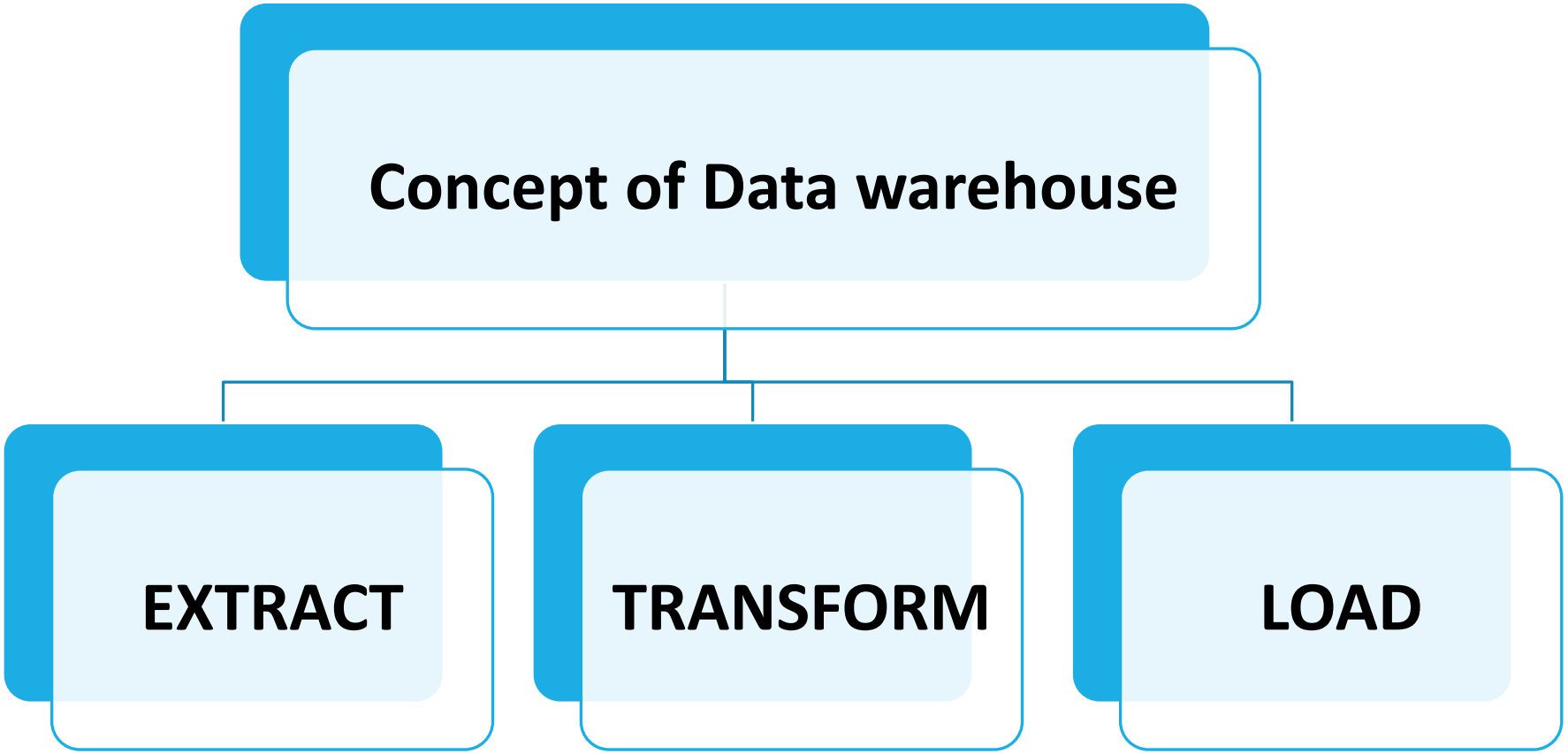
DATABASE

- Stores current real time information.
- Uses OLTP
- Function is to record .

DATAWAREHOUSE

- Stores non operational data.
- Uses OLAP.
- Function is to report, analyze.

PROCESS INVOLVED



- **EXTRACT** – Extracting data from one or more active databases of the organization.

  Loading the extracted data to a temporary area called as Staging area.

- **TRANSFORM** - Perform necessary operations, data edits, to make the extracted data standardized .

- **LOAD** – Load the data after necessary transformations to the data warehouse for storage and analysis.

DESIGNING A DATA WAREHOUSE

Different approaches of designing a data warehouse.

1) **Top down Approach** – Creating an enterprise wide data warehouse and creating data marts as per the need.
2) **Bottom up Approach** – Creating small data mart and combining to form a data warehouse.

CHARACTERISTICS OF A DATAWAREHOUSE

- Time variant
- Non operational
- Standardized

ADVANTAGES OF A DATAWAREHOUSE

- Helps to understand the data better by providing new information and analysis.
- Creates a historical record of data.
- Provides a centralized view of data across the whole enterprise.
- Helps to generate one version of truth by providing consistent information.

MCQ Time!

Q. During the discussions relating to implementation of data warehouse , Finsys Systems is quite apprehensive of whether comparisons could be made between different time period information. Which feature of a data warehouse makes this possible ?

a) Non operational Data

b) Standardization

c) Time Variant

d) All of the above

DATA MINING

Process of analyzing data to find :

- Previously unknown trends
- Patterns
- Associations to make decisions.

- Generally, data mining is accomplished through automated means against extremely large data sets, such as a data warehouse.

STEPS INVOLVED

The steps involved in the Data Mining process are as follows:

Data Integration

Data Selection

Data Cleaning

Data Transformation

Data Mining

Pattern Evaluation and Knowledge Presentation

Decisions Making

BIG DATA

- The term refers to such massively large data sets that conventional database tools do not have the storage, processing power to analyze them.
- Some examples of industries that use big data analytics include the hospitality industry, healthcare companies, public service agencies, and retail businesses.

Benefits of Big Data Processing

- Ability to process Big Data brings in multiple benefits, such as-
  - Businesses can utilize outside **intelligence** while taking decisions.
  - **Access to social data** from search engines to fine tune their business strategies.
  - **Early identification** of risk to the product/services.

Contd..

- Improved customer service
  - Big Data and natural language processing technologies are being used **to read and evaluate consumer responses**.
- Better operational efficiency
  - Integration of Big Data technologies and data warehouse helps an organization **to offload infrequently accessed data**, this leading to better operational efficiency.

COMPARISON

DATABASE	DATA WAREHOUSE	DATA MINING
This stores real time information.	This stores both the historic and transactional data.	This analyses data to find previously unknown trends.
Its function is to record.	Its function is to report and analyze.	Its function is to extract useful data.
Examples include MySQL, MS Access.	Examples include Teradata, Informatica.	Examples include R-Language, Oracle data mining.

MCQ Time!

Q. As the business of Finsys Systems have grown tremendously over the past few years , it was found that SQL Server DBMS does not have the processing power to analyze such massive large datasets. Which is best recommended in this situation.

a) Data warehousing

b) Big Data

c) Data Mining

d) Business Intelligence

NETWORKING AND COMMUNICATION SYSTEMS

- Combination of both hardware and software.
- Connects the various hardware's and transfers the data from one physical location to another.
- Used for exchange of data among different computers .
- To share the resources like CPU, I/O devices, storages, etc. without much of an impact on individual systems.
- Each component, namely the computer in a computer network is called a ‘Node’

SOFTWARE

- Operating System Software
- Application Software

FEATURES OF OS

- Performing hardware functions
- User Interfaces
- Hardware Independence
- Memory Management
- Task Management
- Networking Capability
- Logical Access Security
- File management

FEATURES OF APPLICATION SOFTWARE

- Addressing User needs
- Addressing control against virus
- Providing regular updates

MCQ Time!

Q. Major application software's are also installed in these systems as a part of system configuration. Which among the following is not a function of such application software's?

a) Addressing User needs

b) Addressing control against virus

c) Providing regular updates

d) Task management

NETWORK

A network is a group of devices connected to each other.

Computer Network is a collection of computers and other hardware interconnected by communication channels that allow sharing of resources and information

NETWORK TYPES

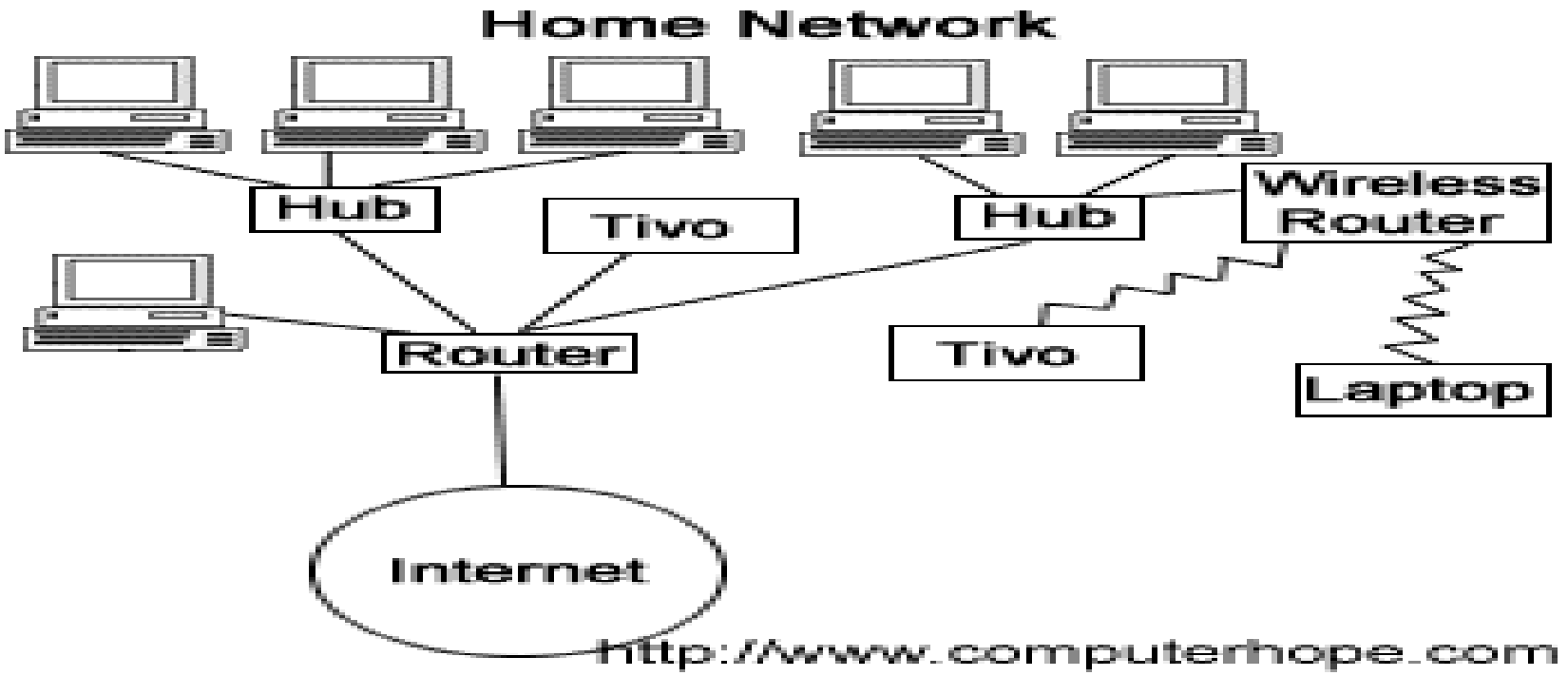
Connection Oriented networks: Wherein a connection is first established between the sender and the receiver and then data is exchanged

Connectionless Networks: Where no prior connection is made before data exchanges. Data which is being exchanged in fact has a complete contact information of recipient and at each intermediate destination, it is decided how to proceed further

ISSUES ADDRESSED

- **Routing:** It refers to the process of deciding on how to communicate the data from source to destination in a network.
- **Bandwidth:** It refers to the amount of data which can be sent across a network in given time.

ILLUSTRATION

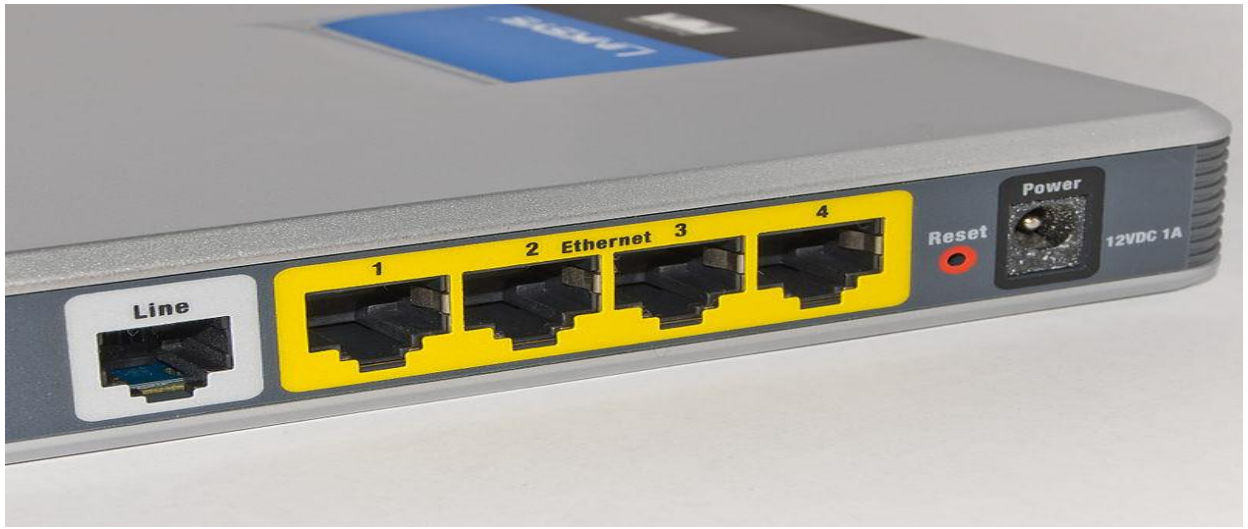


Contd..

- **Resilience:** It refers to the ability of a network to recover from any kind of error like connection failure, loss of data etc.

- **Contention:** It refers to the situation that arises when there is a conflict for some common resource in a network. For example, network contention could arise when two or more computer systems try to communicate at the same time.

ILLUSTRATION



ADVANTAGES

- **Distributed nature of information**
- **Resource Sharing**
- **Computational Power**
- **Reliability**
- **User communication**
- An increase in the efficiency of operations
- Improvements in the effectiveness of management
- Innovations in the marketplace.

HOW IT ACHIEVES

Time compression: Telecommunications enable a firm to transmit raw data and information quickly and accurately between remote sites.

Overcoming geographical dispersion: Telecommunications enable an organization with geographically remote sites to function, to a degree, as though these sites were a single unit. The firm can then reap benefits of scale and scope which would otherwise be unobtainable.

Restructuring business relationships: Telecommunications make it possible to create systems which restructure the interactions of people within a firm

MCQ Time!

Q. Ability of a network to recover from any kind of error like connection failure, loss of data etc is referred to as

a) Bandwidth

b) Routing

c) Contention

d) Resilience

RECAP

- INFORMATION SYSTEM
- Components of IS
- PEOPLE
- HARDWARE
- SOFTWARE
- NETWORK
- DATA
- DATA,DATABASE,DBMS,DATAWAREHOUSE
- BIG DATA,DATA MINING

INFORMATION MANAGEMENT

- Every enterprise needs to manage its information in an appropriate and desired manner. The enterprise must do the following for this:
- Knowing its information needs;
- Acquiring that information;
- Organizing that information in a meaningful way;
- Assuring information quality; and
- Providing software tools so that users in the enterprise can access information they require.

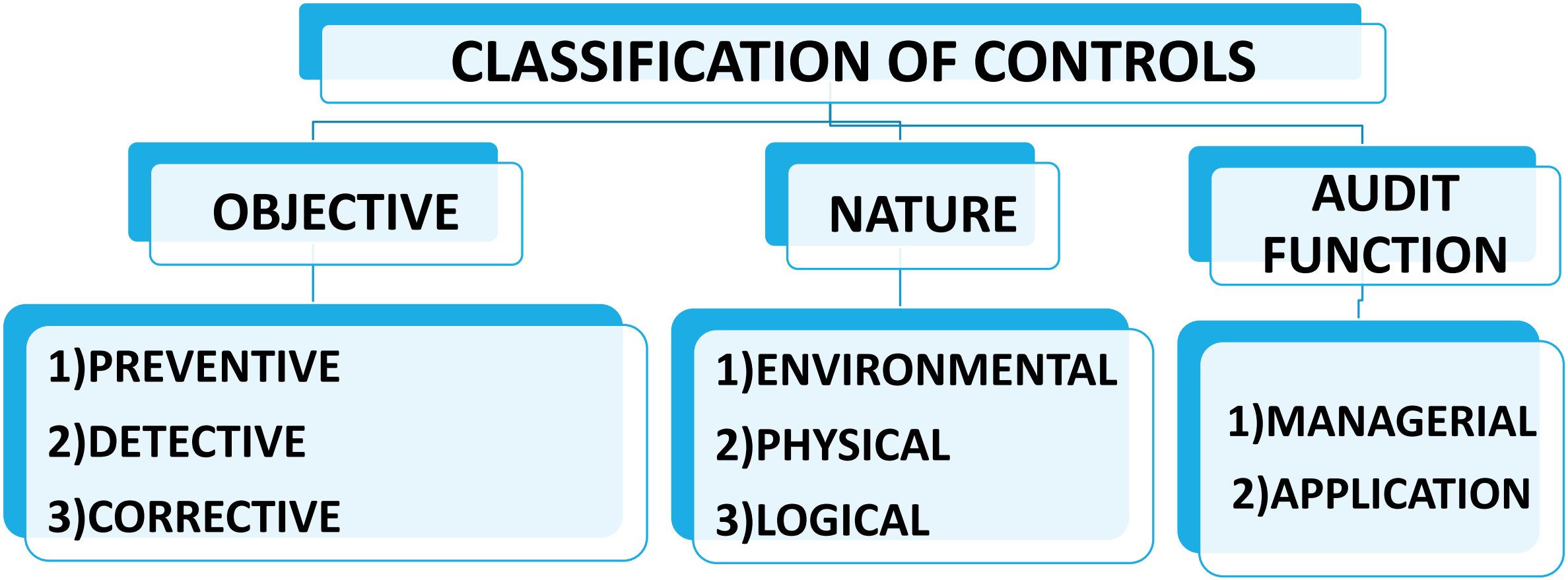
INFORMATION SYSTEM CONTROLS

Some of the critical control lacking in a computerized environment are as follows:

- Lack of management understanding of IS risks and related controls;
- Absence or inadequate IS control framework;
- Absence of weak general controls and IS controls;

Contd..

- Lack of awareness and knowledge of IS risks and controls amongst the business users/ IT staff
- Complexity of implementation of controls in distributed computing environments and extended enterprises
- Lack of control features or their implementation in highly technology driven environments;
- Inappropriate technology implementations or inadequate security functionality in technologies implemented.



PREVENTIVE CONTROLS

These controls **prevent errors, omissions, or security incidents, malicious act from occurring** and can be implemented in both manual and computerized environment . They include:

- Data-entry edits
- Access controls
- Anti-virus software,

Contd..

- Firewalls
- Intrusion prevention systems.
- Training and retraining of staff
- Segregation of duties

DETECTIVE CONTROLS

- Designed to **detect errors, omissions or malicious acts that occur** and report the occurrence.
- Detect errors or incidents that elude preventive controls. They include :

1)Flagging

2)Monitoring activities

3)Reviews and Surprise checks

Contd..

4)Hash totals

5)Intrusion detection system

6) Reconciliations

7)Clear understanding of lawful activities and noting the deviations.

8)Mechanism to refer the reported unlawful activities .

9)Interaction with the preventive control

ILLUSTRATION

Worker ID : 0172 Surname : Ridyard Week Number : 12 Hours Worked : 43	Worker ID : 9023 Surname : Haughton Week Number : 12 Hours Worked : 22.5	Worker ID: 2652 Surname : Ip Week Number : 12 Hours Worked : 37

CASE 1

The batch total would be 3 as there are three documents

- If the field *Hours Worked* was chosen to calculate a hash total then the hash total would be 102.5 as 43+22.5+37=102.5
- If the field *Worker ID* was chosen to calculate a hash total then the hash total would be 11847 as 0172+9023+2652=11847
- The chosen totals would be calculated manually by the user before the data was entered. Probably only one total would be used.

CASE 2

- Now suppose that the data was entered but by mistake the user missed out the middle document.

The computer calculated batch total would be 2.

If the field *Hours Worked* was chosen to calculate a hash total then the computer calculated hash total would be 80 as 43+37=80

If the field *Worker ID* was chosen to calculate a hash total then the computer calculated hash total would be 2824 as 0172+2652=2824

CASE 3

Suppose instead that the user missed out the middle document but entered the last document twice. The computer calculated totals would then be :

Computer batch total is 3.

Computer hash total on *Hours Worked* is 117 as 43+37+37=117.

Computer hash total on *Worker ID* is 5476 as 0172+2652+2652=5476.

CORRECTIVE CONTROLS

- Designed to **Correct errors, omissions, or incidents once they have been detected.**
- Reduce the impact or correct an error once it has been detected.

They include:

1)Default dates

2) Changes to IT access lists

3)Corrective entries

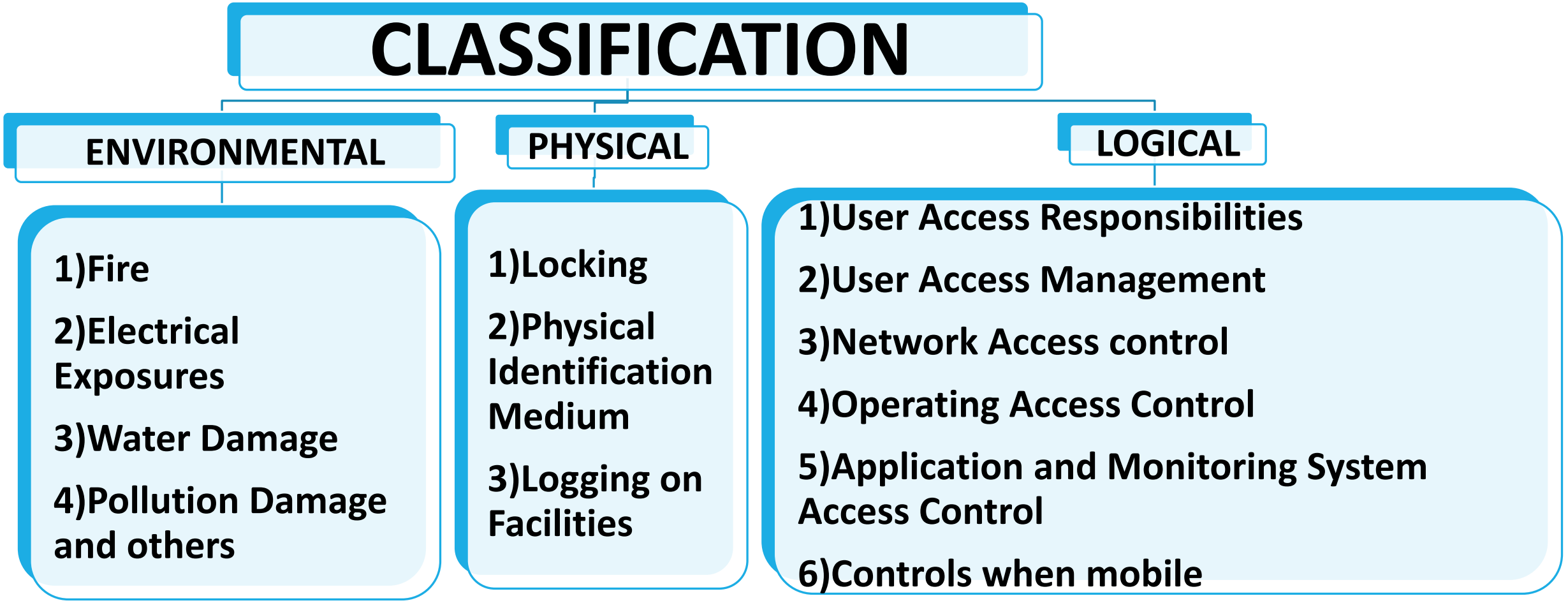
4)Rerun Procedures

5)Back up procedures

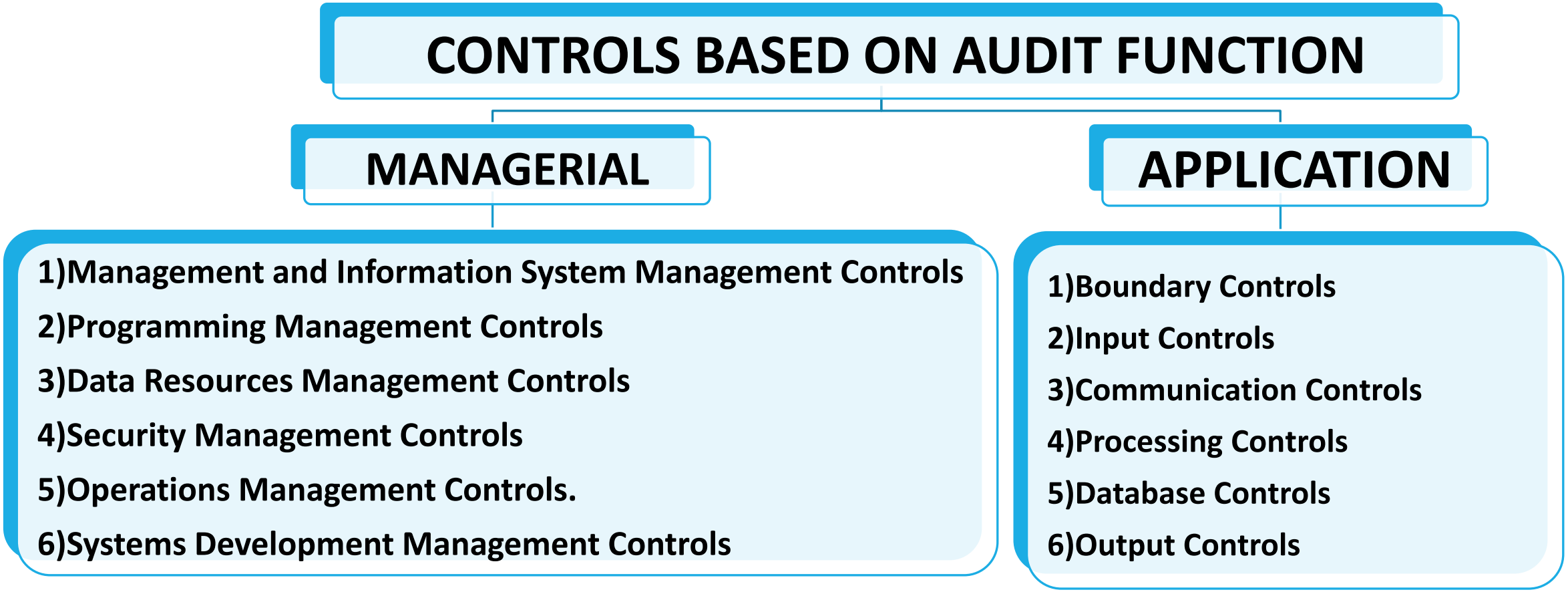
MAIN CHARACTERISTICS

- Minimizing the impact of the threat
- Identifying the cause of the problem
- Providing Remedy to the problems discovered by detective controls
- Getting feedback from preventive and detective controls
- Correcting error arising from a problem
- Modifying the processing systems to minimize future occurrences of the incidents.

CLASSIFICATION BASED ON "NATURE OF INFORMATION SYSTEM RESOURCES"



CONTROLS BASED ON AUDIT FUNCTION



ENVIRONMENTAL CONTROLS

- These are the controls relating to IT environment such as power, air-conditioning, Uninterrupted Power Supply (UPS), smoke detection, fire-extinguishers, dehumidifiers.
- Provide protection against environmental exposures related to Fire, Electrical Exposures, Water Damage, and Pollution damage and others.

FIRE

Automatic and manual fire alarms.

Manual fire extinguishers can be placed at strategic locations.

Fire exits should be clearly marked

Fire alarms

When a fire alarm is activated, a signal may be sent automatically to permanently manned station.

Usage awareness among staff members

Documentation of emergency procedures

Less Wood and plastic should be in computer rooms.

Use a gas based fire suppression system.

Regular Inspection by Fire Department should be conducted.

Fire suppression systems should be supplemented and not replaced by smoke detectors.

DESIGN REQUIREMENTS

- To reduce the risk of firing, the location of the computer room should be strategically planned and should not be in the basement or ground floor of a multi-storey building.
- Fireproof Walls, Floors and Ceilings surrounding the Computer Room
- Fire Resistant Office Materials such as waste-baskets, curtains, desks, and cabinets should be used.

ELECTRICAL EXPOSURES

- These include risk of damages that may be caused due **electrical faults, non-availability of electricity, spikes, fluctuations of voltage** and other such risk.

The risk and their controls

1)Power spikes - **Electrical Surge Protectors**

2) Non-availability of electricity - **Un-interruptible Power System (UPS)/Generator**

3)Power /Voltage Fluctuations -**Voltage regulators and circuit breakers**

4) Immediate power shut during fire or an emergency evacuation -**Emergency Power-Off Switch**

WATER DAMAGE

- Water damage to a computer installation can be the outcome of **water pipes burst** and also result from other resources such as **cyclones, tornadoes, floods** etc.

1. Wherever possible have waterproof ceilings, walls and floors.
2. Ensure an adequate positive drainage system exists;
3. Install alarms at strategic points within the installation
4. Water proofing;
5. Water leakage Alarms.

POLLUTION DAMAGE AND OTHERS

- The major pollutant in a computer installation is dust. Causes permanent damage to data ,write errors and clogs the fans,heat sinks within the system.

They include :

1)Prohibitions against Eating, Drinking and Smoking within the Information Processing Facility

2) Power Leads from Two Substations

PHYSICAL ACCESS CONTROLS

Controls relating to **physical security of the tangible IS resources and intangible resources stored on tangible media .** Physical Exposures includes

1)Abuse of data processing resources;

2)Blackmail;

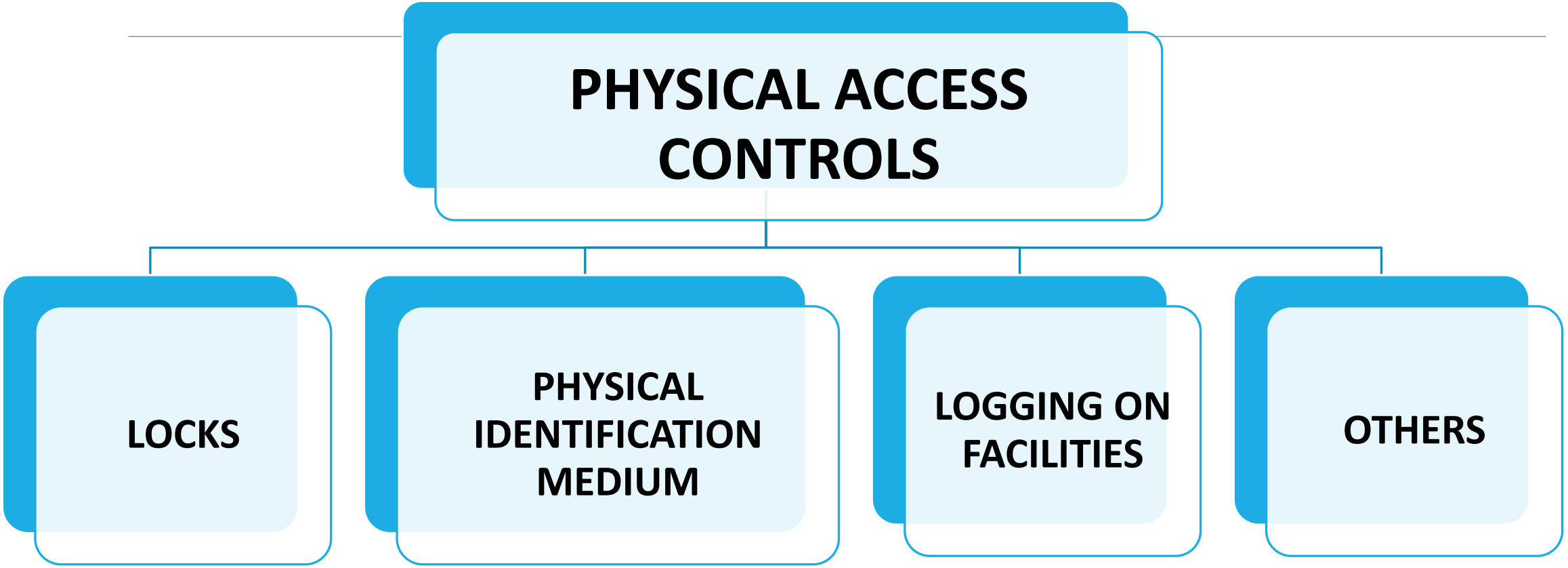
3)Embezzlement

4)Damage

5)Vandalism or theft to equipment's or documents

6)Public disclosure of sensitive information

7)Unauthorized entry



LOCKS ON DOORS

- **Cipher locks (Combination Door Locks)** - Cipher locks are used in low security situations or when many entrances and exits must be usable all the time. To enter, a person presses a four-digit number, and the door will unlock for a predetermined period, usually ten to thirty seconds.

Contd..

- **Bolting Door Locks** – A special metal key is used to gain entry when the lock is a bolting door lock. To avoid illegal entry, the keys should not be duplicated.
- **Electronic Door Locks** – A magnetic or embedded chip-based plastics card key or token may be entered a reader to gain access in these systems.

orbita

PHYSICAL IDENTIFICATION MEDIUM

1) Personal Identification Numbers (PIN):

- A secret number will be assigned to the individual, serves to verify the authenticity of the individual.
- The visitor will be asked to log on by inserting a card in some device and then enter their PIN via a PIN keypad for authentication.
- His/her entry will be matched with the PIN number available in the security database.

Contd..

2) Plastic Cards:

- These cards are used for identification purposes.
- Customers should safeguard their card so that it does not fall into unauthorized hands.

3) Identification Badges:

- Special identification badges can be issued to personnel as well as visitors.
- For easy identification purposes, their color of the badge can be changed. Sophisticated photo IDs can also be utilized as electronic card keys.

LOGGING ON FACILITIES

1) Manual Logging:

All visitors should be prompted to sign a visitor's log indicating their name, company represented, their purpose of visit, and person to see.

Logging may happen at both fronts - reception and entrance to the computer room.

A valid and acceptable identification such as a driver's license, business card or vendor identification tag may also be asked for before allowing entry inside the company.

Contd..

2) Electronic Logging:

This feature is a combination of electronic and biometric security systems.

The users logging can be monitored and the unsuccessful attempts being highlighted.

OTHERS

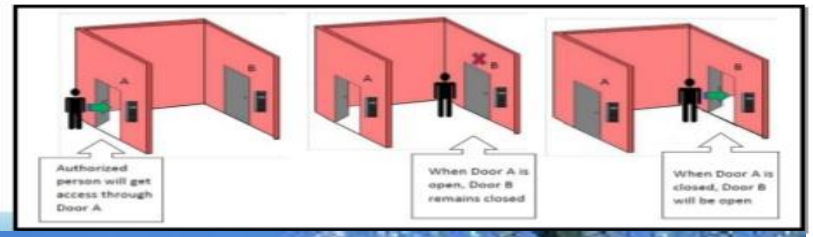
- Video Cameras
- Security Guards
- Controlled Visitor Access
- Bonded Personnel
- Dead Man Doors
- Non–exposure of Sensitive Facilities

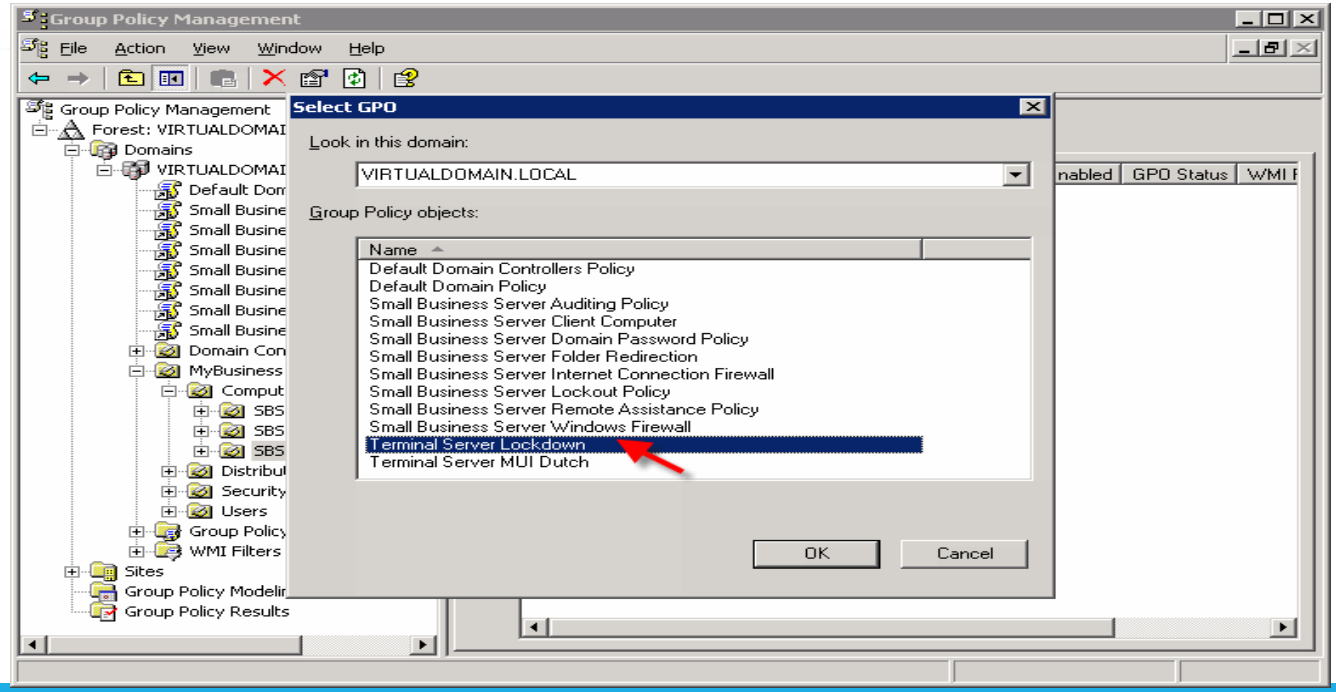
Contd..

- Computer Terminal Locks
- Controlled Single Entry Point
- Alarm System
- Perimeter Fencing
- Control of out of hours of employee-employees
- Secured Report/Document Distribution Cart

Man-Trap

- Useful for Multiple Doors, Arranged in a Sequence
- Regulate Opening and Closing of Doors
- Second Door will Open only After First Door has Closed
- Manage Traffic and Control Dust and Heat
- Useful to Restrict Intruder from Escaping the Premises Quickly
- *Mantrap wait & Door Pulse timer limit is 65535 seconds.*





LOGICAL ACCESS CONTROLS

- Logical access controls are the system-based mechanisms .
- Used to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted.

Logical access controls are implemented to

1. Ensure that access to systems, data and programs is restricted to authorized users.
2. To safeguard information against unauthorized use, disclosure or modification, damage or loss.
3. To mainly deal with security, confidentiality and privacy requirements , incident handling aspects etc.

TECHNICAL EXPOSURES

- Data diddling
- Bombs
- Christmas Card
- Worm

Contd..

- Rounding Down
- Salami Techniques
- Trap Doors
- Spoofing

ASYNCHRONOUS ATTACKS

They occur in many environments where data can be moved synchronously across telecommunication lines.

Data that is waiting to be transmitted are liable to unauthorized access called **Asynchronous Attack**.

TYPES OF ASYNCHRONOUS ATTACKS

1) Subversive Attacks
2) Data Leakage
3) Wire Tapping
4) Piggy Backing

MCQ Time!

Q. In Gakewell Ltd the data security breach happened by duplicating the login procedure, and capturing the user's password. Such type of an attack involving forging one's source address is known as ?

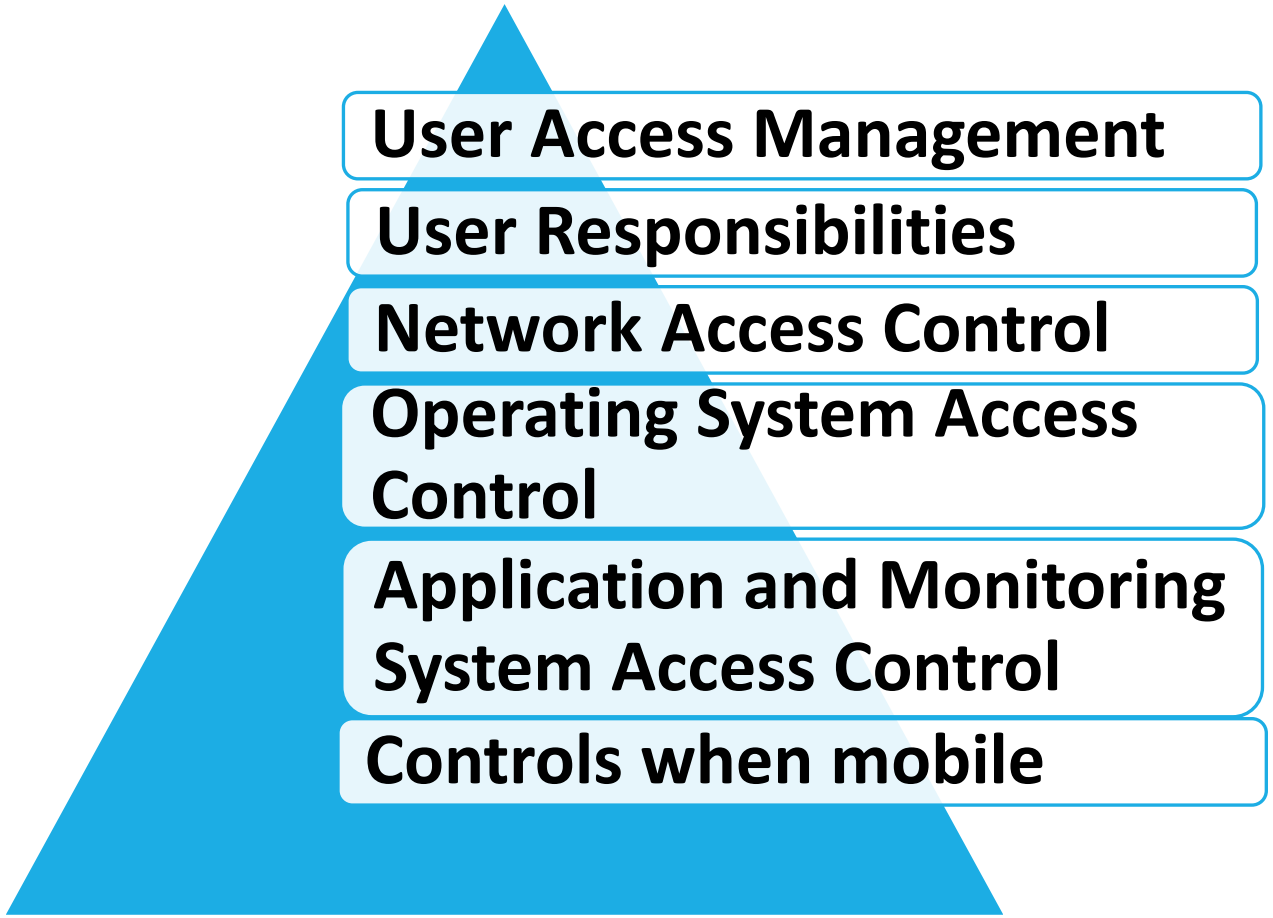
i) Worms

ii) Data Diddling

iii) Spoofing

iv)Salami Technique

LOGICAL ACCESS CONTROLS



USER ACCESS MANAGEMENT

- **User Registration**: Information about every user is documented.
- **Privilege management**: Minimal access privileges are given and is aligned with job requirements and responsibilities.

Contd..

- **User password management**: Involves allocations, storage, revocation, and reissue of password ,educating users about passwords, and making them responsible for their password.
- **Review of user access rights**: Involves periodic review of access rights to check anomalies in the user's current job profile, and the privileges granted earlier.

USER RESPONSIBILITIES

- **Password use:** Mandatory use of strong passwords to maintain confidentiality.
- **Unattended user equipment:** Users should ensure that none of the equipment under their responsibility is ever left unprotected. They should also secure their PCs with a password and should not leave it accessible to others.

MCQ Time!

Q. Gakewell Ltd has made its Privilege management policy more stringent so as to prevent unauthorized users gaining entry and minimum entry is given only as per their job requirement. Privilege management falls under which of the following controls ?

i) Operating System Control

ii) Network Access Controls

iii) User Access controls

iv) Application and Monitoring System control

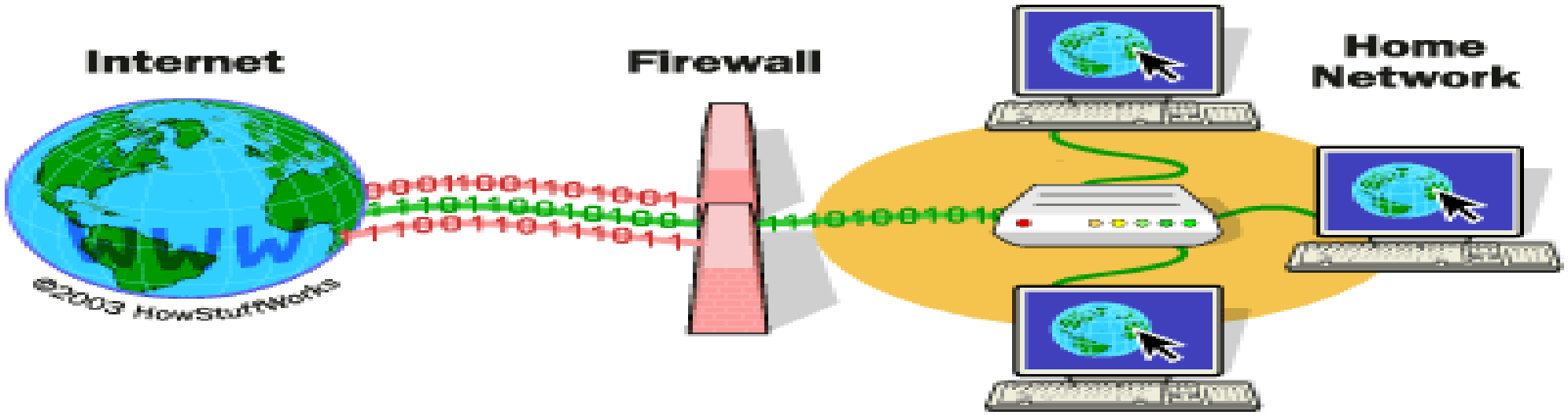
NETWORK ACCESS CONTROL

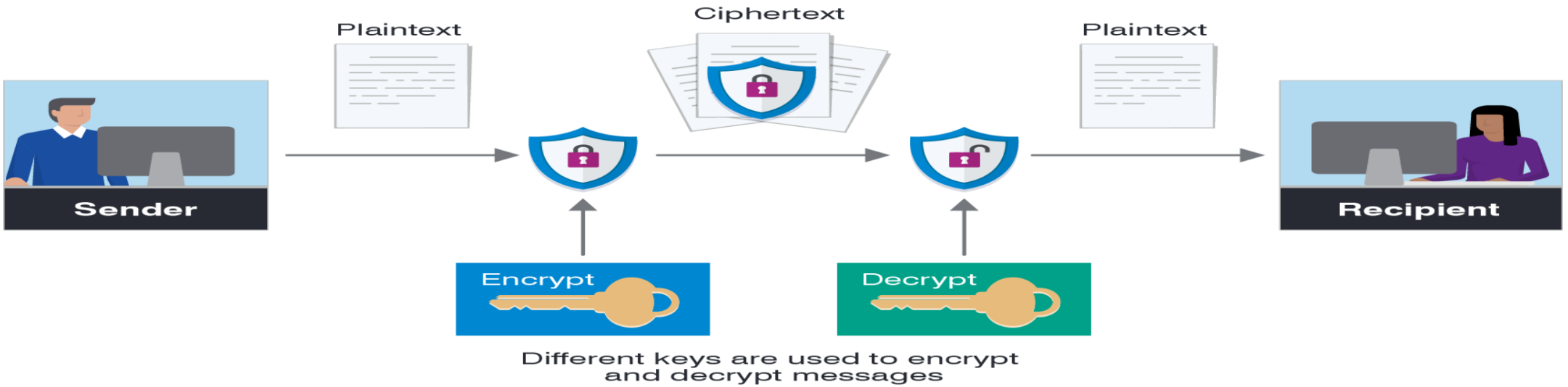
An Internet connection exposes an organization to the harmful elements of the outside world.

The protection can be achieved through the following means:

- Policy on use of network services
- Enforced path
- Segregation of networks

- 4)Network connection and routing control
- 5) Security of network services
- Firewall
- Encryption
- Call Back Devices





MCQ Time!

Q. Based on the risk assessment by the audit team, internet access by the employees was routed through a firewall and proxy. This is referred to as

i)Encryption

ii)Enforced Path

iii)Call Back Devices

iv)None of these

OPERATING SYSTEM ACCESS CONTROL

- Automated terminal identification
- Terminal log-in procedures
- Access Token
- Access Control List

Contd..

- Discretionary Access Control
- User identification and authentication
- Password management system
- Use of system utilities
- Duress alarm to safeguard users
- Terminal time out
- Limitation of connection time

MCQ Time!

Q. Gakewell Ltd also implemented controls to log out the respective user if the terminal is inactive for a defined period. This is known as

i)Terminal Identification

ii) Terminal log in

iii)Terminal time out

iv) Access token

APPLICATION AND MONITORING SYSTEM ACCESS CONTROL

They constitute the following :

1)Information Access restriction
2)Sensitive System isolation
3)Event logging
4)Monitor System use
5)Clock Synchronization

CONTROLS WHEN MOBILE

- As computing facility is not restricted to a certain data center alone , theft of data carried on the disk drives of portable computers is a high-risk factor.
- Both physical and logical access to these systems is critical.
- Information is to be encrypted and access identifications like fingerprint, eye-iris, and smart cards are necessary security features.

MCQ Time!

Q. Gakewell Ltd has made it their routine procedure to check the activity logs generated by the system on hourly basis. Which amongst the following does event logging fall under?

i) Application and Monitoring System control

ii) Operating System Control

iii) Network Access Controls

iv)User Access controls

CLASSIFICATION BASED ON AUDIT FUNCTION

MANAGERIAL CONTROLS

1)Top Management and Information Systems Management Controls

2)Systems Development Management Controls

3)Programming Management Controls

4)Data Resource Management Controls

5)Quality Assurance Management Controls

6)Security Management Controls

7)BCP Controls

8)Operations Management Controls

APPLICATION CONTROLS

1)Boundary Controls

2)Input Controls

3)Communication Controls

4)Processing Controls

5)Database Controls

6)Output Controls

MANAGERIAL CONTROLS

- It is performed to ensure the development, implementation, operation and maintenance of information systems in a planned and controlled manner in an organization.
- The controls at this level provide a stable infrastructure in which information systems can be built, operated, and maintained.

TOP_MANAGEMENT AND INFORMATION SYSTEMS MANAGEMENT CONTROLS

- The controls adapted by the management of an enterprise are to ensure that the information systems function correctly and they meet the strategic business objectives.
- The scope of control here includes framing high-level IT policies, procedures and standards ,sound internal controls framework within the organization.

Contd..

- Top management is responsible for preparing a master plan for the information systems function
- The major functions that a senior manager must perform are **Planning, Organizing, Leading and Controlling.**

PLANNING

Strategic Planning

Operational Planning

ORGANIZING

Resource Allocation

Staffing

LEADING

- Motivation ,guidance , communication
- Achieve harmony of its objectives

CONTROLLING

- Performance monitoring
- Corrective actions

SYSTEMS DEVELOPMENT MANAGEMENT CONTROLS

System development controls are targeted to ensure that proper documentations and authorizations are available for each phase of the system development process.

It includes controls at controlling new system development activities.

The activities deal with system development controls in IT

- System Authorization Activities
- User Specification Activities

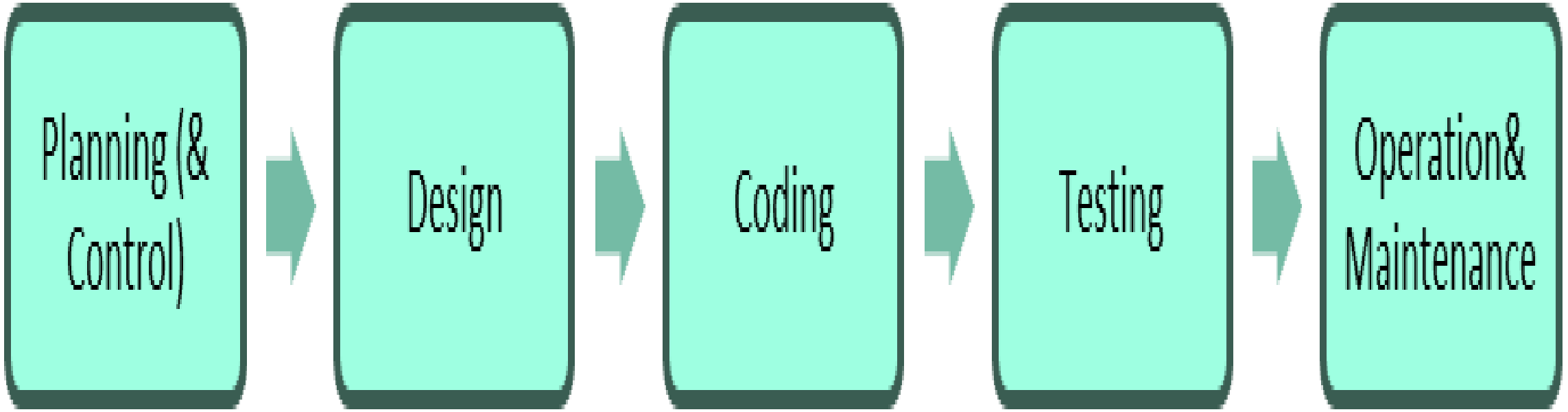
Contd..

- Technical Design Activities
- Internal Auditor’s Participation
- Program Testing
- User Test and Acceptance Procedures

PROGRAMMING MANAGEMENT CONTROLS

- The primary objectives of this phase are to produce or acquire and to implement high-quality programs.
- The Control phase runs in parallel for all other phases during software development or acquisition .
- It monitors progress against plan and to ensure software released for production use is authentic, accurate, and complete.

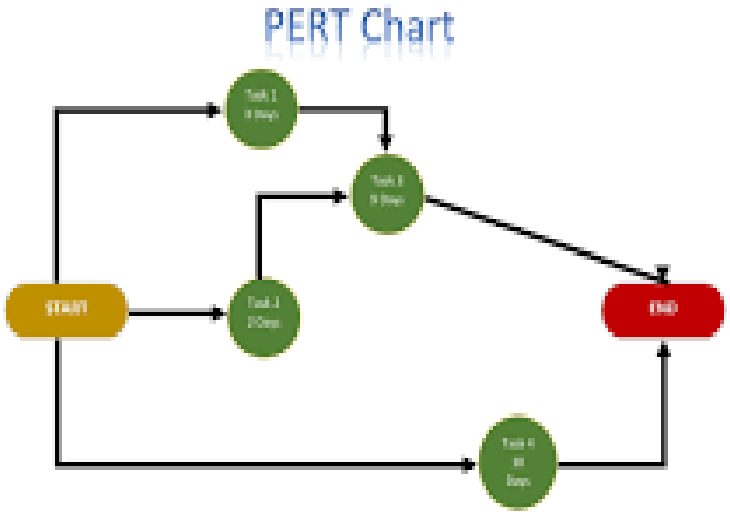
MAIN PHASES



ILLUSTRATION

Gantt Chart

Task Name	Q1 2019			Q2 2019		Q3 2019
	Jan 19	Feb 19	Mar 19	Apr 19	Jun 19	Jul 19
Planning						
Research						
Design						
Implementation						
Follow up						



DATA RESOURCE MANAGEMENT CONTROLS

For data to be managed better :

1)Users must be able to share data

2)Data must be available to users when it is needed,

3)In the location and in the form it is needed.

4) Modify data easily and the integrity of the data be preserved.

Contd..

- If data repository system is used properly, it can enhance data and application system reliability.
- Careful control should be exercised over the roles by appointing senior, trustworthy persons, separating duties to the extent possible.
- Maintaining and monitoring logs of the data administrator's and database administrator's activities should also be carried out.

MCQ Time!

Q. Prior to implementation of controls, Gakewell Ltd faced a security issue where it involved change of data before they were entered in to the system. This type of technical exposure is referred to as

i) Worms

ii) Data Diddling

iii) Spoofing

iv)Salami Technique

QUALITY ASSURANCE MANAGEMENT CONTROLS

Quality Assurance management is concerned with ensuring that :

- Information systems produced achieve certain quality goals.
- Development, implementation, operation and maintenance of Information systems comply with a set of quality standards.
- Quality Assurance (QA) personnel should work to improve the quality of information systems produced, implemented, operated, and maintained in an organization.

Contd..

They perform a monitoring role for management to ensure that:

1)Quality goals are established and understood clearly by all stakeholders; and

2)Compliance occurs with the standards that are in place to attain quality information systems.

SECURITY MANAGEMENT CONTROLS

- They make sure that assets are secure and the expected losses that will occur, are at an acceptable level.
- When disaster strikes, it still must be possible to recover operations and mitigate losses using the last resort controls - A Disaster Recovery Plan (DRP) and Insurance.

A comprehensive DRP comprise four parts –

1) Emergency Plan
2) Backup Plan
3) Recovery Plan
4) Test Plan.

Contd..

- The plan lays down the policies, guidelines, and procedures for all Information System personnel.
- Adequate insurance must be able to replace Information Systems assets and to cover the extra costs associated with restoring normal operations.

BCP CONTROLS

- **BCP** refers to **BUSINESS CONTINUITY PLANNING**
- These controls are related to having an operational and tested IT continuity plan, which is in line with the overall business requirements

Contd..

- It makes sure that IT services are available as required and to ensure a minimum impact on business in the event of a major disruption.
- It ensures that the business is able to continue with its critical operations in minimum downtime when a disaster strikes.

OPERATIONS MANAGEMENT CONTROLS

They are responsible for the daily running of hardware and software facilities and performs controls over the functions as below:

- Computer Operations
- Network Operations
- Data Preparation and Entry
- Production Control

Contd..

- File Library
- Documentation and Program Library
- Help Desk/Technical support
- Capacity Planning and Performance Monitoring
- Management of Outsourced Operations

APPLICATION CONTROLS

- Ensure that data remains **complete, accurate and valid** during its input, update and storage.

The different categories are :

- 1)Boundary Controls
- 2)Input Controls

Contd..

- Communication Controls
- Processing Controls
- Database Controls
- Output Controls

BOUNDARY CONTROLS

- Comprises of access control mechanisms .
- Establishes the interface between the **would-be user** of a computer system and the **computer** itself

Contd..

Major boundary Controls Include :

1)Cryptography

2)Passwords

3)PIN

4)Identification Cards

5)Biometric Devices.

INPUT CONTROLS

Controls where input data is validated for authorization, accuracy, reasonableness, completeness, and integrity

Major Input Controls Include :

1)Source Document Controls

2)Data Coding Controls

3)Batch Controls

4)Validation Controls

MCQ Time!

Q. Bianc Computing Ltd has implemented boundary Controls which are access control mechanisms that links the authentic users to the authorized resource , Which of the following is not a boundary control?

i) Cryptography

ii) Personal Identification Numbers

iii) Identification Cards

iv) Hash totals

COMMUNICATION CONTROLS

Some communication controls are as follows:

- **Physical Component Controls:** These controls incorporate features that mitigate the possible effects of exposures.
- **Line Error Control:** Whenever data is transmitted over a communication line, recall that it can be received in error because of attenuation distortion, or noise that occurs on the line. These errors must be detected and corrected.
- **Flow Controls:** Flow controls are needed because two nodes in a network can differ in terms of the rate at which they can send, received, and process data..

Contd..

- **Link Controls:** In Wide Area Network (WAN), line error control and flow control are important functions in the component that manages the link between two nodes in 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.

MCQ Time!

Q. The network engineers of Bianc Computing Ltd has recommended certain controls to bridge the rate of reception and processing between two nodes. Which types of controls are being referred to here?

i)Link Controls

ii)Flow Controls

iii) Channel Access Controls

iv)Line Error Controls

PROCESSING CONTROLS

Some of these controls are as follows:

1) Processor Controls
2) Real Memory Controls
3) Virtual Memory Controls
4) Data Processing Controls

MCQ Time!

Q. The data validation is performed by the developers by using programmed procedures that examine the characters of the data in the field. This type of validation is called as

i)Field interrogation

ii)Record interrogation

iii)File interrogation

iv)None of the above

DATABASE CONTROLS

Protecting the integrity of a database when application software acts as an interface to interact between the user and the database, are called **Update Controls** and **Report Controls**.

- Sequence Check between Transaction and Master Files
- Ensure All Records on Files are processed
- Process multiple transactions for a single record in the correct order

Contd..

- Maintain a suspense account
- Standing Data
- Print-Run-to Run Control Totals
- Print Suspense Account Entries
- Existence/Recovery Controls

OUTPUT CONTROLS

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

Various Output Controls are as follows:

- Storage and Logging of sensitive, critical forms
- Logging of output program executions

Contd..

- Spooling/Queuing
- Controls over printing
- Report Distribution and Collection Controls

INFORMATION SYSTEMS AUDITING

Major objectives are as follows:

1) Asset Safeguarding
2) Data Integrity
3) System Effectiveness
4) System Efficiency

MCQ Time !

Q. Bianc Computing Ltd when dealing with huge volume of data processing uses a control mechanism that maps virtual memory addresses into real memory addresses. This type of controls come under

i) Virtual Memory Controls

ii)Real Memory Controls

iii) Processor Controls

iv) Data Processing Controls

NEED FOR AUDIT OF INFORMATION SYSTEMS

- Organizational Costs of Data Loss
- Cost of Incorrect Decision Making
- Costs of Computer Abuse
- Value of Computer Hardware, Software and Personnel

Contd..

- High Costs of Computer Error
- Maintenance of Privacy
- Controlled evolution of computer Use

ILLUSTRATION
Auditing User Access Controls

- Authentication
- Access Violations
- User Account Lockout
- Intrusion detection and prevention
- Dormant Accounts
- Shared Accounts
- System accounts

TOOLS FOR IS AUDIT

1)Snapshots

2)Integrated Test Facility

3)Audit hooks

4) Continuous and Intermittent Simulation .

5) System Control Audit Review File (SCARF)

MCQ Time!

Q. Which among the following involves a inbuilt audit module to continuously monitor transactions ?

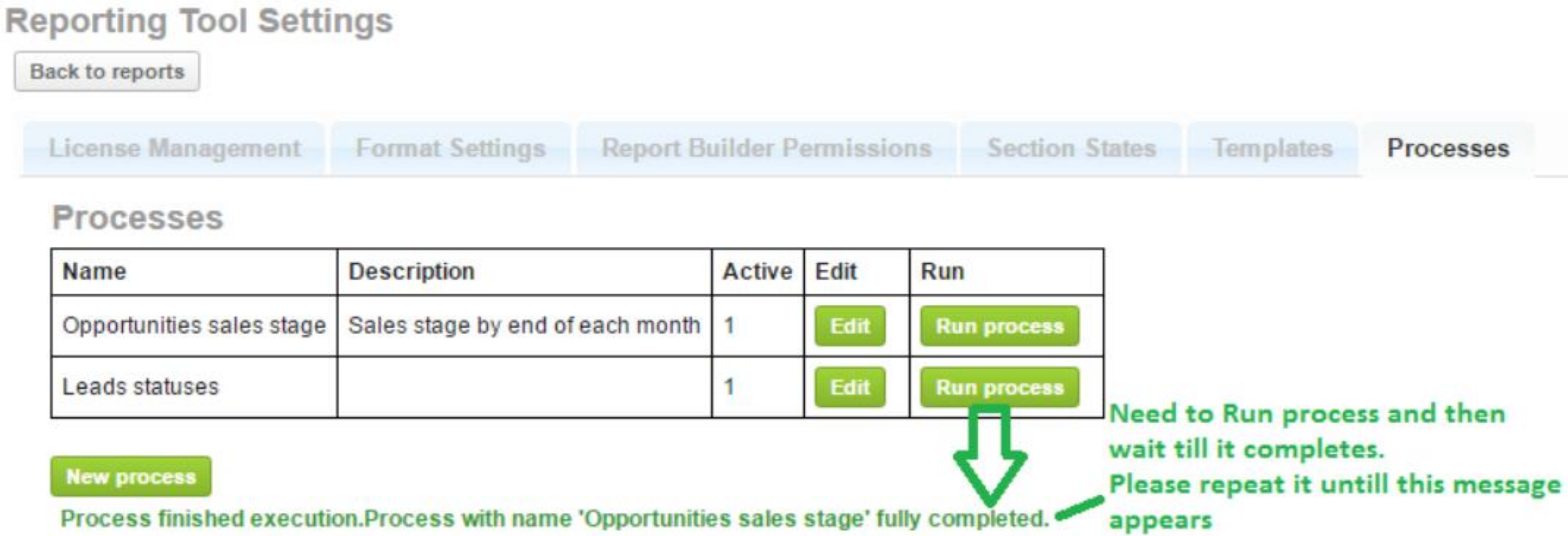
a) CIS

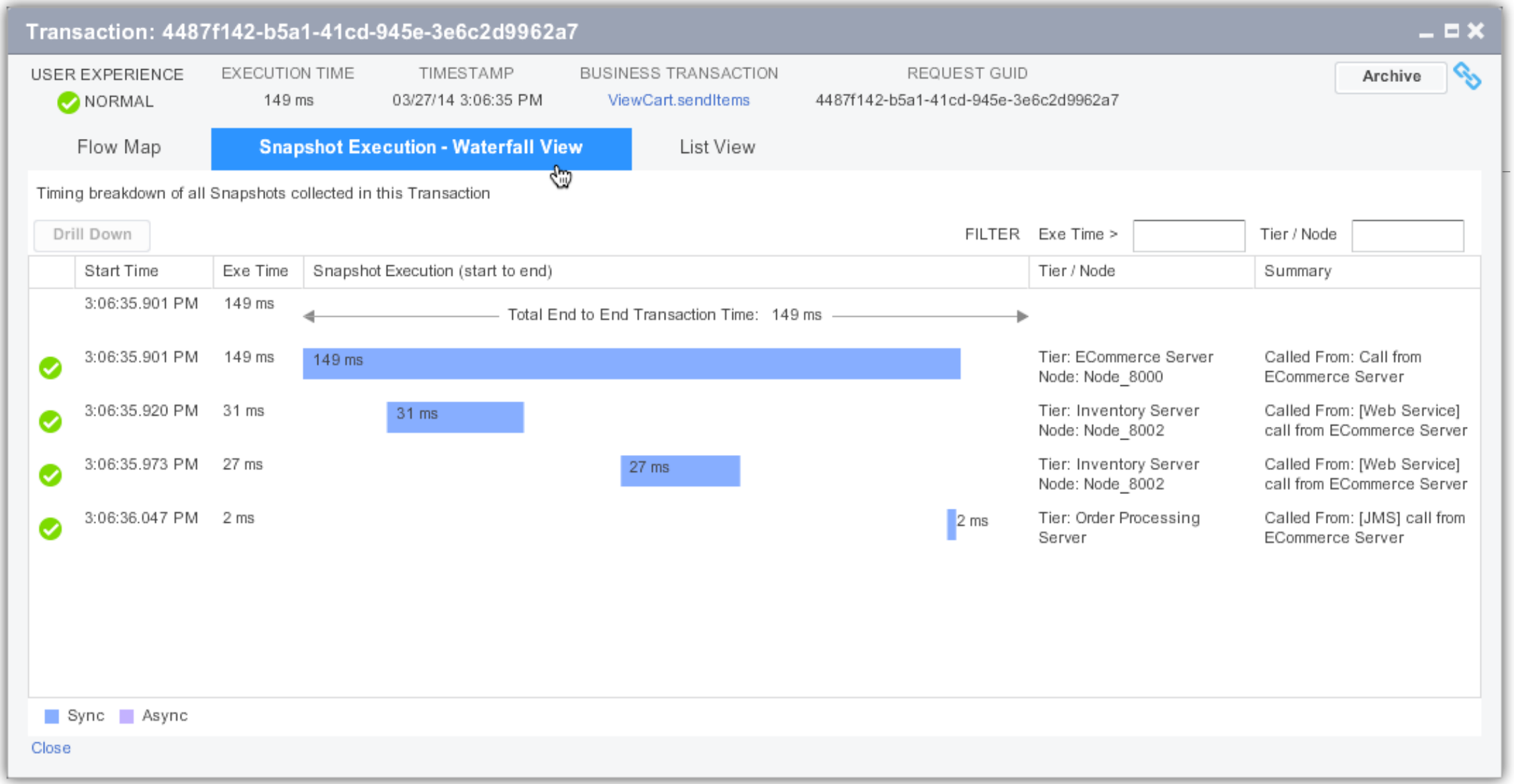
b) Snapshots

c) Audit Hooks

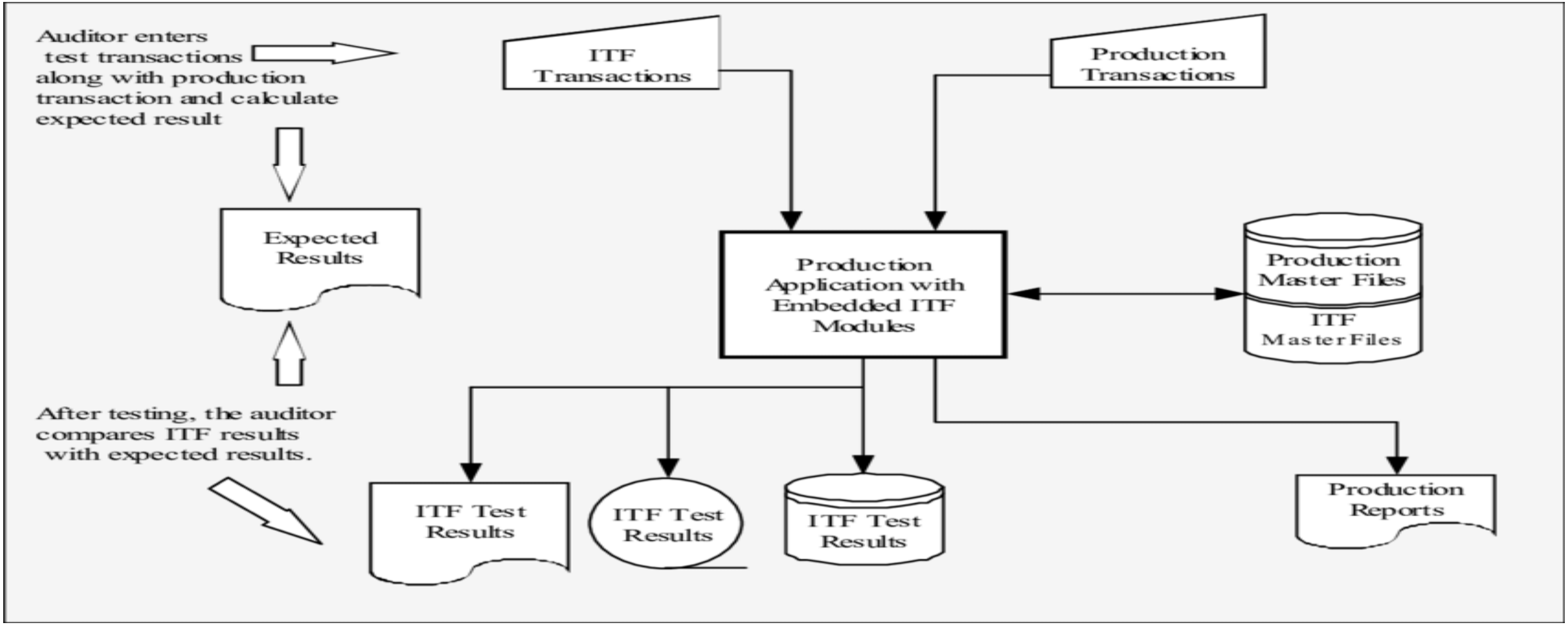
d) SCARF

SNAPSHOT

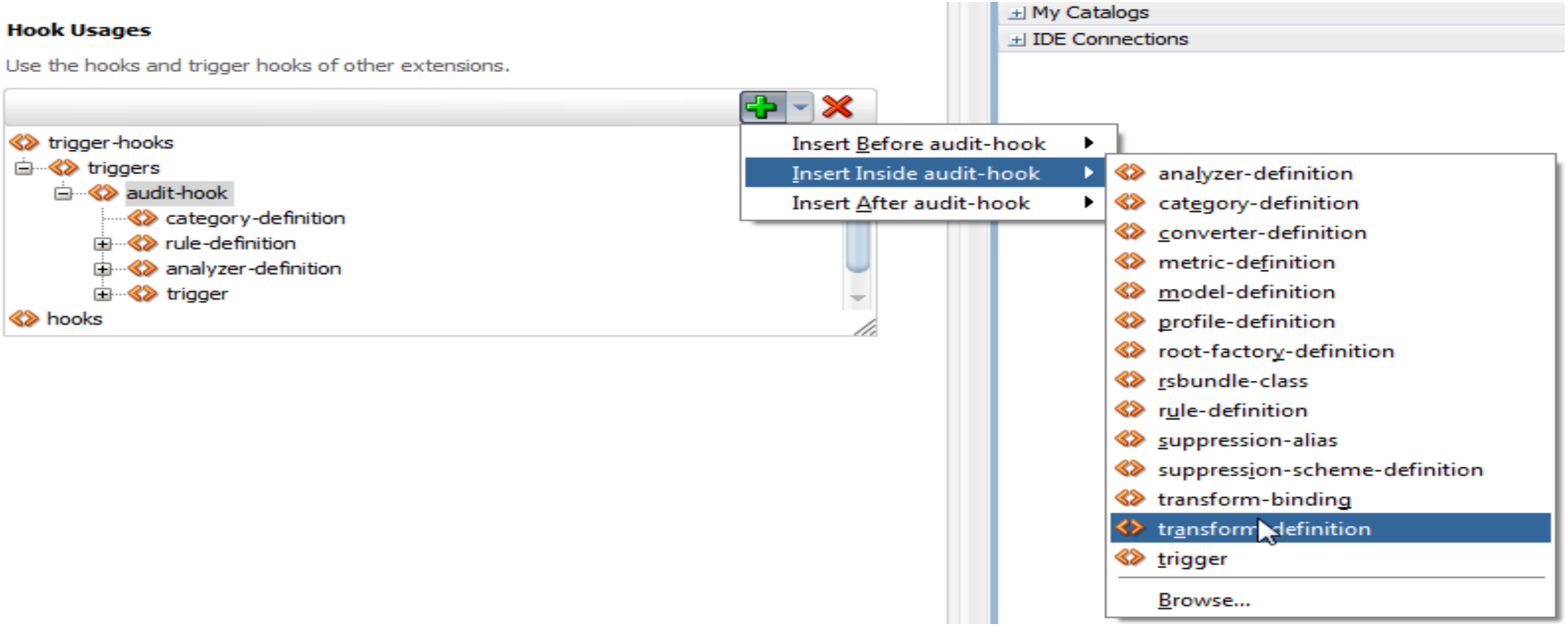




ITF



AUDIT HOOKS



CIS

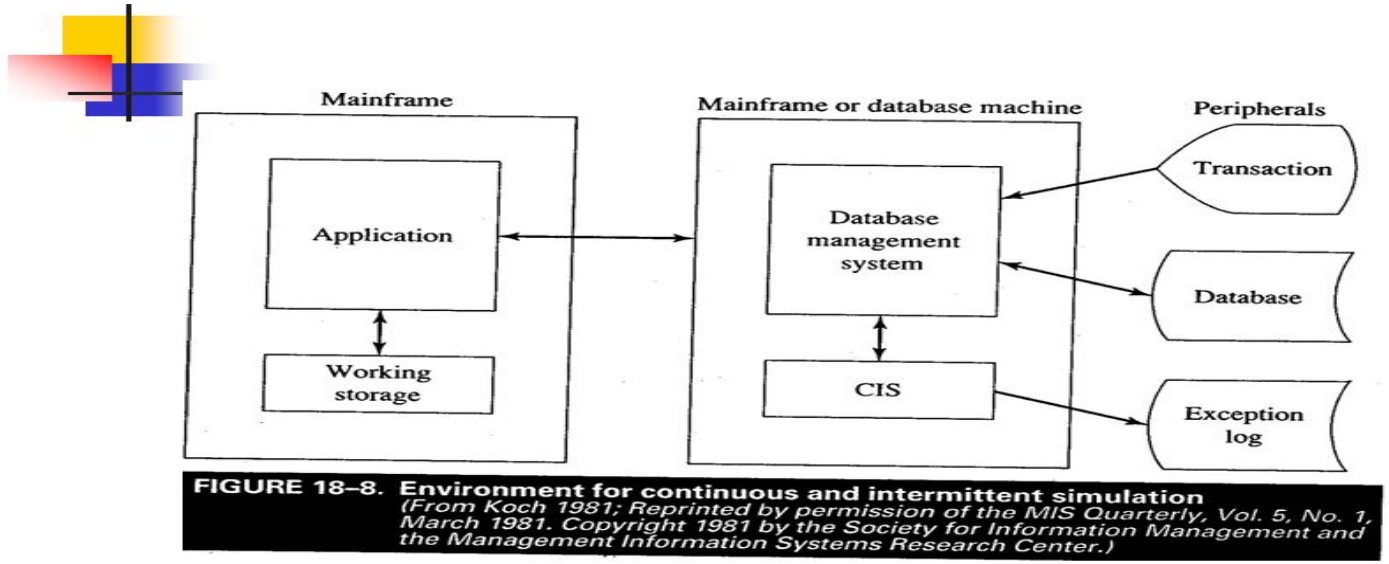
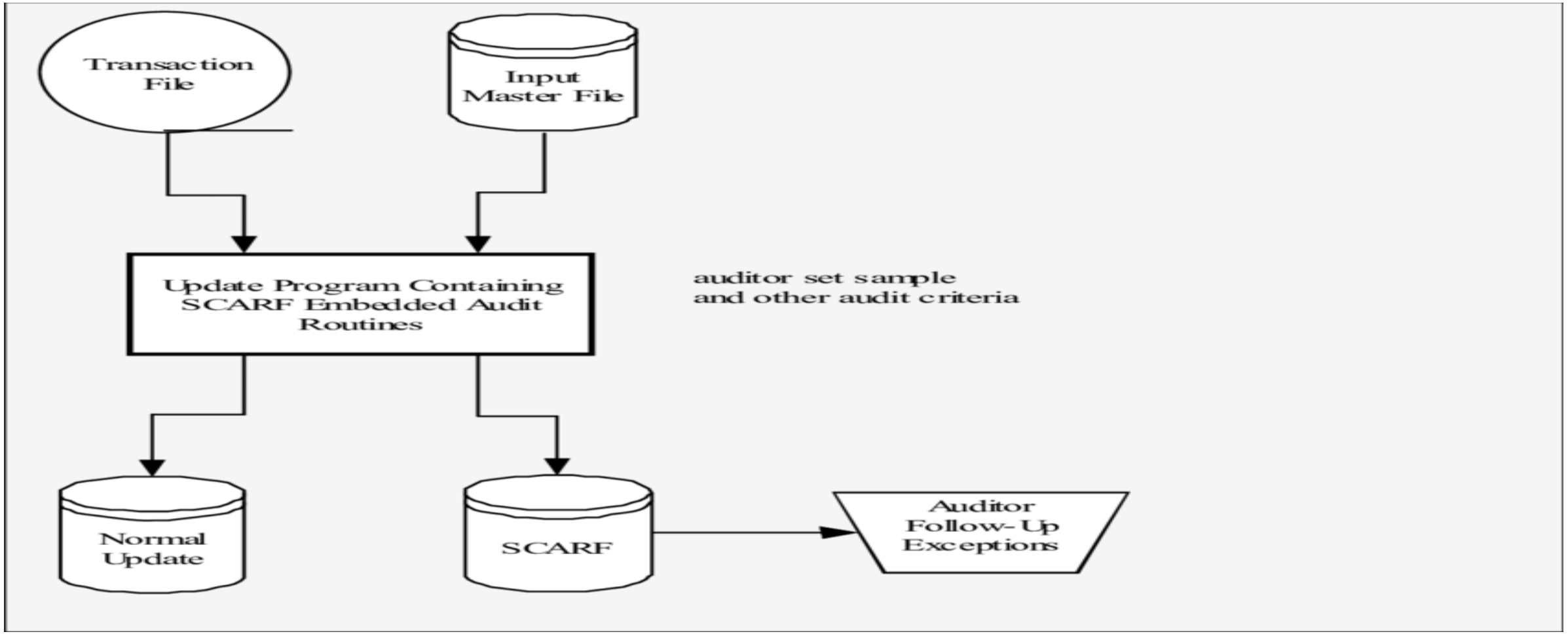


FIGURE 18–8. Environment for continuous and intermittent simulation *(From Koch 1981; Reprinted by permission of the MIS Quarterly, Vol. 5, No. 1, March 1981. Copyright 1981 by the Society for Information Management and the Management Information Systems Research Center.)*

SCARF



MCQ Time !

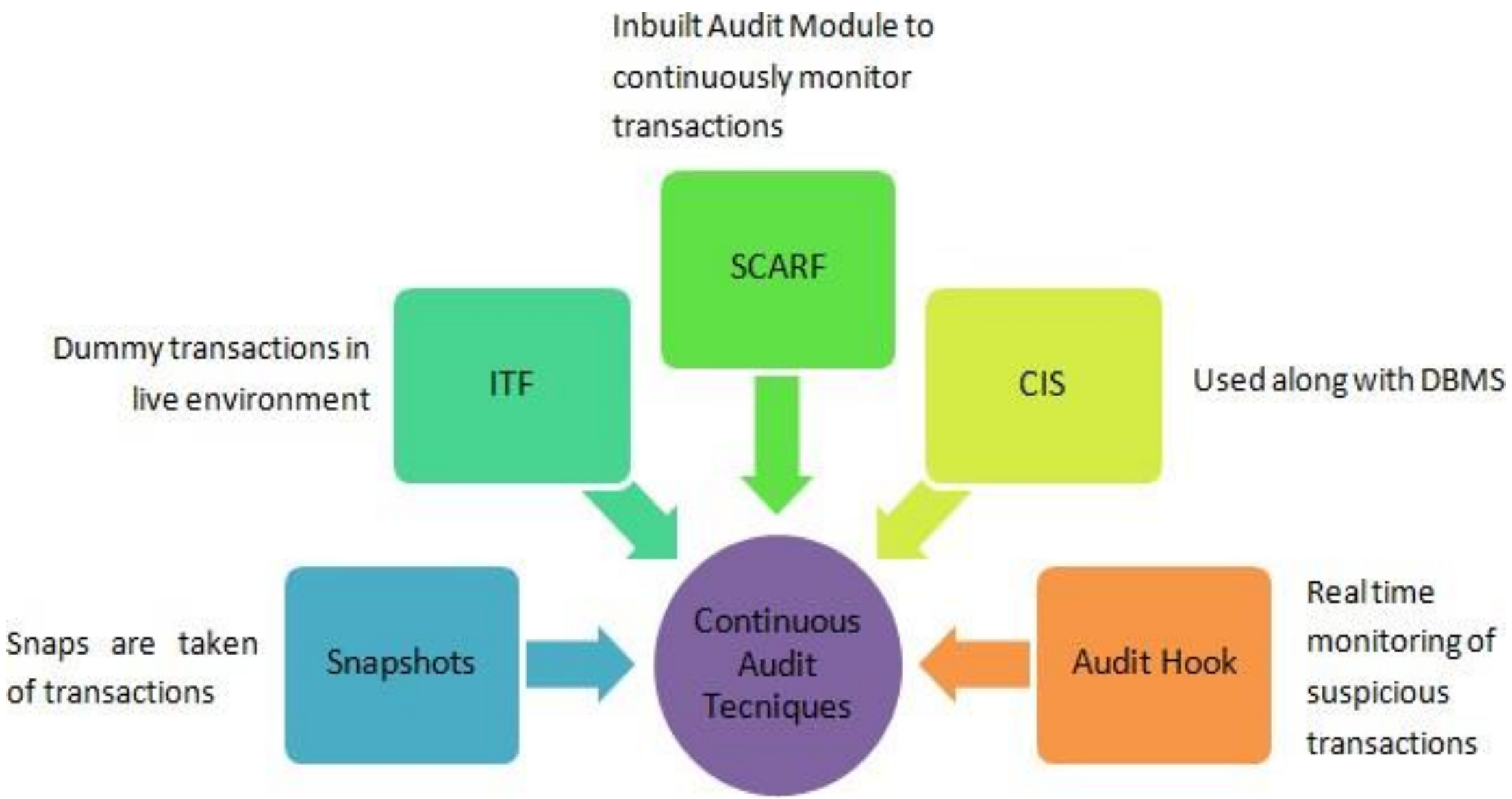
Q. Which among the following involves passing dummy transactions in live environment ?

a) CIS

b) Snapshots

c) ITF

d) SCARF



THANK YOU