B.TECH.

THIRD SEMESTER EXAMINATION 2009-10

IT INFRASTRUCTURE & ITS MANAGEMENT

Time : 3 Hours *Total Marks : 100*

Note: Attempt all questions:

Note: Attempt any four parts of the following: (5×4=20)

Q.1. (a) What is information technology? What are its components?

Ans. Information technology (IT), as defined by the Information Technology Association of America (ITAA), is

"the study, design, development, implementation, support or management of computer-based information systems, particularly software applications and computer hardware."

IT deals with the use of electronic computers and computer software to convert, store, protect, process, transmit and securely retrieve information.

The term information technology has ballooned to encompass many aspects of computing and technology, and the term has become very recognizable. The information technology umbrella can be quite large, covering many fields. IT professionals perform a variety of duties that range from installing applications to designing complex computer networks and information databases. A few of the duties that IT professionals perform may include data management, networking, engineering computer hardware, database and software design, as well as the management and administration of entire systems.

When computer and communications technologies are combined, the result is information technology, or 'infotech'. Information technology is a general term that describes any technology that helps to produce, manipulate, store, communicate, and/or disseminate information. Presumbaly, when speaking of Information Technology (IT) as a whole, it is noted that the use of computers and information are associated.

Components of Information Technology: Technological change is becoming a driving force in our society. Information technology is a generic term used for a group of technologies. James William (1982) has identified the following six major new technologies as most relevant in modern library and information system.

- Processor, memory and input/output channels.
- Micro, Mini and Large scale computers,
- Mass storage technologies,
- Data communication, networking and distributed processing,
- Data entry, display respond, and
- Software

These technologies can also be grouped into three major areas:

- Computer Technology,
- Communication Technology and
- Radiographic, Micrographic and Printing Technologies

(b) Distinguish between the following:

(i) Static RAM and Dynamic RAM

(ii) Magnetic tape and Magnetic disk.

Ans. (i) Static RAM and Dynamic RAM: A computer probably uses both static RAM and dynamic RAM at the same time, but it uses them for different reasons because of the cost difference between the two types. Dynamic RAM is the most common type of memory in use today. Inside a dynamic RAM chip, each memory cell holds one bit of information and is made up of two parts: a transistor and a capacitor. These are, of course, extremely small transistors and capacitors so that millions of them can fit on a single memory chip. The capacitor holds the bit of information -- a 0 or a 1 (see How Bits and Bytes Work for Informatioin on bits). The transitor acts as a switch that lets the control circuitry on the memory chip read the capacitor or change its state. A capacitor is like a small bucket that is able to store electrons. To store a 1 in the memory cell, the bucket is filled with electrons. To store a 0, it is emptied. The problem with the capacitor's bucket is that it has a leak. In a matter of a few milliseconds a full bucket becomes empty. Therefore, for dynamic memory to work, either the CPU or the memory controller has to come along and recharge all of the capacitors holding a 1 before they discharge. To do this, the memory controller reads the memory and then writes it right back. This refresh operation happens automatically thousands of times per second.

This refresh operation is where dynamic RAM gets its name. Dynamic RAM has to be dynamically refreshed all of the time or it forgets what it is holding. The downside of all of this refreshing is that it takes time and slows down the memory. Static RAM uses a completely different technology. In static RAM, a form of flip-flop holds each bit of memory. A flip-flop for a memory cell takes 4 or 6 transistors along with some writing, but never has to be refreshed. This makes static RAM significantly faster than dynamic RAM. However, because it has more parts, a static memory cell takes a lot more space on a chip than a dynamic memory cell. Therefore you get less memory per chip, and that makes static RAM a lot more expensive. So static RAM is fast and expensive, and dynamic RAM is less expensive and slower. Therefore static RAM is used to create the CPU's speed-sensitive cache, while dynamic RAM forms the larger system RAM space.

(ii) Magnetic tape has been used for data storage for over 50 years. In this time, many advances in tape formulation, packaging, and data density have been made. Modern magnetic tape is most commonly packaged in cartridges and cassettes. The device that performs actual writing or reading of data is a tape drive. Autoloaders and tape libraries are frequently used to automate cartridge handling.

When storing large amounts of data, tape can be substantially less expensive than disk or other data storage options. Tape storage has always been used with large computer systems. Modern usage is primarily as a high capacity medium for backups and archives. As of 2008, the highest capacity tape cartridges (Sun StorageTek T10000B, IBM TS1130) can store 1 TB of data without using compression whereas Magnetic Disk storage or disc storage is a general category of starge mechanisms, in which data are digitally recorded by various electronic, magnetic, optical, or mechanical methods on a surface layer deposited of one or more planar, round and rotating platters. A disk drive is a device implementing such a storage mechanism with fixed or removable media; with removable media the device is usually distinguished from the media as in CD drive and CD disc. Notable types are the hard disk drive (which is today almost always use fixed media), the floppy disk drive and its floppy disk, and various optical disc drives and associated media. Disk drives are block storage devices. Each disk is divided into logical blocks (collection of sectors). Blocks are addressed using their logical block addresses (LBA). Read from or writing to disk happens at the granularity of blocks. He drive stores

data onto cylinders, heads and sectors. The sectors unit is the smallest size of data to be stored in a Hard Disk Drive and each file will have many sectors units assigned to it. The smallest entity in a CD is called a frame, which consists of 33 bytes and contains six complete 16-bit stereo samples (two bytes × two channels × six samples = 24 bytes). The other nine bytes consist of eight CIRC error-correction bytes and one subcode byte used for control and display.

(c) What is software piracy and how it can be avoided?

Ans. Software piracy: Software piracy is the unauthorized duplication of computer software. Although most computer users today are aware that unauthorized use and duplication of software is illegal, many show a general disregard for the importance of treating software as valuable intellectual property.

Types of Software Piracy:

- **Softlifting:** Purchasing a single licensed copy of software and loading it onto several computers contrary to the license terms. For example, sharing software with friends, co-workers and others.
- **Uploading and downloading:** Making unauthorized copies of copyrighted software available to end users connected by modem to online service providers and/or the Internet.
- **Software counterfeiting:** Illegally duplicating and selling copyrighted software in a form designed to make it appear legitimate.
- **OEM unbundling:** Selling standalone software that was intended to be bundled with specific accmpanying hardware.
- **Hard disk loading:** Installing unauthorized copies of software onto the hard disks of personal computers, often as an incentive for the end user to buy the hardware from that particular hardware dealer.
- **Renting:** Unauthorized selling of software for temporary use, like you have a video.

Avoidance of Software piracy:

- **Avoid Internet distribution:** Be cautious when ordering software over the Internet. Many resellers with Internet storefronts or those who sell from auction sites knowingly distribute copies of software illegally. Estimates reveal that as much as 90% of software sold over Internet auction sites is either bootlegged or gray market. Some Web sites promise prospects free software downloads. These sites are distributing software illegally. There is also no guarantee that the software is secure or will work properly when installed. Thus, it is recommended that you purchase from an Authorized Reseller.

2. Distribution of inauthentic Software: Many resellers with Internet store software who sell from auction sites knowingly distribute copies of software illegally sold.

3. Report it: The best way to prevent software piracy is to report it. To ensure fast communication regardingly suspected software piracy use our feedback form.

4. Educate others: Those who believe they're saving money by pirating software couldn't be more mistaken. Legal and financial penalities, higher administrative costs, and lowered productivity make piracy very expensive.

(d) Write a short note on IT infrastructure library.

Ans. The IT Infrastructure Library is a set of books with good practice processes on how to manage IT service delivery. The library consists of many books and CD-ROMs.

The core set of material is the following set of seven tightly coupled areas:

- Service Delivery
- Service Support
- Security Management
- The Business Perspective
- Applications Management
- ICT Infrastructure Management

• Planning to implement Service Management.

The Service Support, Service Delivery and Security Management manuals are regarded as the central components of the framework.

These books cover the processes you will need to delivery customer-focused IT services according to your customers' needs, demands and wishes.

They help the IT group to be flexible and reliable enough to ensure consistent IT Service Delivery. The other core books in the library support these central components.

ITIL defines the organizational structure and skill requirements of an information technology organization and a set of standard operational management procedures and practices to allow the organization to manage an IT operatioin and associated infrastructure.

• The 'library' itself continues to evolve, with version three, known as ITIL v3, being the current release.

• These comprises five distinct volumes:

1. ITIL Service Strategy;
2. ITIL Service Design;
3. ITIL Service Transition;
4. ITIL Service Operation; and
5. ITIL Continual Service Improvement.

Benefits of ITIL to the customer/user:

• The provision of IT services becomes more customer-focused and agreements about service quality improve the relationship.

• The services are described better, in customer language, and in more appropriate detail.

• The quality, availability, reliability and cost of the services are managed better. Communication of the IT organization is improved by agreeing on the points of contact.

Benefits of ITIL to the IT organization:

• The IT organization develops a clearer structure, becomes more efficient, and more focused on the corporate objectives.

• The IT organization is more in control of the infrastructure and services it has responsibility for, and changes become easier to manage.

• An effective process structure provides a framework for the effective outsourcing of elements of the IT services.

• Following the ITIL best practices encourages a cultural change towards providing service, and supports the introduction of quality management systems based on the ISO 9000 series or on BS15000.

• ITIL provides a coherent frame of reference for internal communication and communication with suppliers, and for the standardization and identification of procedures.

(c) Describe the process of gathering user requirements.

Ans. Requirement gathering is a process of collecting the user needs to solve a problem or issues and achieve an objective. It is basically a software capability needed by the user to solve a problem or achieve an objective. This is really an important phase/milestone in the project life cycle. If the requirement gathering is not done properly/completely, all the hierarchy phases given below stay incomplete, no matter how best the design, until and unless requirements are complete. So we should carefully plan and carry out the requirements gathering with a systematic approach. It is not quite accurate to say that requirements are in the minds of customers; it would be more accurate to say that they are in the social system of customer organization. They have to be invented, not captured or elicited and that invention has to be a cooperative venture involving the clients, the users and developers. The difficuluties are mainly social, political and cultural and not technical.

Requirements Gathering Techniques: Requirements gathering techniques provide

project team members with a choice of methods for eliciting needs or requirements from customers and for validating requirements with customers. Certain techniques are appropriate in gathering customer needs, while other techniques are most helpful in defining high-level and detailed requirements, or validating detailed requirements with the customers. The three recommended techniques are:

1. Interview: An interview is a conversation with customers to elicit or validate needs and requirements. An interview may include one or more customers. The interview may also involve a question and answer session used to discover other potential customers and any discrepancies betwee needs; the high-level requirements derived from those needs; and the resulting detailed requirements. Interviews facilitate obtaining approval from customers on their needs, requirements, and any changes to them. The following parties are involved in an interview.

- **Interview Leader:** The interview leader may be respnsible for identifying the customers or by working with the appropriate project team member to get the list of customers. The interview leader is responsible for preparing questions ahead of the scheduled meeting and distributing the questions to the customer or customers. The leader is also responsible to either record the notes or schedule a recorder to attend the meeting to record information discussed in the meeting and any decisions resulting from the meeting.
- **Recorder:** The recorder is responsible for recording the informaton discussed in the interview and any decisions resulting from the meeting. In informal interviews the leader is also the recorder.
- **Customer:** The customer is responsible for providing thier needs, expectations, priorities, and constraints. They also validate the results of the interview.

Formal Interview Process Steps:

1. Identify customers to be interviewed.
2. Obtain a general understanding of the customers business.
3. Develop interview questions using open-eneded questions.
4. Set meeting time and location for the interview.
5. Provide a set of questions to interviewees prior to the interview (if they will need to prepare for the interview).
6. Use one or more Recorders to accurately preserve results of the interview.
7. Provide results to interviewees for confirmation of content.

Informal Interview Process Steps:

1. Identify customers to be interviewed.
2. Obtain a general understanding of the customers business.
3. Develop interview questions (for interviewer's use only) to make sure certain questions are answered during the session.
4. Set up a casual meeting or telephone conversation time for the interview.
5. Takes handwritten notes during the interview; avoid using electronic data capture.
6. Provide results to interviewee for confirmation of content.

II. Joint Application Development (JAD) Technique: The Joint Application Development (JAD) technique is an extended, facilated workshop. It involves collaboration between customers and systems analysts to identify needs or requirements in a concentrated and focused effort.

JAD Process Steps:

1. Define Session: Define the purpose, scope, and objectives of the JAD session, selecting the JAD team, invite and obtain commitment to attend sessions from the appropriate customers, and schedule the session. It is important to obtain management commitment to support the process and identify the appropriate customers.

2. Research Product: Become more familiar with the product or service, gather preliminary information, obtaining any models.

3. Prepare: Prepare any visual aids, developing a realistic agenda, training the recorder, and preparing the meeting room.

4. Conduct Session: Follow agenda to gather and document the project needs and requirements. It is important to ensure all participants are given equal treatment during the process.

5. Draft the Document: Prepare the formal documents. The information captured in the JAD session is further redefined through analysis efforts, open questions or issues discovered through the sessions are resolved, and the final document is returned to customers for review and validation.

III. Survey Method: The Survey Method is an electronic or paper based method of soliciting needs or requirements from customers. The survey method is a list of questions, directed at identifying customer needs or requirements.

Survey Method Process Steps:

1. Decide what you want to know and how you will analyze the data before you develop questions.

2. Look for questions or ideas from other sources to inspire the writing of your method.

3. Write questions to be as specific as possible. Use simple, straightforward language, Avoid the use of jargon or terminology specific to a few people.

4. Write short questions to ensure reader understanding including:

— Limit the number of choices available to a question to five or less (if applicable).

— Offer a "don't know" or "no opinion" option, so people do not invent answers.

— Vary the format of the questions to keep people interested.

5. When you have written the survey questions, it is important to test them to make sure that the language is current, the questions are not biased, and the questions are relevant to the purpose of the survey. Deliver the set of questions to the customer for thier response. Provide a date by which the answers are to be returned.

(f) What do you understand by IT service management? How does it impact the business IT relationship?

Ans. IT Service Management is primarily known as the process and service-focussed approach of what was initially known as IT Management. The objective of IT Service Management processes is to contribute to the quality of the IT services. Quality management and process control form part of the organization and its policies. With a process-focussed approach we also have to consider the situation within an organization (policies, culture, size, etc.).

ITIL, the best known approach to IT Service Management, does not prescribe the type of organization, but instead describes the relationships between the activities in processes, which are relevant to any organization. This provides a framework for exchanging experiences between organizations. This approach also provides a framework for learning from the experience of dynamic organizations.

Impact on Business IT relationship: Organizations are becoming increasingly dependent on IT to fulfill their corporate objectives. This increasing dependence has resulted in a growing need for IT services of a quality corresponding to the objectives of the business, and which meet the requirements and expectations of the customer. Over the years, the emphasis has shifted from the development of IT applications to the management of IT services. An IT application (sometimes referred to as an information system) only contributes to realizing corporate objecties if the system is available to users and, in the event of fault or necessary modifications, it is

supported by maintenance and operational management. In the overall life cycle of IT products, the operations phase amounts to about 70 to 80% of the overall time and cost, the rest is spent on product development (or procurement). Thus, effective and efficient IT Service Management processes are essential to the success of IT. Thus, effective and efficient IT Service management processes are essential to the success of IT. This applies to any type of organization, large or small, public or private, with centralized or decentralized IT services, with internal or outsourced IT services. In all cases, the service has to be reliable, consistent, of a high quality, and of acceptable cost.

IT Service Management addresses the provision and support of IT services tailored to the needs of the organization. ITIL was developed to disseminate proven IT Service Management best practices systematically and cohensively. The approach is based on service quality and developing effective and efficient processes.

Q.2. Attempt any TWO parts of the following: **(2×10=20)**

(a) What is the importance of the folloiwng items to availability

(i) Resilience

(ii) Serviceability

Ans. (i) Resilience: Adequate reliability means that the service is available for an agreed period without interruptions. This concept also includes resilience. The reliability of a service increases if downtime can be prevented. Reliability is calculated using statistics. The reliability of a service is determined by a combination of the following factors:

- Reliability of the components used to provide the service.
- Ability of a service or component to operate effectively despite failure of one or more subsystems (resilience).
- Preventive maintenance to prevent downtime.

(*ii*) Serviceability: Serviceability relates to contractual obligations of external service providers (contractors, third parties). The contracts define the support to be provided for the outsourced services. As this only concerns a part of the IT service, the term does not refer to the overall availability of the service. If a contractor is responsible for the service as a whole - for example when a Facilities Management contract is concluded. - then serviceability and availability are synonymous.

Effective Availability Management requires a thorough understanding of both the business and the IT environment. It is important to be aware that aailability cannot simply be 'bought'. Availability has to be included in the design and implementation from the initial design stage. Finally, availability depends on the complexity of the infrastructure, the reliability of the components, the professionalism of the IT organization and its contractors, and the quality of the process itself.

(b) How does OLA differ from the SLA?

Ans. Service Level Agreement (SLA): A Service Level Agreement is an agreement between the IT organization and the customer, which details the service or services to be provided. The SLA describes the services in non-technical terms, in line with the perception of the customer, and during the term of the agreement it serves as the standard for measuring and adjusting the IT services. SLA's normally have a hierarchical structure, for example, general services such as network and Service Desk services are defined for the organization as a whole and approved by management. More specific services, associated with the business activities, are agreed at a lower level in the organization, for example, with the business unit management, budget holder or customer representative.

The structure of a SLA depends on a number of the variables such as:

Physical aspects of the organization:

- Scale
- Complexity
- Geographical distribution

Cultural aspects:

- Language(s) of the document (for international organizations).
- Relationship between the IT organization and the customer.
- Charging policy.
- Uniformity of the business activities.
- Profit or non-profit organization.

Nature of the business activities:

- General terms and conditions.
- Business hours - 5 × 8 hours or 7 × 24 hours.

Whereas an Operational Level Agreement (OLA) is an agreement with an internal IT department detailing the provision of certain elements of a service. For example, if the SLA contains targets for restoring a high prority incident, then the OLAs should include targets for each of the elements in the support the IT organization providing the services.

(c) Discuss the benefits that can be expected from IT service management.

Ans. Advantages of IT Service Management: IT Service Management (ITSM) is a discipline for managing information technology (IT) systems, philosophically centered on the customer's perspective of IT's contribution to the business. ITSM stands in deliberate contrast to technology-centered approaches to IT management and business interaction.

1. By implementing IT Service Management in your IT organization you support the IT objectives of delivering services that are required by the business. This can't be done without aligning the IT strategy with the business strategy. You can't deliver effective IT services without knowing about the demands, needs and wishes of the customer. IT services management supports the IT organisation to align IT activities and service delivery, with business requirements.

2. IT Service Management helps the IT organisation to manage the service delivery by organising the IT activities into end-to-end processes. These processes have no functional boundaries within the IT group.

3. IT services generally depend on several departments, customers or disciplines. Processes that span several departments can monitor the quality of the service by measuring aspects, such as availability, capacity, cost and stability. IT Service Management matches these quality aspects with the customer's demands. ITIL provides a concise and commonsense set of processes to help with the management, monitoring and delivering of services.

4. Align IT services with current and future business and Customer needs.

5. Partner with the business to create new business opportunities.

6. Reduce long-term cost of services, driving down term cost of services, driving down Total Cost of Ownership (TCO).

7. Improve quality of IT services.

8. Deliver current services consistently.

(d) What are the goals and objectives of capacity management?

Ans. Capacity Management aims to provide the required capacity for data processing and storage, at the right time and in a cost effective way. It is a balancing act. Good capacity management eliminates panic buying at the last minute, or buying the biggest box possible and crossing your fingers. Both of these situations are costly. Many data centers, for example, perpetually run at or below 20% average utilization (used capacity), over the business day (not making any allowance for system types, but including file & print servers, etc.). This is not so bad when you have a handful of servers. But when you have thousands of servers, as many enterprise IT organizations do, these percentages mean vast

sums of money are being wasted. Capacity Management addresses the following issues:

- Can the purchase cost of processing capacity be justifid in the light of business requirements, and is the processing capacity used in the most efficient way (cost versus capacity)?
- Does the current processing capacity adequately fulfill both current and future demands of the customer (supply versus demand)?
- Is the availability processing capacity performing at peak efficiency (performance tuning)?
- Precisely when should additional capacity be made available?
- Do we know what future IT capacity is needed and when?

To implement its objective, Capacity Management needs a close relationship with business and IT strategy processes. Hence, this process is both reactive (measuring and improving) and proactive (analyzing and forecasting). Capacity Management aims to consistently provide the required IT resources at the right time (when they are needed), and at the right cost, aligned with the current and future requirements of the business. Thus, Capacity Management needs to understand both the expected business developments affecting customers, as well as anticipating technical developments. The Capacity Management process has an important role in determining returns on investment and cost justifications.

(e) Describe the various subprocesses of financial management.

Ans. Sub processes of Financial Management: Financial Management for IT Services contains 3 sub-processes:

- IT Accounting
- Charging

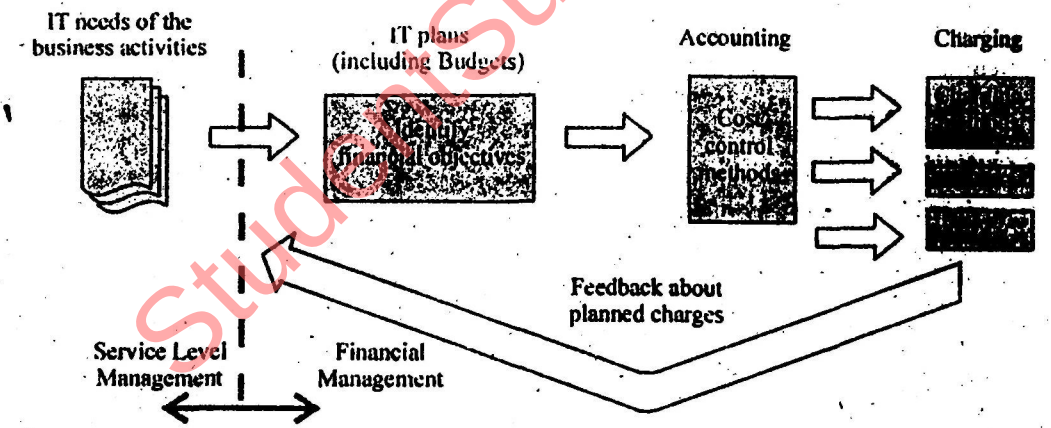


Fig. *Financial Management process.*

1. Budgeting: Budgeting enables an organization to plan future IT expenditure, thus reducing the risk of over-spending and ensuring the revenues are available to cover the predicted expenditure. Additionally it allows an organization to compare actual costs with previously predicted costs in order to improve the reliability of budgeting predictions.

Budgeting methods: One of the following methods is selected, depending on the financial policy of the business:

- **Incremental budgeting:** Last year's figures are used as the basis for the new budget. This is then adjusted to reflect the expected changes.

- **Zero-Base budgeting:** This method starts with a blank piece of paper: the Zero Base. Past experience is ignored. This requires managers to justify all their resource needs in terms of costs in their budget. This means that every expense has to be evaluated and decided if it should be made, as well as what the cost should be. Obviously, this method is much more time-consuming, and it is therefore normally only used every few years. The incremental method is used for the years in between.

Budgeting process: Budgeting starts by identifying the key factors that limit the growth of the company. In many businesses this is the sales volume; however, it could also be a lack of space or materials. Often, financial constraints determine the budget. This process includes defining the following secondary budgets:

- **Sales and marketing budget:** If the sales volume determines the budget, then the marketing department is responsible for a large part of the process. An accurate assessment and analysis of the customers, markets, sales regions, products, etc. is essential for drawing up a good budget.
- **Production budget:** The production budget provides detailed information about the servies to be provided: quantities, delivery times, person-hours required, materials required etc.
- **Administrative budgets:** Based on the service to be provided, you have to determine the overhead budgets for the relevant departments such as production, sales and distribution, research and development, etc.
- **Cost and investment budgets:** The cost budget results from the plans in the above budgets. The investment budget identifies the expenditure associated with the replacement and purchase of the means of production. Investment projects initiated in the preceding year may also affect the investment budget.

Budget period: The financial (fiscal) year would be an obvious choice for the budget period. For a regular comparison between the actual and budget figures, the budget period is then divided into months or another regular period, such as four-week windows.

2. IT Accounting: IT Accounting is concerned with the amount of money spent in providing IT Services. It allows an organization to perform various financial analyses to gauge the efficiency of the IT service provision and determine areas where cost savings can be made. It will also provide financial transparency to aid management in the decision making process. Several Cost Elements can be used to control your accounting:

- **Capital Costs:** Any type of purchases which would have a residual value as hardware and building infrastructure.
- **Operational Costs:** Day to day recurring expenses cost like rental fees, monthly electrical invoices and salaries.
- **Direct Costs:** Any cost expenses which are directly attributed to one single or specific service or customer. A typical example would be the purchase of a dedicated server which cannot be shared and is needed to host a new application for a specific service or customer.
- **Indirect Costs:** One specific service provision which cost needs to be distributed in between several customers in a fair breakdown. A fair example is the cost associated to overall Local Area Network on which every customer are connected to. Breakdown could be done using total amount of users per customer or total amount of bandwidth usage per customer to accurately distribute the cost of providing this service..
- **Fixed Costs:** Any expenses established for long periods of time like annual maintenance contracts or a lease contracts.

One of the primary Accounting activities is defining the cost elements. This structure is fixed for one year, after which it can be modified.

In most cases, a cost accounting method will have been selected when introducing a cost element structure to the business. Thus, the cost element structure should be compatible with the methods adopted by the business. In many cases, costs are recorded for each department, customer or product. However, ideally the structure should reflect the services provided. Even when the process is not used for charging, it is often useful to have the cost type structure on a service structure, such as that used in a service catalogue.

3. Charging: Charging provides the ability to assign costs of an IT Service proportionally and fairly to the users of that service. It may be used as a first step towards an IT organisation operating as an autonomous business. It may also be used to encourage users to move in a strategically important direction - for example by subsidising newer systems and imposing additional charges for the use of legacy systems. Transparency of charging will encourage users to avoid expensive activities where slightly more inconvenient but far cheaper alternatives are available. For example, a user might browse a dump on screen rather than printing it off.

Charging is the most complex of the three sub-processes, requiring a large investment of resources and a high degree of care to avoid anomalies, where an individual department may benefit from behaviour which is detrimental to the company as a whole. Charging policy needs to be simultaneously simple, fair and realistic.

Charging need not necessarily mean money changing hands (Full Charging). It may take the form of information passed to management on the cost of provision of IT services (No Charging), or may detail what would be charged if full charging were in place without transactions actually being applied to the financial ledgers (Notional Charging). Notional Charging may also be used as a way of plotting Full Charging.

(f) Describe the various documents generated by service level management.

Ans. Documents generated by SLM:

1. Service Level Requirements (SLR): Service Level Requirements cover the detailed definitions of customer needs, and are used to develop, modify and initiate services. Service Level Requirements can serve as a blueprint for designing a service and its associated SLA(s), and may also be used as a design assessment.

2. Service Specification Sheets (Space Sheets): Service Spec Sheets describe the relationship between functionality (as agreed with the customer, therefore customer-focused) and technology (as implemented within the IT organization, therefore IT-focused) and provide a detailed specification of the service. The Spec Sheets translate Service Level Requirements (external specifications) into technical definitions needed to provide the service (internal specifications). The Spec Sheets also describe any links between the SLA's, any UC's and any OLA's. The Spec Sheets are an important tool to monitor correspondence between the internal and external specifications.

3. Service Catalogue: Developing a Service Catalogue can help the IT organization to profile itself and to present itself as an IT Service Provider as opposed to a mere implementer and maintainer of technology. The Service Catalogue provides a detailed description of the operational services in the customer's language, along with a summary of the associated service levels that the IT organization can provide to its customers. As such, it is an important communications tool. The Service Catalogue can help steer customer expectations, and in this way facilitate the alignment process between service customers and service providers. This document is derived

from the external specifications in the Spec Sheets and should therefore be written in the customer's language, and not in the form of technical specifications.

4. Service Level Agreement (SLA): A Service Level Agreement is an agreement between the IT organization and the customer, which details the service or services to be provided. The SLA describes the services in non-technical terms, in line with the perception of the customer and during the term of the agreement it serves as the standard for measuring and adjusting the IT services. SLA's normally have a hierarchical structure, for example general services such as network and Service Desk services are defined for the organization as a whole and approved by management. More specific services, associated with the business activities, are agreed at a lower level in the organization, for example with the business unit management, budget holder or customer representative.

5. Service Improvement Program (SIP): The Service Improvement Program, often implemented as a project, defines the activities, phase and milestones associated with improving an IT service.

6. Service Quality Plan (SQP): The Service Quality Plan is an important document as it contains all management information needed to manage the IT organization. The service Quality Plan defines the process parameters of the Service Management processes and operational management.

7. Operational Level Agreement (OLA): An Operational Level Agreement is an agreement with an internal IT department detailing the provision of certain elements of a service. For example, if the SLA contains targets for restoring a high priority incident, then the OLA's should include targets for each of the elements in the support chain (target for the Service Desk to answer calls, escalate, etc., targets for Network Support to start to investigate and to resolve network related errors assigned to them, etc.). OLA's support the IT organization providing the services.

8. Underpinning Contract (UC): An Underpinning Contract is a contract with an external provider defining the provision of certain elements of a service; for example troubleshooting workstations, or leasing a communications line. This is similar to the external implementation of an OLA.

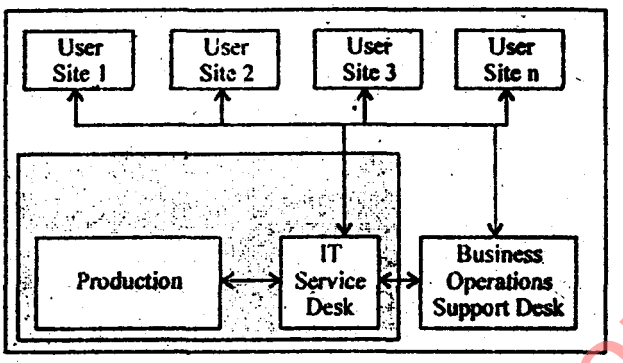
Q.3. Attempt any FOUR parts of the following:

(a) Define various types of service desks.

Ans. There are several options for the structure of the Service Desk. Common approaches include:

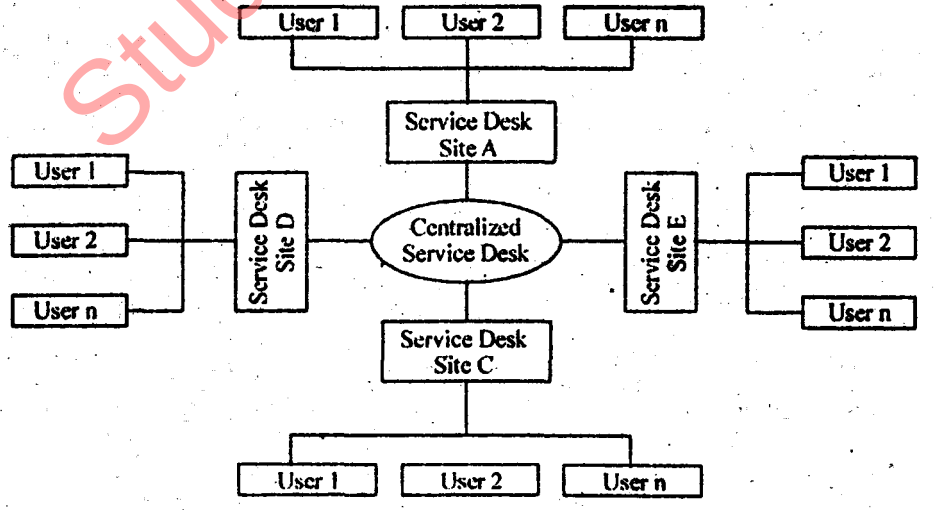
1. Centralized Service Desk as a single point of contact for all users, possibly with a separate Service Desk close to the users for business applications (split function Service Desk). If the IT organization is responsible both for providing the service (the Information System) and supporting the use of the Information System then it is best if the user can approach the Service Desk as a single point of contact. In that case, the IT Service Desk is responsible for call acceptance and recoding, progress monitoring and escalation. Here, the business operations support function is part of the IT Service Desk or it is the responsibility of a support team managed by the Service Desk. This requires a common incident recording system. If the IT organization is not responsible for buisness operations support, then the business operations support desk will represent the users when the IT service provider's support is required. This approach can be combined with an operations bridge (a physical concentration of operational management activities, e.g. a Service Desk in combination with an Operations department) to provide direct communication between the Service Desk and operational management (Production, Operations), where Production includes Network Management, Computer Operations, etc. This direct communication facilitates a rapid response if there are errors that cannot be resolved

immediately by the Service Desk.. Ideally, the departments should be located in close proximity to each other.



2. Local (distributed) Service Desks across a number of sites. Normally, dividing the Service Desk across a number of sites wil make it more difficult to manage. Distributed Service Desks are split across a number of sites, in different buildings or even in different countries. Fig. shows an example of the structure of a distributed Service Desk. There is a further choice between:

- **A central point of contact** - routes calls through to local support. The central Service Desk can serve as the initial point of contact for users and specialize in incident recording. Modern call routing software increases the effectiveness of the Service Desk in resolving incidents.
- **Local points of contact** - with a central Service Desk to track and monitor incidents. This approach is often used if the local organization has its own language and culture. It is also used when the organization has a substantial number of custom applications in each line of business.
- **A call center** - this option is becoming increasingly popular and is often used by suppliers. A central telephone number, usually toll-free, provides access to a voice response menu where the user can select the subject about whom they need assistance, such as e-mail or Office applications. The call is then routed to a specialist support team. These support teams may be in different geographical areas, but the user will not be aware of this.



3. Virtual Service Desk where the location is immaterial due to the use of communications technology. A modern, specialized version of the distributed Service Desk is the virtual Service Desk. This consists of a number of local Service Desks, which appear to form one unit as modern telecommunication technology and networks make the location immaterial. The Service Desk and support can now be located anywhere. Using a number of sites in different time zones around the world ('follow the sum support') support can be provided around the clock. The disadvantage of a virtual Service Desk is that it is more difficult to provide on-site support. Lately, we have seen 'self-help' as a form of providing 'automated' Service Desk functionality. Self-help in the form of, for instance, web access to the knowledge database (look for known errors) and incident records (check status, etc.) is an important option to reduce cost and empower the end user community.

(b) What are the objectives and benefits of configuration management?

Ans. Configuration management (CM) is a field of management that focuses on establishing and maintaining consistency of a system's or product's performance and its functional and physical attributes with its requirements, design, and operational information throughout its life. For informatin assurance,

CM can be defined as the management of security features and assurances through control of changes made to hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the life cycle of an information system.

The goals of configuration management are:

- Account for all the IT assets and configurations within the organization and its services.
- Provide accurate information or configurations and their documentation to support all the other Service Management processes.
- Provide a sound basis for Incident Management, Problem Management, Change Management and Release Management.
- Verify the configuration records against the infrastructure and correct any exceptions.

Advantages:

1. Managing IT components: The IT components are essential to the delivery of IT services. Each element of the IT services will include one or more CI's and Configuration Management checks what happens to them.

2. High quality IT services: Configuration Management assists with processing changes, identifying and solving problems and supporting users. This reduces the number of errors and therefore also reduces costs by preventing duplication of effort.

3. Effective problem solving: Configuration Management assists with localizing the affected CI's and manages the modification and replacement of the CI's. Configuration Management also provides information about trends as an input to Problem Management.

4. More rapid processing of changes: Configuration Management facilitates rapid and accurate impact analysis so changes can be processed more quickly and more effectively.

5. Better control of software and hardware: The rollout of packages can be combined, possibly also with hardware rollouts, such that the whole combination can be tested in advance.

6. Improved security: Managing the versions used provides information about the authorized changes to CI's and the use of different software versions. Information from the CMDB can also assist with monitoring licenses.

7. Compliance with legal requirements: Illegal copies will be identified when audit results are compared with the CMDB. This can bring extra benefits because illegal software can contain viruses. In this way Configuration Management can prevent the introduction of viruses into the organization.

8. More precise expenditure planning: The CMDB can provide information about maintenance costs and contracts, licenses and expriation dates.

9. Better support for Availability Management and Capacity Management: These processes depend on correct configuration details for analyzing and planning services.

10. A solid foundation for IT Service Continuity Management: If there is a backup copy of the CMDB in a safe place, it can play an important part in restoring services after a disaster. The CMDB is also essential in identifying the CI's requirement for disaster recovery, including the relevant procedures and the manuals if they are included in the CMDB.

(c) What are the various inputs, outputs and activities of incident management?

Ans. Usually as part of the wider management process in private organizations, incident management is followed by post-incident analysis where it is determined why the incident happened despite precautions and controls. This information is then used as feedback to further develop the security policy and/or its practical implementation. In the USA, the National Incident Management System, developed by the Department of Homeland Security, integrates effective practices in emergency management into a comprehensive national framework. Fig. shows the entire incident management procedure, showing the goal, inputs, outputs etc. of the incident management process.

The various activities are:

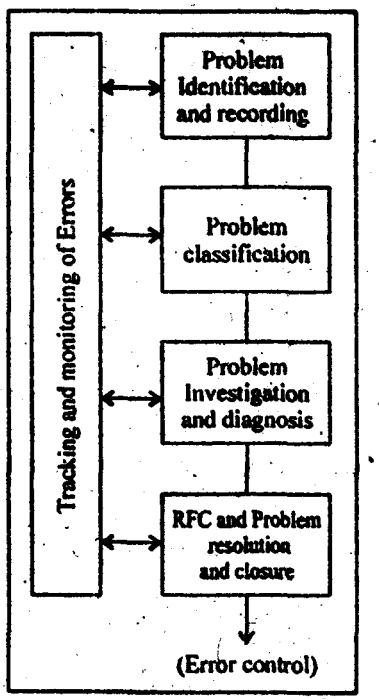
- **Incident acceptance and Recording:** The incident is detected or reported and an incident record is created.
- **Classification and initial support:** The incident is coded by tape, status, impact, urgency, priority, SLA, etc. The user may be given suggestions to solve or work around the issue, even if only temporarily.

If the call concerns a Service Request the relevant procedure is initiated.

- **Matching:** A check is made to see if the incident is known, and possibly related to an existing incident, problem or known error and if there is a solution or a workaround.
- **Investigation and Diagnosis:** If there is no known solution then the incident is investigated.
- **Resolution and Recovery:** Once the solution has been found, the issue can be resolved.
- **Closure:** The user is asked if they are satisfied with the solution an then the incident can be closed.
- ***Progress monitoring and tracking:*** The entire incident cycle is monitored, if it appears that an incident cannot be resolved in time or with the current level of expertise, then escalation will occur.

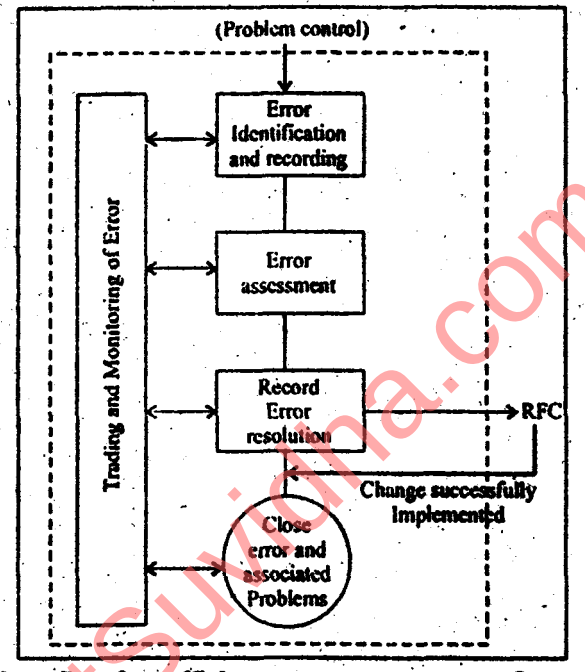
(d) Describe the problem control and error control processes in problem management.

Ans. Problem Control: This activity is responsible for identifying problems and investigating their root cause. The imperative of Problem Control is to turn problems into known errors by identifying the underlying cause of the problem and identifying a workaround. Problem Control activities are shown in figure.



Error Control: Error control consists of monitoring and managing known errors until

they are successfully resolved, where possible and appropriate. Error control does this by raising a Request For Change to Change Management, and by evaluating the changes in a Post-Implementation Review (PIR). Error Control monitors all known errors from their identification through resolution. Error Control may involve many departments and covers both the production and development environments.



(e) What are the benefits of an efficient storage management?

Ans. The benefits of efficient storage management are:

Features	Benefits
Backup and Recovery Management	Centralized protection based on smart-move and smart store technology leading to faster backup and restores with less network and storage resources needed.
Hierarchical Storage Management	Ability to automate critical processes relating to the media on which data is stored while reducing storage media and administrative costs associated with managing data.
Archive Management	Ability to easily protect and manage documents that need to be kept for a certain period of time.
Advanced Data Reduction	Reduces the costs of data storage, environmental requirements, and administration.

(f) What do you mean by disaster recovery process? Write down the various steps in disaster recovery process.

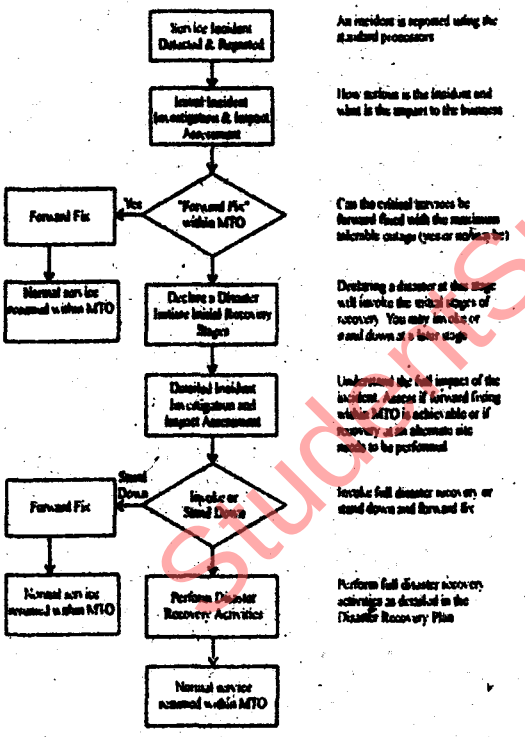
Ans. Disaster Recovery refers to the set of technical measures and organisational processes designed to restore the systems, data and infrastructures necessary to resume business operations

following a severe disruption.

The purpose behind Disaster Recovery is to ensure business continuity, i.e. the ability of a company to continue to operate its business after catastrophic events.

To accomplish this, systems, and business data are typically backed up and stored at a secondary site so that, in the event of a disaster (earthquake, flood, terrorist attack, etc.) that renders the primary site unusable, operations can be resumed as soon as possible at the secondary site, with the least amount of data loss possible.

The following diagram gives a high level *incident management and DR invocation flow*:



The main steps for effective Disaster Recovery Process are as follows:

Step 1: Risk Analysis: The first step in drafting a disaster recovery plan is conducting a thorough risk analysis of your computer systems. List all the possible risks that threaten system uptime and evaluate how imminent they are in your particular IT shop. Anything that can cause a system outage is a threat, from relatively common man made threats like virus attacks and accidental data deletions to more rare natural threats like floods and fires. Determine which of your threats are the most likely to occur and prioritize them using a simple system: rank each threat in two important categories, probability and impact. In each category, rate the risks as low, medium or high.

For example, a small Internet company (less than 50 employees) located in California could rate an earthquake threat as medium probability and high impact, while the threat of utility failure due to a power outage could rate high probability and high impact. So in this company's risk analysis, a power outage would be a higher risk than an earthquake and would therefore be a higher priority in the disaster recovery plan.

Step 2: Establish the Budget: Once you have figured out your risks, ask 'what can we do to suppress them, and how much will it cost?' Can I detect a threat before it hits? How do I reduce the potential of it occurring? How do I minimize its impact to the business? For example, our small California Internet company could employ an emergency power supply to mitigate its power outage threat and have all its data backed up daily on RAID tapes, which are stored at a remote site in case of an earthquake. The more preventative measures you establish upfront the better. Emerson says, "dollars spent in prevention are worth more than dollars spent in recovery. The results of Step 1 should be a comprehensive list of possible threats, each with its corresponding solution and cost. It is imperative that IT present all of these threats to the business operations units, so they can make an informed decision regarding the size of the disaster recovery budget (i.e., which risks the company can afford to tolerate and which it must pay to mitigate). Ultimately, the

business operations unit decides which threats the business can tolerate. Disaster recovery budgets vary from company to company but they typically run between 2 and 8 percent of the overall IT budget. Companies for which system availability is crucial usually are on the higher end of the scale, while companies that can function without it are on the lower end. However, these percentages may be too small.

Step 3: Develop the Plan: The feedback from the business units will begin to shape your DRP procedures. If, for example, they determine that the company must be up within 48 hours of an incident to stay viable, then you can calculate the amount of time it would take to execute the recovery plan and have the business back up in that timeframe. The recovery procedure should be written in a detailed plan or "script". Establish a Recovery Team from among the IT staff and assign specific recovery duties to each member. The manner in which your team conducts its recovery probably will be no different than its regular production procedures: the chain of command likely won't change and neither will the aspects of the network for which each member is responsible.

Step 4: Test: Once your DRP is set, test it frequently. Eventually you'll need to perform a component-level restroation of your largest databases to get a realistic assessment of your recovery procedure, but a periodic walk-through of the procedure with the Recovery Team will assure that everyone knows their roles. Test the systems you are going to use in recovery regularly to validate that all the piece work. Always record your test results and update the DRP to address any shortcomings.

Q.4. Attempt any FOUR parts of the following: (4×5=20)

(a) Why is the need for security policy felt in an organization? What are the various components of security policy?

Ans. A security policy is a formal statement of the rules through which people are given access to an organization's technology, system and information assets. The security policy defines what business and security goals and objectives management desires, but not how these solutions are engineered and implemented. A security policy should be economically feasible, understandable, realistic, consistent, procedurally tolerable, and also provide reasonable protection relative to the stated goals and objectives of management. Security policies define the overall security and risk control objectives that an organization endorses.

Basic Purpose of Security Policy: The primary purpose of a security policy is to inform users, staff, and managers of those essential requirements for protecting various assets including people, hardware, and software resources, and data assets. The policy should specify the mechanisms through which these requirements can be met. Another purpose is to provide a baseline from which to acquire, configure, and audit computer systems and networks for compliance with the policy. This also allows for the subsequent development of operational procedures, the establishment of access control rules and various application, system, network, and physical controls and parameters. A security policy should fulfill many purpose. It should:

- Protect people and information.
- Set the rules for expected behaviour by users, system administrators, management and security personnel.
- Authorize security personnel to monitor, probe, and investigate.
- Define and authorize the consequences of violation.
- Define the company consensus baseline stance on security.
- Help minimize risk.
- Help track compliance with regulations and legislation.

Information security policies provide a framework for best practice that can be followed by all employees. They help to ensure risk is minimized and that any security incidents are effectively responded to. Information security policies will also help turn staff into participants in the company's efforts to secure its information assets, and the process of developing these policies will help to define a company's information assets. Information security policy defines the organization's attitude to information, and announces internally and externally that information is an asset, the property of the organization and is to be protected from unauthorized access, modification, disclosure, and destruction.

Components of Security Policy: Following are the basic components of a security policy:

- Purpose includes the objectives of the program, such as:
  - Improved recovery times
  - Reduced costs or downtime due to loss of data
  - Reduction in errors for both system changes and operational activities
  - Regulatory compliance
  - Management of overall confidentiality, integrity and availability
- Scope provides guidance on whom and what are covered by the policy. Coverage may include:
  - Facilities
  - Lines of business
  - Employees or departments
  - Technology
  - Processes
- Responsibilities for the implementation and management of the policy are assigned in this section. Organizational units or individuals are potential assignment candidates.
- Compliance provides for the policy's enforcement. Describe oversight activities and disciplinary considerations clearly. But the contents of this section are meaningless unless an effective awareness program is in place.

(b) What is firewall? Discuss the various basic types of firewall.

Ans. A Firewall disrupts free communication between trusted and un-trusted networks, attempting to manage the information flow and restrict dangerous free access.

There are numerous mechanisms employed to do this, each one being somewhere between completely preventing packets flowing, which would be equivalent to completely disconnected networks, and allowing free exchange of data, which would be equivalent to having to Firewall.

Types of Firewall: There are a number of different kinds of technique which may be employed by a Firewall in order to correctly identify a conversation and act on it. The techniques used by a particular Firewall have an impact on the accuracy with which it can identify traffic, the level of sophistication of the checks it can implement, but also it's complexity and therefore cost and likelihood that it incorporates bugs.

1. Packet Filter: The network level operations corresponding to the security policy above were actually an example of a simple packet filter. A Firewall implementing a packet filter looks at one packet at a time, and considers it in isolation in order to make a forwarding decision. Becuase of the way that a packet filtering firewall works, it can implement a restricted range of filtering decisions.

2. Stateful inspection: It takes the basic principles of packet filtering and adds the concept of history, so that the Firewall considers the packets in the context of previous packets. So for example, it records when it sees a TCP SYN packet in an internal table, and in many implementations will only allow TCP packets that match an existing conversation to be forwarded to the network.

(b) Write short notes on the following:

(i) Identity Management

(ii) Access Management

Ans. (i) Identity Management: Identity management is the management of the identity life cycle of entities (subjects or objects). Identity management is multidisciplinary and covers many dimensions such as:

- **Technical.** With identity management systems.
- **Legal.** Such as legislation for data protection.
- **Police.** For instance for dealing with identity theft.
- **Social and humanity.** Dealing with issues such as privacy.
- **Security.** With elements such as access control.
- **Organizations.**

Identity Management or IDM is a term related to how humans are identified and authorized across computer networks. It covers issues such as how users are given an identity, the protection of that identity and the technologies supporting the protection such as network protocols, digital certificates, passwords and so on. The term digital identity is often used it refers to Personal identifying information (PII) selectively exposed over a network.

While the term management requires little explanation, the term identity is a more abstract concept that will always be difficult to define in a way that satisfies everyone. It is a concept that is fluid and contextual depending on a number of factors including culture. Thus the term management is appended to "identity" to indicate that there is technological and best practices framework around a somewhat intractable philosophical concept. Digital identity can be interpreted as the codification of identity names and attributes of a physical instance in a way that facilitates processing. In each organisation there is normally a role or department that is responsible for managing the schema of digital identities of their staff and their own objects, these represented by object identities or object identifiers (OID).

- IDM provides significantly greater opportunities to online businesses beyond the process of authenticating and granting access to authorized users via cards, tokens and web access control systems.
- User-based IDM has started to evolve away from username/password and web-access control systems toward those that embrace preferences, parental controls, entitlements, policy-base routing, presence and loyalty schemes.
- IDM provides the focus to deal with system-wide data quality and integrity issues often encountered by fragmented databases and workflow processes.
- IDM embraces what the user actually gets in terms of products and services and how and when they acquire them.
- Therefore, IDM applies to the products and services of an organization, such as health, media, insurance, travel and government services.
- It is also applicable to means by which these products and services are provisioned and assigned to (or removed from) "entitled" users.
- IDM can deliver single-customer views that include the presence and location of the customer, single products and services as well as single IT infrastructure and network views to the respective parties.

(ii) Access Management: Access management is a simple concept. Every business has information that needs to be protected from unauthorized disclosure. To protect information, companies define policies that govern who can access specific classes of business and/or personal information. For example, if a manager seeks to access the salary of a subordinate, they should have authorization to do so, however, they should

not be authorized to access the same information about a chief executive.

- Access Management software has a simple goal. It allows the human who previously acted as a guardian of sensitive information to be removed from the process without loss of access control.
- This sounds simple, but most businesses are struggling with the implementation of access management as they integrate and extend their applications.
- This is because machines cannot classify information or make access decisions unless they are explicitly programmed with algorithms to accomplish this.
- It becomes necessary to insert software guards into your applications.
- The access policy used by software guards is often coded directly into the business application (typically requiring new database tables and/or directory infrastructure).
- When access policy or audit requirements change, application software must be modified, tested and redeployed.
- Additionally, when access policy needs to be examined or applications audited for conformance a code review is required.

Often, individuals are granted access to business applications using operating system, database and/or network "access control" mechanisms. That is, the application has no responsibility for access management; application access is controlled by the runtime infrastructure. Increasingly, however, existing applications are being integrated and/or extended to an expanded base of end-users by leveraging technologies that bypass or tunel through operating system and network security. These modernized applications not only steward business and personal information, they also span technology boundaries (e.g. the Web, J2EE, JMS, CORBA, RDBMS). It may be impossible for existing security infrastructure (not designed for multi-tier access) to maintain and communicate the identity of the user through each technical tier, making it impossible to leverage existing identity-based access control mechanisms. In fact, emerging identity management standards only address sharing identity in the e-business (i.e. "Web" technology) domain. Integrated business applications, however, are increasingly being held responsible for user and access management in service-oriented architectures that span technology boundaries to deliver functionality.

This is because the focus of security infrastructure (and associated security organizations) has been on protecting networks and operating systems, not applications. This is understandable. Overwhelmed with attacks on their networks, corporate security groups have no resources available to assist with deployment of a security infrastructure for application-level security (often characterized as fine-grain access control).

Application security, therefore, must address any security-related requirements not provided by the runtime security infrastructure. In the areas of access management, any requirement to restrict the:

(a) usage of application features or

(b) access to business and personal information, is part of "application security".

Q.5. Write short notes on any two of the following: (2×10=20)

(a) Computer Forensics

(b) Cyber Crimes

(c) Electronic Commerce

Ans. (a) Computer Forensics: Comptuer forensics is a branch of forensic science pertaining to legal evidence found in computers and digital storage mediums. Computer forensics is also known as digital forensics. The goal of computer forensics is to explain the current state of a digital artifact. The term digital artifact can inclue a computer system, a storage medium (such as a hard disk or CD-

ROM), an electronic document (e.g. an email message or JPEG image) or even a sequence of packets moving over a computer network. The explanation can be as straightforward as "what information is here?" and as detailed as "what is the sequence of events responsible for the present situation?" The field of Computer Forensics also has sub branches within it such as Firewall Forensics, Database Forensics and Mobile Device Forensics. Special measures should be taken when conducting a forensic investigation if it is desired for the results to be used in a court of law. One of the most important measures is to assure that the evidence has been accurately collected and that there is a clear chain of custody from the scene of the crime to the investigator--and ultimately to the court. In order to comply with the need to maintain the integrity of digital evidence, British examiners comply with the Association of Chief Police Officers (A.C.P.O.) guidelines. These are made up of four principles as follows:

Principle 1. No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.

Principle 2. In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaning the relevance and the implications of their actions.

Principle 3. An audit trail or other record of all processes applied to computer based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

Principle 4. The person in charge of the investigatino (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

There are many applications of computer forensics:

- In legal cases, computer forensic techniques are frequently used to analyze computer systems belonging to defendants (in criminal cases) or litigants (in civil cases).
- To recover data in the event of a hardware or software failure.
- To analyze a computer system after a break-in, for example, to determine how the attacker gained access and what the attacker did.
- To gather evidence against an employee that an organization wishes to terminate.
- To gain information about how computer systems work for the purpose of debugging, performance optimization, or reverse-engineering.

(b) Cyber Crimes: The term 'cyber crime' is a misnomer. This term has nowhere been defined in any statute/Act passed or enacted by the Indian Parliament. The concept of cyber crime is not radically different form the concpet of conventional crime. Both include conduct whether act or omission, which cause breach of rules of law and counterbalanced by the sanction of the state. Cyber crime is the latest and perhaps the most complicated problem in the cyber world. "Cyber crime may be said to those species, of which, genus is the conventional cime, and where either the computer is an object or subject of the conduct constituting crime." "Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber crime." A generalized definition of cyber crime may be "unlawful acts wherein the computer is either a tool or target or both". The computer may be used as a tool in the following kinds of activity-financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, e-mail spoofing, forgery, cyber defamation, cyber stalking. The computer may

however be target for unlawful acts in the following cases-unauthorized access to computer/computer system/computer networks, theft of information contained in the electronic form, e-mail bombing, data didling, salami attacks, logic bombs, Trojan attacks, internet time thefts, web jacking, theft of computer system, physically damaging the computer system.

• **Unauthorized access to computer systems, or networks/Hacking:** This kind of offence is normally referred as hacking in the generic sense. However the framers of the information technology act 2000 have no where used this term so to avoid any confusion we would not interchangeably use the word hacking for 'unauthorized access' as the latter has wide connotation.

• **Theft of information contained in electronic form:** This includes information stored in computer hard disks, removable storage media etc. Theft may be either by appropriating the data physically or by tampering them through the virtual medium.

• **Email bombing:** This kind of activity refers to sending large numebrs of mail to the victim, which may be an individual or a company or even mail servers there by ultimately resulting into crashing.

• **Data diddling:** This kind of an attack infolves altering raw data just before a computer processes it and then changing it back after the processing is completed. The electricity board faced similar problem of data diddling while the department was being computerised.

• **Salami attacks:** This kind of crime is normally prevalent in the financial institutions or for the purpose of committing financial crimes. An important feature of this type of offence is that the alteration is so small that it would normally go unnoticed.

• **Denial of Service attack:** The computer of the victim is flooded with more requests than it can handle which cause it to crash. Distributed Denial of Service (DDoS) attack is also a type of denial of service attack, in which the offenders are wide in numebr and widespread. E.g. Amazon, Yahoo.

• **Virus/worm attacks:** Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. ?They usually affect the data on a computer, either by altering or deleting it. Worms, unlike viruses do not need the host to attach.

(c) Electronics Commerce: Electronic Commerce, commonly known as (electronic marketing) e-commerce or a eCommerce, consists of the buying and selling of products or services over electronic systems such as the Internet and other computer networks. Electronic commerce is doing business online. It is about using the power of digital information to understand the needs and preferences of each customer and each partner to customize products and services for them, and then to deliver the products and services as quickly as possible. Personalized, automated services offer businesses the potential to increase reveues, lower costs, and establish and strengthen customer and partner relationships. To achieve these benefits, many companies today engage in electronic commerce for direct marketing, selling and customer service; online banking and billing; secure distribution of information; value chain trading; and corporate purchasing. Although the benefits of electronic commerce systems are enticing, developing, deploying, many companies will need to reengineer their business processes to maximize the benefits of electronic commerce. An electronic commerce strategy should help deliver a technology platform, a portal for online services, and a professional expertise that companies can leverage to adopt new ways of doing business. An e-commerce platform should be the foundation of technologies and products that enable and support electronic commerce. With it, businesses can develop low-cost, high-

value commerce systems that are esy to grow as business grows. An e-commerce platform's breadth should also be unmatched, ranging from operating systems to application servers, to an application infrastructure and development tools, and to a development system. Portals are the crossroads of the Internet, where consumers gather and where businesses can connect with them. Indepndent software vendors (ISVs) have created specialized commerce software components that extend the platform. The consumer moves through the internet to the merchant's web side. From there, he decides that he wants to purchase something, so he is moved to the online transaction server, where all of the information he gives is encrypted. Once he has placed his orde,r the information moves through a private gateway to a Processing Network, where the issuing and acquiring banks complete or deny the transaction. This generally takes place in no more than 5-7 seconds. There are many different payment systems available to accommodate the varied processing needs of merchants, from those who have a few orders a day to those who process thousands of transactions daily. With the addition of Secure Socket Layer technology, eCommerce is also a very safe way to complete transactions.