

Total Marks = 90

Q.2 (a)

Ecommerce vs E- Business:-

E-business is the practice of performing and coordinating critical business processes such as designing products, obtaining supplies, manufacturing, selling, fulfilling orders and providing services through the extensive use of computers and communication technologies and computerized data.

E-business includes everything having to do with the application of information and communication technologies (ICT) to the conduct of business between organizations or from company to consumer.

The part of E-business that a customer experience directly is often called **E-Commerce**. This refers to using the Internet and other communication technology for marketing, selling, and servicing products. E-commerce often includes tasks such as:

- Informing a customer of a product's existence.
- Providing in-depth information about the product.
- Establishing the customer's requirements.
- Performing the purchase transactions
- Delivering the product electronically if the product happens to be software or information.
- Providing customer service electronically.

b) **SLA in ITSM:-**

To support IS Operations, many organizations have implemented IT service management. ITSM comprises processes and procedures for efficient and effective delivery of IT services to business.

A service level agreement (SLA) is an agreement between the IT organization and the customer. It describes the services in nontechnical term, from the viewpoint of the customer. SLA is the process of defining agreeing upon, documenting and managing levels of service that are required and cost justified. SLA includes the production and service improvement plans (SIP) for areas that are not achieving their SLAs. The aim of SLA is to maintain and improve customer satisfaction, minimized downtime, and to improve the service delivered to the customer. With clear definition of service level, the organization or service provider can design the service based on the service level, and the customer can monitor the performance of the IT services. If the services provided don't meet the SLA, the IT organization or service provider has to improve the services. Many tools are available to monitor the efficiency and effectiveness of service provided to meet SLA requirements.

Q.3 (a) **Challenges associated with effective management of IS Projects:**

Effective project management requires clear goals (which is a result if the project is carried out successfully), deliverables (tangible work products) and schedules (terse project description identifying the timing of major steps and who will do the work).

Many of the challenges of project management mirror those of any other form of management: assigning the right people to the right jobs, getting people to do high-quality work, getting people to report their progress realistically, and resolving issues and disputes. Especially important in project oriented work are estimating project scope and duration, minimizing rework on completed steps, and recovering from delays.

Estimating project scope and duration:

It is difficult to estimate the scope and duration of project for a number of reasons, including uncertain project scope, changes in scope, individual differences in productivity, and the way work is distributed in projects.

Minimizing rework on completed steps:

Although some steps of an IS project may be performed simultaneously, many steps build on the outputs of previous steps. Sometimes output from previous steps may have to be changed because more is understood now or because the previous work contained errors. Consequently, there is often some rework even though a project is described as a sequence of successive steps.

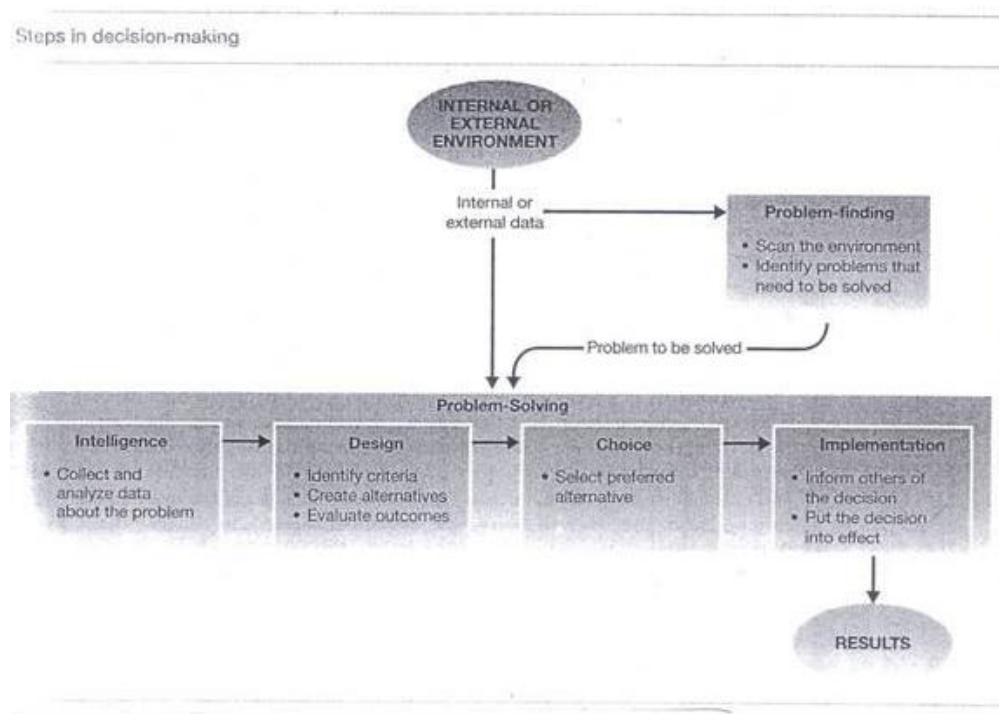
Recovering from delays:

The most natural unit for estimating the size of system development projects and tracking their progress is the person-week or person-month. This tactic fails for IS projects, even if it might work for other projects. Adding many new workers to an ongoing project can temporarily halt progress.

The amount of communication and coordination time absorbed by large project teams is also a reason to avoid allowing a project to get too large too soon.

b) Basic Decision-Making Concepts:

Information systems are designed to support decision-making in one way or another. Decision-making is represented as a problem-solving process preceded by a separate problem-finding process. Problem-finding is the process of identifying and formulating problems that should be solved. Although often overlooked, problem-finding is the key to effective decision-making because a seemingly good solution to the wrong problem may miss the point.



Problem-solving is the process of using information, knowledge, and intuition to solve a problem. The problem-solving portion says that most decision processes can be divided into four phases: intelligence, design, choice, and implementation.

- Intelligence includes the collection and analysis of data related to the problem identified in the problem-finding stage. Key challenges in the intelligence phase include obtaining complete and accurate data and figuring out what the data imply for the decision at hand.
- Design includes systematic study of the problem, creation of alternatives, and evaluation of outcomes. Key challenges in this phase include bounding the problem to make it manageable, creating real alternatives, and developing criteria and models for evaluating the alternatives.
- Choice is the selection of the preferred alternative. Key challenges here include reconciling conflicting objectives and interests, incorporating uncertainty, and managing group decision processes.
- Implementation is the process of putting the decision into effect. This includes explaining the decision to the appropriate people, building consensus that the decision makes sense, and creating the commitment to follow through. Key challenges involve ensuring that the decision and its implications are understood and that others in the organization will follow through, whether or not their preferred alternative is chosen.

Q.4 (a) WAN:

A WAN needs to be monitored and managed similarly to a LAN. ISO, as part of its

DISCLAIMER: The suggested answers provided on and made available through the Institute's website may only be referred, relied upon or treated as a guide and substitute for professional advice. The Institute does not take any responsibility about the accuracy, completeness or currency of the information provided in the suggested answers. Therefore, the Institute is not liable to attend or receive any comments, observations or critics related to the suggested answers.

communications modelling effort, has defined five basic tasks related to network management:

- Fault management – Detects the devices that present some kind of technical fault.
- Configuration management – Allows users to know, define and change, remotely, the configuration of any device.
- Accounting resources – Holds the records of the resource usage in the WAN (who uses what).
- Performance management – Monitors usage levels and sets alarms when a threshold has been surpassed.
- Security management – Detects suspicious traffic or users, and generates alarms accordingly.

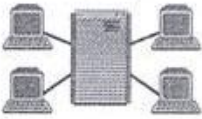

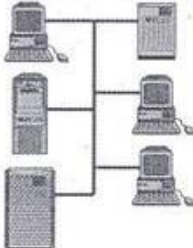
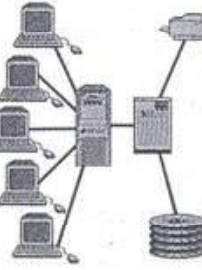
Simple Network Management Protocol:

This TCP/IP-based protocol monitors and controls different variables throughout the network, manages configurations, and collects statistics on performance and security. A master console polls all the network devices on a regular basis and displays the global status. Simple Network Management Protocol (SNMP) software is capable of accepting, in real-time, specific operator requests. Based on the operator instructions, SNMP software sends specific commands to an SNMP-enabled device and retrieves the required information. To perform all of these tasks, each device (routers, switches, hubs, PCs, servers) needs to have a SNMP agent running. The actual SNMP communications occur between all the agents and the console.

b) Four Approaches to Computing in Organizations:

Computer systems should be deployed in a way that mirrors business processes. If people work individually and rarely share their work products, computer systems should provide effective tools for individual work. If people work as a group, computer systems should make it easier to share work. If the organization relies on a central database for orders, reservations, or inventory, computer systems should provide access to the database.

Four approaches to computing in organizations

Approach to computing	Basic Idea of the approach	Advantages	Disadvantages
	In centralized computing, terminals are attached to a central computer that performs all the computations and controls all the peripherals, such as printers.	<ul style="list-style-type: none"> Greater security because all processing is controlled at a central location 	<ul style="list-style-type: none"> Central computer must perform computing and must do work to control the remote terminals Total reliance on the central computer; if it goes down, so does the entire system
	In personal computing, individual microcomputers are used for individual work but are not linked in a network.	<ul style="list-style-type: none"> Greater flexibility for individual users doing inherently individual work Less impact from what others are doing using a computer 	<ul style="list-style-type: none"> Difficulty sharing the work individuals do Duplication of underutilized hardware and software
	In distributed computing, multiple workstations are linked to share data and computing resources. The data and resources may be at the local site or may be elsewhere.	<ul style="list-style-type: none"> Greater ability to share work, information, and resources Ability to continue doing some useful work even if part of the network is down 	<ul style="list-style-type: none"> Complex to administer Security more difficult because computing and data are so spread out
	In network computing, multiple network computers are linked to a central server that controls their operation and that provides links to other servers.	<ul style="list-style-type: none"> Greater ability to share work, information, and resources Easier to administer than distributed computing 	<ul style="list-style-type: none"> Reliance on a central server Limited processing ability at user's computer

Q.5 (a) Effect of Laws & Regulations on IS Audit Planning:

Each organization, regardless of its size or the industry, will need to comply with a number of governmental and external requirements related to computer system practices and controls and to the manner in which computers, programs and data are stored and used. Additionally, business regulations can impact the way data are processed, transmitted and stored.

Special attention should be given to these issues in industries that are closely regulated. Several countries are making efforts to add legal regulations concerning IS audit. The content of these legal regulations pertains to:

- Establishment of legal requirements
- Responsibilities assigned to corresponding entities.
- Financial, operational and IT audit functions.

Management personnel as well as audit management at all levels, should be aware of the external requirements relevant to the goals and plans of the organization, and to the responsibilities and activities of the information services department /function/activity.

There are two major areas of concerns: legal requirements placed on audit or IS audit, and legal requirements placed on the auditee and its system, data management, reporting etc. These areas would impact audit scope and audit objectives. The latter is important to internal and external auditors. Legal issues also impact the organizations business operations in terms of compliance with ergonomic regulations.

The following are steps an IS auditor would perform to determine an organization's level of compliance with external requirements:

- Identify those government or other external requirements.
- Document applicable laws and regulations.
- Assess whether the management of the organization and the IS function have considered the relevant external requirement in making plans and in setting policies, standard and procedures, as well as business application features.
- Review internal IS department /function/activity documents that address adherence to established procedures that address adherence to laws applicable to industry.
- Determine adherence to established procedures that address these requirements.
- Determine if there are procedures in place to ensure contracts or agreements with external IT services providers reflect any legal requirements related to responsibilities.

b) Policies and Procedures:

Policies and procedures reflect management guidance and directions in developing controls over information system, related resources and IS department processes.

IS auditors should understand that policies are a part of the audit process and test the policies for compliance. IS controls should flow from the enterprise's policies, and IS auditors should use policies as a benchmark for evaluating compliance. However, if policies exist that hinder the achievement of business objectives, these policies must be identified and reported for improvement. The IS auditor should also consider the extent to which the policies apply to third parties or outsourcers the extent to which third parties or outsourcers comply with the policies, and whether the policies of the third parties or outsourcers are in conflict with the enterprise's policies. The IS auditor ensure effective implementation of Acceptable internet usage policy, Internet security policy and other organization internal policies.

Q.6 (a) Key features of ISMS:

An IT system packed with security features and devices will not be protected unless it is properly implemented and managed and carefully operated, monitored and reviewed. IS security is more than just a mechanism. IS security also includes cultural aspects that must be embraced by all individuals within an organization for IS security to be effective.

An **information security management system** (ISMS) is a frame work of policies, procedures, guidelines and associated resources to establish, implement, operate, monitor, review, maintain and improve information system security for all types of organizations. Some key elements of Information security management are as follows:

- i) Senior Management commitment and support
- ii) Policies and procedures
- iii) Security awareness and education
- iv) Monitoring and compliance
- v) Incident handling and response.

b) Change Management process:

The change management process begins with authorizing changes to occur. For this purpose, a methodology should exist for prioritizing and approving system change requests.

A change request is a document containing a call for an adjustment of a system. A change request is declarative and should be in a format that ensures all changes are considered for actions and allows the system management staff to easily track the status of the request. Users and systems management should review such changes and determine whether the changes are appropriate for the organization or will negatively affect the existing system.

Q.7 (a) Disaster Planning:-

A disaster plan is a plan of action to recover from occurrences that shut down or harm major information systems. The need for such a plan is apparent from the potential impact of accidents, sabotage, and natural events. The nature and extent of an information systems disaster plan for a business depend on the role of information systems in the day-to-day operation of the business. Reliable online transaction processing systems are essential for banks, distributors, and airlines etc. For business such as these, any unplanned downtime can cut into customer service and revenues. These businesses may go to great expense maintaining redundant real-time databases in different locations, with several databases updated simultaneously whenever a transaction occur. Even businesses that use information system primarily for accounting and management reporting still need definitive plans for recovering from unexpected downtime.

b) BACKUP SCHEMES:

There are three main schemes for backup: full, incremental and differential. Each one has its advantages and disadvantages. Usually, the methods are combined, in order to complement each other.

Full Backup

This type of backup scheme copies all files and folders to the backup media, creating one backup set (with one or more media, depending on media capacity). The main advantage is having a unique repository in case of restoration, but it requires more time and media capacity.

Incremental Backup

An incremental backup copies the files and folders that changed or are new since the last incremental or full backup. If you have a full backup on day 1, your incremental backup on day 2 will copy only the changes from day 1 to day 2. On day 3, it will copy only the changes from day 2 to day 3, and so on. Incremental backup is a faster method of backup and requires less media capacity, but it requires that all backup sets restore all changes since a full backup, and restoration will take more time.

Differential Backup

A differential backup will copy all files and folders that have been added or changed since a full backup was performed. This type of backup is faster and requires less media capacity than a full backup and requires only the last full and differential backup sets to make a full restoration. It also requires less time to restore than incremental backups, but it is slower and requires more media capacity than incremental backups because data that are backed up are cumulative.

THE END