**Total Marks = 56**

## SECTION – "A"

**Q. 2 (a) OBSTACLES WHEN APPLYING INFORMATION TECHNOLOGY IN THE READ WORLD:**

Some of the obstacles to applying IT successfully in the real world of business include:

**Unrealistic expectations and techno-type:**

Computer technology has always received more than its share of speculation and hype.

In today's business world, computer mystique has expanded to encompass business and social environments that use computers extensively.

Hardware and software vendors often add to the confusion by claiming that they "sell solutions." The work system framework shows why this is misleading. Unless the totality of a problem is poor technology that can be replaced without changing anything else, technology is almost never a solution by itself.

There has also been a lot of hype about the Internet.

**Difficulty Building and Modifying IT-Based Systems:**

Today it is much easier to build IT-based than it ever has been, but the task is still difficult. The fact that IT still has a long way to go is illustrated by the enormous effort that went into the Year 2000 (Y2K) problem, which was related to the way many information systems use just two digits to identify the year portion of a date.

These generalizations are consistent with the findings of surveys concerning the success rate for information systems. A Gartner Group survey of 1,375 IT professionals in September 2000 found that roughly 40% of IT projects fail to meet business requirements.

**Difficulty Integrating IT-Based Systems:**

One of the most difficult issues related to building and maintaining IT-based systems is the requirement that these systems be integrated with the organization's other systems. This issue arises frequently when hardware and software best suited for one purpose must be used in conjunction with hardware acquired for a different purpose.

**Organizational Inertia and Problems of Change:**

A distressing reality for those who are enthusiastic about any particular technology-based innovation is that it is simply difficult to change the way an organization operates.

**Genuine Difficulty Anticipating What Will Happen:**

A final aspect of real-world limitations to IT-based innovation is that no one really knows how any particular innovation will develop or will be adapted over time. For example, the electronic transfer of money seemed like a good idea and had numerous advantages for legitimate business; however, it also allows criminals to move drug money surreptitiously.

**Q. 2 (b) THE PRINCIPLE-BASED SYSTEMS ANALYSIS (PBSA) METHOD:**

PBSA converts the four steps of systems analysis into three steps that can be pursued at whatever level of detail makes sense in the situation. These steps involve:

**Defining the Problem and the Work System:**

The first step in analyzing a system is to define the problem by identifying the purpose of the analysis and the scope of the work system that is being analyzed. The purpose is typically to accomplish a goal such as increasing the efficiency of a business process, producing a better product, or solving an employee turnover problem.

**Using Work System principles to Explore Situation and Search for Possible Improvements:**

The next phase of the analysis after defining the problem involves looking at different facets of the work system and trying to imagine potential improvements. Each of the seven work system principles is used in turn as a lens for focusing on a particular part of the work system, thinking about how well it is operating, and identifying possible directions for improvement.

**Making a Recommendation That Addresses the Problem While Supporting the Organization's Priorities:**

Analyzing a system is a fruitless exercise unless the understanding developed in the analysis is used to set a course of action. Accordingly, deciding what to do is the last step in the PBSA method. The briefest possible recommendation simply identifies a direction for change and explains something about why this type of change is a good idea.

**Q. 3 (a) FOUR SYSTEM APPROACHES OF SYSTEM LIFE CYCLES:**

The four system approaches are idealized models, each involving different processes and emphasizing different issues. Understanding these issues helps in deciding what methods to use for a project.

The traditional system life cycle establishes control to avoid developing information systems that miss the mark or are difficult to maintain.

Prototypes focus on helping users determine requirements based on real understanding. Rapid iterations of prototypes support this but often produce software that is more difficult to maintain than software designed carefully before programming begins. When the prototype takes shape, the users often wonder why they cannot put it into operation immediately.

Application packages keep company resources focused on the company's business, rather than on building information systems to support the company's business. But the company does not have compete control over how the package works. Business processes may have

to change to conform to the logic built into the package.

End-user development may be more responsive to end-user needs because it bypasses the IS department and avoids delays.

**Q. 3 (b) Determinants of Information Usefulness and Related Roles of Information Systems:**

| Characteristic | Related information system role |
|---|---|
| **Information quality** | |
| ▫ Accuracy | Control data to ensure accuracy; identify likely errors |
| ▫ Precision | Provide information with adequate precision |
| ▫ Completeness | Provide information that is complete enough for the user and situation; avoid swamping the user with excessive information |
| ▫ Age | Update information more frequently and transmit it to user more quickly |
| ▫ Timeliness | Provide information quickly enough that it is useful |
| ▫ Source | Verify source of information; provide information from preferred sources; analyze information for bias |
| **Information accessibility** | |
| ▫ Availability | Make information available with minimum effort |
| ▫ Admissibility | No automatic approach even though it is possible to provide legal guidelines in an organized form |
| **Information Presentation** | |
| ▫ Level of summarization | Manipulate the data to the desired level of summarization |
| ▫ Format | Manipulate the data to the desired format |
| **Information security** | |
| ▫ Access restriction | Use passwords or other schemes to prevent unauthorized users from accessing data or systems that process data |
| ▫ Encryption | Encrypt and decrypt the data |

**Q. 3 (c) The Convergence of Computing and Communications:**

Four aspects of the convergence of computing and communications are :

**Reliance of Telecommunications on Computers**

The earliest telephone systems included human operators who established telephone connections by plugging wires into a switchboard. Later, electromechanical switches automated this work by establishing the connections mechanically. Today, computers make the long distance connections electronically.

**Role of Telecommunication in computing**

During the first decades of computer use, people thought of computing as something that occurs when using a single computer. More recently, the convergence of computing and communications has made distributed processing more practical, with the data stored anywhere and the computing occurring anywhere.

**New Options in Wired and Wireless Transmission**

Shows how progress in wired and wireless transmission is creating a wide range of telecommunication options. In metropolitan areas, wireless transmission of radio and television broadcasts has been challenged by cable broadcasting, which can provide more choices and higher quality reception. At the same time, direct satellite broadcasting is creating a new wireless option.

**New Combinations of Data and Computing**

Some of the new combinations of data computing that have emerged by combining certain elements of telephone, telegraph, broadcasting, and data processing.

**Q. 4 (a) MEDIA MANAGEMENT:**

Media management is required to record, issue, receive and safeguard all program and data files that are maintained on removable media.

**Systems Administration:**

the system administrator is responsible for maintaining major multiuser computer systems, including local area networks (LANs), wireless local area networks (WLANs), wide area networks (WANs), personal area networks (PANs), storage area networks (SANs), intranets and extranets, and mid-range and mainframe systems.

**Security Administration:**

Security administration begins with management's commitment. Management must understand and evaluate security risks, and develop and enforce a written policy that clearly states the standards and procedures to be followed.

**Quality Assurance:**

**Quality assurance personnel** usually perform two distinct tasks:

- **Quality assurance (QA)** Helps the IS department to ensure that personnel are following prescribed quality processes.
- **Quality control (QC)** – Responsible for conducting tests or reviews to verify and ensure that software is free from defects and meets user expectations.

**Database Administration:**

The database administrator (DBA), as custodian of an organization's data, defines and maintains the data structures in the corporate database system. The DBA must understand the organization, and user data and data relationship (structure) requirements. The DBA is responsible for the actual design, definition and proper maintenance of the corporate databases.

**Network Administrators:**

Network administrators are responsible for key components of this infrastructure (routers, switches, firewalls, network segmentation, performance management, remote access, etc.). Because of geographical dispersion, each LAN may need an administrator.

**Q. 4 (b) POLICIES:**

Policies are high-level documents that represent the corporate philosophy of an organization and the strategic thinking of senior management and business process owners.

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.

**Information Security Policy:**

A security policy communicates a coherent security standard to users, management and technical staff. A security policy for information and related technology is a first step toward building the security infrastructure for technology-driven organizations.

**Procedures:**

Procedures are detailed steps defined and documented for implementing policies. They must be derived from the parent policy and must implement the spirit (intent) of the policy statement. Procedures must be written in a clear and concise manner so they may be easily and properly understood by those governed by them. Procedures document business processes (administrative and operational) and the embedded controls. Procedures are formulated by process owners as an effective translation of policies.

**INFORMATION SECURITY POLICY DOCUMENT:**

The policy document should contain:

- A definition of information security, its overall objectives and scope, and the importance of security as an enabling mechanism for information sharing.
- A statement of management intent, supporting the goals and principles of information

security in line with the business strategy and objectives.

- A framework for setting control objectives and controls, including the structure of risk assessment and risk management.
- A brief explanation of the security policies, principles, standards and compliance requirements of particular importance to the organization.
- A definition of general and specific responsibilities for information security management, including reporting information security incidents.
- References to documentation which may support the policy; e.g., more detailed security policies, standards, and procedures for specific information systems or security rules with which users should comply.

**Q. 5 (a) SAMPLING:**

The two general approaches to audit sampling are statistical and nonstatistical:

1. **Statistical sampling.** An objective method of determining the sample size and selection criteria. Statistical sampling uses the mathematical laws of probability to: a) calculate the sampling size, b) select the sample items, and c) evaluate the sample results and make the inference. With statistical sampling, the IS auditor quantitatively decides how closely the sample should represent the population (assessing sample precision) and the number of times in 100 that the sample should represent the population (the reliability or confidence level).
2. **Nonstatistical sampling (often referred to as judgmental sampling).** Uses auditor judgment to determine the method of sampling, the number of items that will be examined from a population (sample size) and which items to select (sample selection). These decisions are based on subjective judgment as to which items/transactions are the most material and most risky.

To perform attribute or variable sampling, the following statistical sampling terms need to be understood:

- Confidence coefficient
- Level of risk
- Precision
- Expected error rate
- Sample mean
- Sample standard deviation
- Tolerable error rate

- Population standard deviation

**Q. 5 (b) ROLES AND RESPONSIBILITIES OF GROUPS AND INDIVIDUALS:**

The various roles and responsibilities of groups/individuals that may be involved in the development process are summarized as follows:

- **Senior management.** Demonstrates commitment to the project and approves the necessary resources to complete the project. This commitment from senior management helps ensure involvement by those needed to complete the project.
- **User management.** Assumes ownership of the project and resulting system, allocates qualified representatives to the team, and actively participates in business process redesign, system requirements definition, test case development, acceptance testing and user training. User management should review and approve system deliverables as they are defined and implemented.
- **Project steering committee.** Provides overall direction and ensures appropriate representation of the major stakeholders in the project's outcome. The project steering committee is ultimately responsible for all deliverables, project costs and schedules.
- **Project sponsor.** Provides funding for the project and works closely with the project management to define the critical success factors (CSFs) and metrics for measuring the success of the project. It is crucial that success is translated to measurable and quantifiable terms.
- **Systems development management.** Provides technical support for hardware and software environments by developing, installing and operating the requested system. This area also provides assurance that the system is compatible with the organization's computing environment and strategic IT direction, and assumes operating support and maintenance activities after installation.
- **Project manager.** Provides day-to-day management and leadership of the project, ensures that project activities remain in line with the overall direction, ensures appropriate representation of the affected departments, ensures that the project adheres to local standards, ensures that deliverables meet the quality expectations of key stakeholders, resolves interdepartmental conflicts, and monitors and controls costs and the project timetable.
- **Systems development project team.** Completes assigned tasks, communicates effectively with users by actively involving them in the development process, works according to local standards and advises the project manager of necessary project plan deviations.

- **User project team.** Completes assigned task, communicates effectively with the systems developers by actively involving themselves in the development process as subject matter experts (SMEs), works according to local standards and advise the project manager of expected and actual project plan deviations.
- **Security officer.** Ensures that system controls and supporting processes provide an effective level of protection, based on the data classification set in accordance with corporate security policies and procedures.
- **Quality assurance (QA).** Personnel who review results and deliverables within each phase and at the end of each phase, and confirm compliance with requirements.

**THE END**