SECTION – "A"

Q. 2 (a) TYPICAL WAYS EACH TYPE OF INFORMATION SYSTEM SUPPORTS COMMUNICATION AND DECISION-MAKING:

Although people often think of information systems as tools for decision-making, each type of information system supports both communication and decision-making in a number of ways:

System Type	Impact on Communication	Impact on Decision-Making
Office automation system: provides individuals effective ways to process personal and organizational business data, to perform calculations, and to create documents	▫ Provides tools for creating documents and presentations, such as word processors and presentation systems	▫ Provides spreadsheets and other tools for analyzing information ▫ Communication tools also help in implementing decisions
Communication system: helps people work together by interacting and sharing information in many different forms	▫ Telephones and video conferencing for communication ▫ E-mail, v-mail, fax, for communication using messages and documents ▫ Access to memos and other shared information ▫ Scheduling meetings ▫ Organizing and expediting interactions during meetings ▫ Controlling flow of work	▫ Telephones and teleconferencing for decision-making ▫ E-mail, v-mail, fax, other tools for obtaining information ▫ Support sharing information related to making joint decisions
Transaction processing system (TPS): collects and stores information about transactions; controls some aspects of transactions	▫ Creates a database that can be accessed directly, thereby making some person-to-person communication unnecessary	▫ Gives immediate feedback on decisions made while processing transactions ▫ Provides information for planning and management decisions

System Type	Impact on Communication	Impact on Decision-Making
Management information system (MIS) and executive information system (EIS): converts TPS data into information for monitoring performance and managing an organization; provides executive information in a readily accessible interactive format	❑ Provides a basis of facts rather than opinions for explaining problems and their solutions ❑ May combine e-mail and other communication methods with presentation of computerized data	❑ Provides summary information and measures of performance for monitoring results ❑ May provide easy ways to analyze the types of information provided in less flexible form by older MIS
Decision support system (DSS): helps people make decisions by providing information, models, or analysis tools	❑ Analysis using DSS helps provide a clear rationale for explaining a decision	❑ Provides tools for analyzing data and building models ❑ Analysis using a DSS helps define and evaluate alternatives
Enterprise system: creates and maintains consistent data processing methods and an integrated database across multiple business functions	❑ Maintains a database that can be accessed directly, thereby making some person-to-person communication unnecessary ❑ Establishes and maintains uniformity that makes communication easier	❑ Maintains a database that provides uniform, consistent information for decision-making ❑ Establishes and maintains uniformity that makes it easier to use information while making decisions

(b) (i) EVALUATING BUSINESS PROCESS PERFORMANCE:

Business process participants and managers should be involved in designing and evaluating information systems because they have the most direct insight about the advantages and disadvantages of different levels of process performance. Seven of many possible performance variables that can be used are:

- Activity rate;
- Output rate;
- Consistency;
- Productivity;
- Cycle time;
- Downtime;
- Security.

Activity Rate and Output Rate:

Activity rate and *output rate* are separate performance variables that focus on the amount of work being done per unit of time. Like other performance variables, activity rate and output rate are determined by a combination of the ways the business process is designed, the preparation and enthusiasm of the participants, the quality of the available information, and the operation of the technology.

Output rate is the amount of output (completions) that a process produces per unit of time, whereas *activity rate* is the number of interim work steps that are performed per unit time. This distinction is important mainly for processes that take a long time to complete or are complicated.

Consistency:

Consistency in a business process means applying the same techniques in the same way to obtain the same desired results. Because one of the TQM movement's main tenets is that unwarranted variation destroys quality, TQM calls for careful specification of exactly how a process should be performed and careful monitoring to ensure that it is being performed consistent with those specifications. One of the main benefits of some information systems is that they force the organization to do things consistently.

Productivity:

Productivity is the relationship between the amount of output produced by a business process unit and the amount of money, time, and effort it consumes. It is measured in terms such as units of output per labour hour or dollar sales per month. As a firm's overall productivity improves, it can make a profit at lower selling prices. Business process productivity can be improved by changing the process to produce more output from the same level of inputs or to produce the same output from lower levels of inputs. One approach for improving productivity is to increase the rate of work, thereby reducing the labour time and inventory costs related to a particular level of output.

Cycle time:

It is easy to say time is a scarce resource, but many business processes operate as though time barely matters. For example, in conventional batch manufacturing the time during which value is actually being added often constitutes less than 5% of total manufacturing cycle time. Over 95% of the time, the product is either sitting in batches awaiting processing or being moved to another work centre. Delays of this type can be just as important in information-based processes, such the processing of insurance or loan applications.

Downtime:

The bane of computerized systems, *downtime* is the amount or percentage of time during which the process is out of operation. Downtime of a process may occur because a computer system is out of operation unexpectedly or for planned maintenance. It may also occur for any number of other reasons involving the system participants and the context. Even planned maintenance sometimes becomes an unacceptably long period of downtime.

Security:

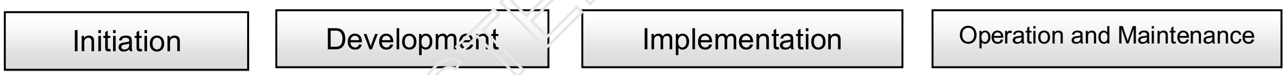
The *security* of a business process is the likelihood that it is not vulnerable to unauthorized uses, sabotage, or criminal activity. Although companies avoid discussing security issues publicly, a number of security problems are well known. One of these involves telephone fraud, in which someone steals another person's telephone credit card number and then uses it illegally.

Information systems can improve security or can weaken it. They improve security when they contain effective safeguards against unauthorized access and use. They weaken security when they remove control from people and lead the people in the system to become complacent about security concerns and to "trust the computer".

(ii) BUILDING AND MAINTAINING SYSTEMS:

Initiation is the process of defining the need to change an existing work system, identifying the people who should be involved in deciding what to do, and describing in general terms how the work system should operate differently and how any information system that supports it should operate differently. This phase may occur in response to recognized problems, such as data that cannot be found and used effectively, or high error rates in data. In other cases, it is part of a planning process in which the organization is searching for ways to improve and innovate, even if current systems pose on overt problems.

Development is the process of acquiring and configuring hardware, software, and other resources needed to perform both the required I.T-related functions and the required functions not related to I.T. This phase starts by deciding exactly how the computerized and manual parts of the work system will operate. If the hardware is not already in place, development includes purchasing and installing the hardware. If the software is not in place, it includes purchasing the software, producing it from scratch, or modifying existing software. The development phase concludes with thorough testing of the entire information system to identify and correct misunderstandings and programming errors.



Implementation is the process of making a new work system operational in the organization. This phase starts from the point when the software runs on the computer organization. This phase starts from the point when the software runs on the computer and has been tested. Activities in implementation include planning, user training, conversion to the new information system and work system, and follow up to make sure the entire system is operating effectively.

Operating and maintenance is the ongoing operation of the work system and the information system, plus efforts directed at enhancing either system and correcting bugs. At minimum, this requires that someone be in charge of ensuring that the work system is operating well, that the information system is providing the anticipated benefits, and that the work system and information system are changed further if the business situation calls for it.

The main point about the four phases is that the work of building and maintaining systems in organizations is not just technical work. Regardless of how the four phases are performed, business professionals play an important role in all four of the phases.

Q. 3 (a) METHODS FOR ACCESSING DATA IN A COMPUTER SYSTEM:

A computer system finds stored data either by knowing its exact location or by searching for the data. Different DBMSs contain different internal methods for storing and retrieving data. Three methods that could be used: sequential access, direct access, and indexed access. Programmers set up DBMSs to use whatever method is appropriate for the situation, and shield users from technical details of data access.

Sequential Access:

The earliest computerized data processing used *sequential access,* in which individual records within a single file are processed in sequence until all records have been processed or until the processing is terminated for some other reason. Sequential access is the only method for data stored on tape, but it can also be used for data on a direct access device such as a disk. Sequential processing makes it unnecessary to know the exact location of each data item because data are processed according to the order in which they are sorted.

Direct Access:

Processing events as they occur requires *direct access,* the ability to find an individual item in a file immediately. Magnetic disk storage was developed to provide this capability. To understand how direct access works, imagine that the phone directory described earlier is stored on a hard disk. For example, a user needing Sam Patterson's telephone number enters that name into the computer system. A program uses a mathematical procedure to calculate the approximate location on the hard disk where Sam Patterson's phone number is stored. Another program instructs the read head to move to that location to find the data. Using the same logic to change George Butler's phone number, one program calculates a location for the phone number, and another program directs the read head to store the new data in that location.

Index Access:

A third method for finding data is to use *indexed access.* An *index* is a table used to find the location of data. The example in figure shows how indexed access to data operates. The index indicates where alphabetical groups of names are stored. For instance, Palla to Pearson are on track 43. The user enters the name Sam Patterson. The program uses the index to decide where to start searching for the phone number.

Using indexes makes possible to perform both sequential processing and direct access efficiently. Therefore, access to data using such indexes is often called the *indexed sequential access method (ISAM).*

Although they solve many problems, using indexes also causes complications. Once again, these are the details the DBMS and technical staff take care of because most users have neither the desire nor the need to think about them.

(b) LEVELS OF INTEGRATION:

Integration is mutual responsiveness and collaboration between distinct activities or processes. The five levels of integration include common culture, common standards, information sharing, coordination, and coloration. The extent of integrations between two processes or activities is related to the speed with which one responds to events in the other. This speed depends on both the immediacy of communication and the degree to which the processes respond to the information communicated. Information systems can play roles in both aspects of integration, first by supporting the communication, and second by making it easier for each business process to use the information to respond effectively.

Five Levels of Integration:

The first two levels are conditions that make it easier to work together, although they are not inherently related to responsiveness and typically exist for reasons totally outside of any particular business process. Longtime employees of dissimilar organization that have merged are painfully aware that cultural differences make it more difficult to communicate and work together.

Sharing information, the third level of coordination, is the least obtrusive way to attain responsiveness between processes. Information sharing occurs when all the lawyers working on a large legal case can easily access any document about the case, or when the sales force can access a manufacturing database to determine available capacity for additional orders. This approach to integration to integration sounds easier than it really is because personal and political incentives in the organization often motivate people not to share.

Coordination, the fourth level of integration, can be defined as managing dependencies among activities. These dependencies might involve the synchronization of inputs and outputs among activities, such as not starting manufacturing steps until the materials have arrived. They might involve the sharing of resources, such as machines or people who cannot do two things at once. They also might involve the fit between outputs, such as when several engineers are designing different parts of the same product.

By attaining collaboration, the fifth level of integration, interdependence between processes is so strong that their unique identity begins to disappear. To develop products more quickly and to make them easier to manufacture, for example, many firms have moved toward product development processes that involve close collaboration between marketing, engineering, and manufacturing. These highly collaborative processes try to minimize the problems of less integrated approaches in which marketing handed requirements to engineering, which then produced a product design that could not be manufactured economically. Full collaboration between different parts of a business is effective for some product design processes, but in most other situations it contradicts the efficiencies of applying the division of labour and assigning different types of tasks to different people.

The difference between information sharing, coordination, and collaboration is especially important for thinking about potential benefits of moving toward e-business. Although often touted as a major benefit of e-business approaches, genuine coordination or collaboration requires much more than just sharing the same information. Network technology can provide information access, but coordination and collaboration require active commitment by the participants. The level of integration designed into a business process should therefore be consistent with the level of integration the participants are ready to accept and commit to.

Tightly integrated (also called tightly coupled) systems are also more prone to catastrophic failure than less integrated systems. Tightly coupled systems have little slack, require that things happen in a particular order, and depend on all components to operate within particular ranges. When one component fails, the others may also fail immediately. The most tightly coupled systems in our society include aircraft, nuclear power plants, power grids, and automated warfare systems.

SECTION – "B"

Q. 4 (a) EVIDENCE:

Evidence is any information used by the IS auditor to determine whether the entity or data being audited follows the established criteria or objectives, and supports audit conclusions. It is a requirement that the auditor's conclusions be based on sufficient, relevant and competent evidence. When planning the IS audit, the IS auditor should take into account the type of audit evidence to be gathered, its use as audit evidence to meet audit objectives and its varying levels of reliability.

Audit evidence may include the IS auditor's observations (presented to management), notes taken from interview, material extracted from correspondence and internal documentation or contracts with external partners, or the results of audit test procedures. While all evidence will assist the IS auditor in developing audit conclusions, some evidence is more reliable than others. The rules of evidence and sufficiency as well as the competency of evidence must be taken into account as required by audit standards.

DETERMINANTS FOR EVALUATING THE RELIABILITY OF AUDIT EVIDENCE:

Determinants for evaluating the reliability of audit evidence include:

Independence of the provider of the evidence:

Evidence obtained from outside source is more reliable than from within the organization. This is why confirmation letters are used for verification of accounts receivable balances. Additionally, signed contracts or agreements with external parties could be considered, reliable if the original documents are made available for review.

Qualification of the individual providing the information/ evidence:

Whether the providers of the information/ evidence are inside or outside of the organization, the IS auditor should always consider the qualifications and functional responsibilities of the person providing the information. This can also be true of the IS auditor. If an IS auditor does not have a good understanding of the technical area under review, the information gathered from testing that area may not be reliable, especially if the IS auditor does not fully understand the test.

Objectivity of the evidence:

Objective evidence is more reliable than evidence that requires considerable judgment or interpretation. An IS auditor's review of media inventory is direct, objective evidence. An IS auditor's analysis of the efficiency of an application, based on discussions with certain personnel, may not be objective audit evidence.

Timing of the evidence:

The IS auditor should consider the time during which information exists or is available in determining the nature, timing and extent of compliance testing and, if applicable, substantive testing. For example, audit evidence processed by dynamic systems, such as spreadsheets, may not be retrievable after a specified period of time if changes to the file are not controlled or the files are not backed up.

The IS auditor gathers a variety of evidence during the audit. Some evidence may be relevant to the objectives of the audit, while other evidence may be considered peripheral. The IS auditor should focus n the overall objectives of the review and not the nature of the evidence gathered.

(b) PROJECT PHASES OF PHYSICAL ARCHITECTURE ANALYSIS:

Review of Existing Architecture:

To start the process, the latest documents about the existing architecture must be reviewed. Participants of the first workshop will be specialists of the ICT department in all areas directly impacted by physical architecture. Examples are server, storage, security and overall I.T infrastructure.

Special care must be taken in characterizing all the operational constraints that impact physical architecture such as:

- Ground issues;
- Size limits;
- Weight limits

- Current power supply;
- Physical security issues.

The output of the first workshop is a list of components of the current infrastructure and constraints defining the target physical architecture.

Analysis and Design:

After reviewing the existing architecture, the analysis and design of the actual physical architecture has to be undertaken, adhering to best practices and meeting business requirements.

Draft Functional Requirements:

With the first architecture design in hand, the first (draft) of functional requirements is composed. This material is the input for the next step and the vendor selection process.

Vendor and Product Selection:

While the draft functional requirements are written, the vendor selection process proceeds in parallel.

Writing Functional Requirements:

After finishing the draft functional requirements and feeding the second part of this project, the functional requirements document is written, which will be introduced at the second architecture workshop with staff from all affected parties.

Proof of Concept:

Establishing a POC is highly recommended to prove that the selected hardware and software are able to meet all expectations, including security requirements. The deliverable of the POC should be a running prototype, including the associated document and test protocols describing the tests and their results.

To start, the POC should be based on the results of the procurement phase. For this purpose, a reprehensive subset of the target hardware is used. The software to run the POC can be either test versions or software already supplied by the vendor; therefore, additional costs are expected to be minimal.

Planning Implementation of Infrastructure:

To ensure the quality of the results, it is necessary to use a phased approach to fit the whole puzzle together. It is also fundamental to setup the communication process to other projects like those described earlier. Through these different phases the components are fit together, and a clear understanding of the available and contactable vendor is established by using the selection process during the procurement phase and beyond. Furthermore, it is necessary to select the scope of key business and technical requirements to prepare the next steps, which include the development of the delivery, installation and test plans. Moreover, to ensure a future proven solution, it is crucial to choose the right partners with the right skills.

During the four different phases it is necessary to fit all the components together to get prepared for projects downstream (e.g., data migration).

Procurement Phase:

During the procurement phase the communication processes is established with the analysis project to get an overview of the chosen solution and determine the quantity structure of the deliverables. The requirements statements are also produced.

Delivery Time:

During the delivery time phase, the delivery plan is developed. This phase overlaps in some parts with the procurement phase.

The delivery plan should include topics such as priorities, goals, and nongoals, key indicators, progress on key tasks, and responsibilities.

Installation Plan:

During the installation planning phase, the installation plan is developed in cooperation with all affected parties.

An additional step is to review the plan with the involved parties and of course with those responsible for this integration projects. This is an iterative process.

Installation Test Plan:

Based on the known dependencies of the installation plan, the test plan is developed.

Q. 5 (a) CONTROL SELF ASSESSMENT (CSA):

Control self assessment (CSA) can be defined as a management technique that assures stakeholders, customers and other parties that the internal control system of the organization is reliable. It also ensures that employees are aware of the risks to the business and they conduct periodic, proactive reviews of controls. It is a methodology used to review key business objectives, risks involved in achieving the business objectives and internal controls designed to manage these business risks in a formal, documented collaborative process.

Objectives of CSA:

There are several objectives associated with adopting a CSA program. The primary objective is to leverage the internal audit function by shifting some of the control monitoring responsibilities to the functional areas. It is not intended to replace audit's responsibilities, but to enhance them. Auditees such as line managers are responsible for controls in their environment; the managers also should be responsible for monitoring the controls. CSA programs also must educate management about control design and monitoring, particularly concentration on areas of high risk. These programs are not just policies requiring clients to comply with control standards. Instead, they offer a variety of support ranging from written suggestions outlining acceptable control environments to in-depth workshops, when workshops are included in the program, an additional objective – the empowerment of workers to assess or even design the control environment – may be included in the program.

When employing a CSA program, measure of success for each phase (planning, implementation and monitoring) should be developed to determine the value derived from CSA and its future use.

Benefits of CSA:

Some of the benefits of a CSA include the following:

- Early detection of risks;
- More effective and improved internal controls;
- Creation of cohesive teams through employee involvement;
- Developing a sense of ownership of the controls in the employees and process owners, and reducing their resistance to control improvement initiatives;
- Increased employee awareness of organizational objectives, and knowledge of risks and internal controls;
- Increased communication between operational and top management;
- Highly motivated employees;
- Improved audit rating process;
- Reduction in control cost;
- Assurance provided to stakeholders and customers;
- Necessary assurance given to top management about the adequacy of internal controls as required by the various regulatory agencies and laws such as the US Sarbanes-Oxley Act.

Disadvantages of CSA:

CSA does potentially contain several disadvantages which include:

- It could be mistaken as an audit function replacement;
- It may be regarded as an additional workload (e.g., one more report to be submitted to management);
- Failure to act on improvement suggestions could damage employee morale;
- Lack of motivation may limit effectiveness in the detection of weak controls.

(b) (i) IS auditor can play a preventive or detective role in the testing process.

ELEMENTS OF A SOFTWARE TESTING PROCESS:

To guide the testing process and help ensure that all the facets of the system function as expected, basic elements for application software testing activities have been defined and include:

- **Test Plan:**

  Developed early in the life cycle and refined until the actual testing phase, test plans identify the specific portions of the system to be tested. Test plans may include a categorization of types of deficiencies that can be found during the test. Categories of such deficiencies may be system defects, incomplete requirements, designs, specifications, or errors in the test case itself. Test plans also specify severity levels of problems found as well as guidelines on identifying the business priority.

  The project sponsor, end-user management and the project manager decide early in the test phase on the severity definitions. Test plans also identify test approaches, such as the two reciprocal approaches, to software testing, bottom up and top down.

- **Conduct and Report Test Results:**

  Describe resources implied in testing, including personnel involved and information resources / facilities used during the test as well as actual vs. expected test results. Results reported, along with the test plan, should be retained as part of the system's permanent documentation.

- **Address Outstanding Issues:**

  Identify errors and irregularities from the actual tests conducted. When such problems occur, the specific tests in question have to be redesigned in the test plan until acceptable conditions occur when the test are redone.

TESTING CLASSIFICATIONS:

The following tests relate, to varying degrees, to the above approaches that can be performed based on the size and complexity of the modified system:

- **Unit Testing:**

  The testing of an individual program or module. Unit testing uses a set of test cases that focus on the control structure of the procedural design. These tests ensure that the internal operation of the program performs according to specification.

- **Interface or Integration Testing:**

  A hardware or software test that evaluates the connection of two or more components that pass information from one area to another. The objective is to take unit-tested modules and build an integrated structure dictated by design. The term integration testing is also used to refer to test that verify and validate the functioning of the application under test with other systems, where a set of data is transferred from one system to another.

- **System Testing:**

  A series of tests designed to ensure that modified programs, objects, database schema, etc., which collectively constitute a new or modified system, function properly. These test procedures are often performed in a nonproduction test/ development environment by software developers designated as a test team. The following specific analyses may be carried out during system testing:

  - **Recovery testing:**

    Checking the system's ability to recover after a software or hardware failure.

  - **Security testing:**

    Making sure the modified/ new system include provisions for appropriate access controls and does not introduce any security holes that might compromise other systems.

  - **Load testing:**

    Testing an application with large quantities of data to evaluate its performance during peak hours.

  - **Volume testing:**

    Studying the impact on the application by testing with an incremental volume of records to determine the maximum volume of records (data) that the application can process.

  - **Stress testing:**

    Studying the impact on the application by testing with an incremental number of concurrent users/ services the application can process.

  - **Performance testing:**

    Comparing the system's performance to other equivalent systems using well-defined benchmarks.

- **Final Acceptance Testing:**

  After the system staff is satisfied with their initial and/ or system tests, the modified system is ready for the acceptance testing, which occurs during the implementation phase. During this testing phase, the defined methods of testing to apply should be incorporated into the organization's QA methodology. Final acceptance testing has two major parts: quality assurance testing (QAT) focusing on technical aspects of the application, and user acceptance testing (UAT) focusing on functional aspect of the application. QAT and UAT have different objectives and therefore should not be combined.

(ii) CORPORATE GOVERNANCE:

Ethical issues, decision making and overall practices within an organization must be fostered through corporate governance practices. Corporate governance has been defined as 'the system by which business corporations are directed and controlled'.

More specifically, corporate governance is a set of responsibilities and practices used by an organization's management to provide strategic direction, thereby ensuring that goals are achievable, risks are properly addressed and organizational resources are properly utilized. Corporate governance also provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined. Good corporate governance should provide proper incentives for the board and management to pursue objectives that are the interests of the company and its shareholders and should facilitate effective monitoring'.

I.T GOVERNANCE:

I.T governance, one of the domains of the enterprise governance, comprises the body of issues addressed in considering how I.T is applied within the enterprise.

Effective enterprise governance focuses individual and group expertise and experiences on specific areas where they can be most effective. Information technology, long considered only an enabler of an organization's strategy, is now regarded as an integral part of that strategy. Chief executive officers (CEOs) chief operating officers (COOs), chief financial officers (CFOs), chief information officers (CIOs) and chief technology officers (CTOs) agree that strategic alignment between I.T and enterprise objectives is a success factor. I.T governance helps achieve this critical success factor by economically, efficiently and effectively deploying secure, reliable information and applied technology. Information technology is so critical to the success of enterprises that it cannot be relegated to either I.T management or I.T specialists, but must receive the attention of both in coordination with senior management.

AUDIT ROLE IN I.T GOVERNANCE:

I.T is now intrinsic and pervasive within enterprises rather than being a separate function marginalized from the rest of the enterprise. How I.T is applied within the enterprise will have an immense effect on whether enterprise will attain its mission, vision or strategic goals. For this reason, an enterprise needs to evaluate its I.T governance since it is an important part of the overall enterprise governance.

Audit plays a significant role in the successful implementation of I.T governance within an organization. Audit is well positioned to provide leading practice recommendations to senior management to help improve the quality and effectiveness of the I.T governance initiatives implemented.

As an entity monitors compliance, audit helps ensure compliance with I.T governance initiatives implemented within an organization. The continual monitoring, analysis and evaluation of metrics associated with I.T governance initiatives require an independent and balanced view to ensure a qualitative assessment that subsequently facilitates the qualitative improvement of I.T processes and associated I.T governance initiatives.

THE END