SECTION – "A"

Q. 2 (a) WHAT IS AN INFORMATION SYSTEM PLAN?

A plan is a statement of what will be done, who will do it, when they will do it, how it will be done, and what are the desired results. At the strategic level. IS plans focus on priorities and goals for information systems and the technical and organizational approaches that will be used. At the project level, they focus on specific capabilities required in each system and on who will do what and when will they do it to produce specific results.

The work of planning, building, and managing information systems can be viewed in work system terms and can be described, evaluated, and improved just like any other work system. The same issues apply, such as identifying the customer and product of the business process and attaining alignment between the business process, participants, information technology, and the result expected by the customer.

Q. 2 (b) WHY DO USERS AND MANAGERS HAVE TO PARTICIPATE IN INFORMATION SYSTEM PLANNING AND DEVELOPMENT?

Even though the IS department compiles the IS plan, members of user departments have to ensure that the right systems are developed, are used efficiently and effectively, and have the desired impact.

A firm's IS department is usually responsible for producing the IS plan in conjunction with the user departments, such as marketing and finance. As happens in other departments, managers in the IS department start the planning process by reviewing their progress on the existing plan. They look at special problems, such as systems approaching technical obsolescence. They confer with managers in the user departments to learn about user priorities and needs for system improvements, new systems, and user support. IS department management also look at the needs of their own department such as training, hiring, and personnel development.

Many questions and issues arise in producing and reviewing an initial IS plan. Users are often frustrated by how long it takes to build new systems and how much effort it takes to make what might seem like small changes to existing systems. The IS department often feels frustrated by its inability to keep up with many of the business's pressing problems.

It is especially important to allocate resources carefully because most firms don't come close to having the IT resources needed to develop all of the information systems that people in the company say they need. It is not unusual for a central IS department to have more than a two-year backlog of committed projects, with many other requests simply turned down or never submitted formally because of the minimal chance that they would be acted upon.

Q. 2 (c) ELECTRONIC COMMUNICATION SYSTEMS:

Electronic communication systems help people work together by exchanging or sharing information in many different forms. New communication capabilities have changed the way many business operate by making it possible to do many things at a distance that previously required being present in a specific location.

1. Teleconferencing:

The use of electronic transmission to permit same-time, different-place meetings is called teleconferencing. We can think of a traditional telephone call as a minimal teleconference, but the term normally is applied to other options including audio conferencing, audiographic conferencing, and video conferencing.

2. Instant Messaging and Chat Rooms:

The Internet brought several additional forms of online messaging that have seen wide use. One of these is instant messaging, the ability to direct a message to someone on your "buddy list" who happens to be online when you are. All you do is click on a list that highlights your "buddies" who happen to be online, type a message, and it appears immediately on your buddy's screen. The other form of messaging is an online chat room, an ongoing, informal computer conference that someone can join, participate in, and then leave.

3. Groupware:

Coined in the late 1980s, the term groupware refers to software and related procedures that help teams work together by sharing information and by controlling internal workflows. This relatively new and still somewhat unshaped type of communication system has attained wide recognition due to the increasing need for dispersed teams to work together effectively at a distance at a distance as a result of downsizing and rapid organizational change. Groupware starts with messaging but goes further by facilitating access to documents and controlling team-related workflows. Many groupware products are related to specific group-related tasks such as project management, scheduling meetings ("calendaring"), and retrieving data shared databases.

4. Intranets and Extranets:

The widespread use of the World wide Web has led many firms to apply the information sharing concepts of groupware on a much larger scale by creating a fourth type of communication system, intranets and extranets. Intranets are private communication networks that use the type of interface popularized by the Web but are accessible only by authorized employees, contractors, and customers. They are typically used to communicate nonsensitive but broadly useful information such as recent corporate news, general product information, employee manuals, corporate policies, telephone directories, details of health insurance and

other employee benefits, and calendars.

Extranets:

Extranets are private networks that operate similarly to intranets but are directed at customers rather than at employees. Extranets provide many types of information customers need, such as detailed product descriptions, frequently asked questions about different products, maintenance information, warranties, and how to contact customer service and sales offices. Much of this information was formerly difficult for customers to access because paper versions of it at the customer site became scattered and outdated. By using extranets, companies are making this type of information increasingly available at a single interactive site that is easy to navigate.

5. Knowledge Management:

Today's leading businesses are increasingly aware that the knowledge of their employees is one of their primary assets. In consulting companies and other organizations that rely heavily on unique competencies and methods, knowledge has more competitive significance than physical assets because the physical assets can be replaced or replenished easily.

Knowledge management systems are communication systems designed to facilitate the sharing of knowledge rather than just information. As with groupware, the idea of knowledge management is still emerging and is applied in many different ways in different firms. Tacit knowledge and explicit knowledge require different types of knowledge management efforts.

6. Group Support Systems:

A form of groupware called a group support system (GSS) supports communication by helping facilitate meetings. The original idea was an offshoot of DSS research and was originally called group decision support systems (GDSS), although many of the people associated with these systems have shifted the term to GSS because many meetings are directed at brainstorming, discussions, and other purposes that may not be linked directly to decisions.

In its original concept, a GDSS was a specially outfitted conference room containing hardware and software that facilitates meetings. This technology may include advanced presentation devices, computer access to databases, and capabilities permitting the participants in a meeting to communicate electronically. These rooms improve same-time, same-place communication by a group of people working together in a meeting. The meeting's purpose could be anything from brainstorming about possible new product features to reviewing business operations or responding to an emergency.

Q. 3 (a) Customers think about product performance in terms of a variety of performance variables. Other possible criteria, such as image and aesthetics, are not included because information

systems usually affect them only indirectly.

Notice that these variables often interacts, sometimes by working together and sometimes by working in opposite directions. Despite the overlaps and contradictions, it is useful to consider ways in which each of these variables helps clarify the customer's view of how good the product is and how it might be improved. At least a few of the five product performance variables could be irrelevant in any particular situation, but each performance variable should be considered, if for no other reason than to assure yourself that it is not important in a given situation.

1. Cost:

Cost is a prime determinant of customer satisfaction. When considering cost, we are not thinking about it in a strict accounting sense but as what the internal or external customer must give up in order to obtain, use, and maintain the product of a work system. Often called the total cost of ownership (TCO), this includes money plus time, effort, and attention that could be used for other purposes. This view of cost illustrates how the product of any work system involves cost to the internal or external customer even when no money is transferred.

2. Quality:

The concept of quality has been interpreted many different ways and spans many aspects of performance. Even though product quality is often linked to the consistency of the process that produced the product, we will view quality as a criterion by which the customer evaluates the product.

For our purposes, quality refers to the customer's perception that the product has desired features and that these features are in line with the product's costs. As in the example of increasingly computerized automobiles, incorporation of information systems into physical products sometimes provides capabilities and aesthetic features associated with quality. For information products, the perception of quality is related to accessibility and usefulness, such as the way graphical user interfaces made it easier for nonprogrammers to extract data from databases. For services, the perception of quality is related to whether the service seems complete and whether it is delivered attentively.

3. Responsiveness:

With regard to customer satisfaction, responsiveness means taking timely action based on what the customer wants, such as when a sales clerk uses a company-wide inventory system to find an out-of-stock item at another store and has it shipped to the customer's home. As another example, many architectural firms now use computer-aided design systems to provide simulated walk-throughs of proposed buildings, this sometimes enables them to make immediate modifications based on customer feedback. The highest levels of responsiveness often require creating or modifying a product or service based on a specific customer's needs, thereby increasing its value for that customer.

4. Reliability:

The reliability of a work system's product refers to the likelihood that it will not fail when the customer wants to use it. Although computerizing work systems often creates an additional layer of structure that increases reliability, there is no way to guarantee that computers are programmed correctly or that communication networks will always stay up.

5. Conformance to Standards and Regulations:

Adherence to standards and regulations imposed by external bodies such as major customers, industry groups, or the government is a crucial issue for the product of many work systems. We will call performance in this area conformance to standards and regulations. Unlike cost and quality, conformance does not play a direct role in the return on investment, yet it is the driving force behind the way many work systems operate.

Q. 3 (b) Common Roles of Information Systems in Improving the Product of a Work System.

Product performance variable	Typical measures	Common information system roles
Cost	▫ Purchase price ▫ Cost of ownership ▫ Amount of time and attention required	▫ Reduce internal cost of business process or increase productivity, making it easier to charge or allocate lower prices to customers ▫ Improve product performance in ways that reduce the customer's internal costs
Quality	▫ Defect rate per time interval or per quantity of output ▫ Rate of warranty returns ▫ Perceived quality according to customer	▫ Insure the product is produced more consistently ▫ Make it easier to customize the product for the customer ▫ Build information systems into the product to make it more usable or maintainable
Responsiveness	▫ Time to respond to customer request ▫ Helpfulness of response	▫ Improve the speed of response ▫ Systematize communication with customers ▫ Increase flexibility to make it easier to respond to what the customer wants
Reliability	▫ Average time to failure ▫ Failure rate per time interval ▫ Compliance to customer commitment dates	▫ Make the business process more consistent ▫ Make the business process more secure ▫ Build features into the product that make it more reliable on its own right
Conformance to standards and regulations	▫ Existence of nonconformance ▫ Rate of complaints about nonconformance.	▫ Clarify the standards and regulations so that it is easier to determine whether they are being followed ▫ Systematize work to make the output more consistent

Q. 3 (c) Efficiency – effectiveness – Relation to Work System Framework:

Customers may not even perceive distinction between external and internal aspects of

performance, which is often summarized as the difference between efficiency and effectiveness. Efficiency involves doing things in the right way, whereas effectiveness involves doing the right things, Efficiency is an internal view focusing on how well resources are used within a work system to produce a particular output. Typical internal performance measures related to efficiency include business process measures such as consistency, productively, and cycle time. Effectiveness is an external view related to whether the products and services produced are what the customer really wants. It is measured in terms of things the customer perceives directly, such as the cost, quality, and responsiveness. Although they are measured separately and should be considered separately, efficiency usually has an impact on effectiveness because work done well is more likely to produce good results than work done poorly.

Performance variables can be described or measured at different levels of clarity. Quality experts are adamant that careful performance measurement is essential for process improvement.

A work system is a system in which human participants and/or machines perform a business process using information, technology, and other resources to produce products and/or services for internal or external customers. Typical business organizations have work systems for obtaining materials from suppliers, producing and delivering end products, finding customers, creating financial reports, hiring employees, coordinating work across departments, and many other functions.

- The **customers** are the people who use and receive direct benefits from the products and services produced by the work system. They may be external customers who receive the organization's products and/or services or they may be internal customers inside the organization.
- The **products & services** are the combination of physical things, information, and services that the work system produces for its customers. The work system exists to produce these products and services.
- The **business process** is the set of work steps or activities that are performed within the work system. These steps may be defined precisely in some situations or may be relatively unstructured in other. In some situations, different participants might perform the same steps differently based on differences in their skills, training, and interests.
- The **participants** are people who perform the work steps in the business process. Some participants may use computers and information technology extensively, whereas others may use little or no technology.
- The **information** is the information used by the participants to perform their work. Some of the information may be computerized, but other important information may never be captured on a computer.

- The **technology** is the hardware, software, and other tools and equipment used by the participants while doing their work. The technology considered to be within a work system is dedicated to that system, whereas technical infrastructure I s technology shared with other systems.
- **Context** is the organizational, competitive, technical, and regulatory realm within which the work system operates. These environmental factors affect the system's performance even though the system does not rely on them directly in order to operate.
- **Infrastructure** is shared human and technical resources that the work system relies on even though these resources exist and are managed outside of it. This typically includes human infrastructure such as support and training staff, information infrastructure such as shared databases, and technical infrastructure such as networks and programming technology.

Information system is often important to recognize that work system participants may give higher priority to aspects of the work system not related to the information system.

Even when looking at a Web site, referring to participants in a work system instead of users of a Web site emphasizes the way work system participants perform a business process, rather than the less significant topic of how they interact with a computer while performing certain business process steps.

A work system to serve its participants is a direct way to encourage the participants to perform their to the fullest. Assuring they have the right skills and providing the right tools makes it easier for them to achieve satisfaction from doing a job well. This also shows that the organization actually cares about what they are doing. Providing appropriate work conditions, such as a reasonable workload, stress level, degree of autonomy, and possibilities for personal growth, encourages interest and commitment by demonstrating that the organization genuinely cares about serving the participants.

Work systems have impacts on their participants even though many of these systems are designed as though their impacts on participants were irrelevant or unimportant. The nature of these impacts depends on a participant's individual characteristics because people bring vastly different capabilities and backgrounds to their work. Highly structured, repetitive systems may be fine for some participants, but unsatisfying for others with different skills or personality traits. Applying technology to change a work system may foster personal learning and growth by instilling jobs with a more appropriate degree of engagement and challenge.

Q. 4 (a) RISK MANAGEMENT

Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives and deciding what countermeasures (safeguards or controls), if any, to take in reducing risk to an acceptable level (i.e., residual risk), based on the value of the information resource to the organization.

Effective risk management begins with a clear understanding of the organization's appetite for risk. This drives all risk management efforts and, in an IT context, impacts future investments in technology, the extent to which IT assets are projected and the level of assurance required. Risk management encompasses identifying, analyzing, evaluating, treating, monitoring and communicating the impact of risk on IT processes. Having defined risk appetite and identified risk exposure, strategies for managing risk can be set and responsibilities clarified. Depending on the type of risk and its significance to the business, management and the board may choose to:

- Avoid e.g., where feasible, choose not to implement certain activities or processes that would incur risk (i.e., eliminate the risk by eliminating the cause).
- Mitigate e.g., lessen the probability or impact of the risk by defining, implementing, and monitoring appropriate controls.
- Transfer (deflect, or allocate) e.g., share risk with partners or transfer via insurance coverage, contractual agreement, or other means.
- Accept i.e., formally acknowledge the existence of the risk and monitor it.

In other words, risk can be avoided, reduced, transferred, or accepted. An organization can also choose to reject risk by ignoring it, which can be dangerous and should be considered a red flag by the IS auditor.

To develop a risk management program:

Establish the purpose of the risk management program:

The first step is to determine the organization's purpose for creating a risk management program. The program's purpose may be to reduce the cost of insurance or reduce the number of program-related injuries. By determining its intention before initiating risk management planning, the organization can define key performance indicators (KPIs) and evaluate the results to determine its effectiveness. Typically, senior management, with the board of directors, set the tone for the risk management program.

Assign responsibility for the risk management plan:

The second step is to designate an individual or team responsible for developing and implementing the organization's risk management program. While the team is primarily responsible for the risk management plan, a successful program requires the integration of risk management within all levels of the organization. Operations staff and board members should assist the risk management committee in identifying risk and developing suitable loss control and intervention strategies.

Q. 4 (b) RISK ANALYSIS METHODS

Qualitative Analysis Methods:

Qualitative risk analysis methods use word or descriptive rankings to describe the impacts or

likelihood. They are the simplest and most frequently used methods. They are normally based on checklists and subjective risk ratings such as high, medium or low.

Semi-quantitative Analysis Methods:

In semi-quantitative analysis, the descriptive rankings are associated with a numeric scale. Such methods are frequently used when it is not possible to utilize a quantitative method or to reduce subjectivity in qualitative methods.

Quantitative Analysis Methods:

Quantitative analysis methods use numeric value to describe the likelihood and impacts of risks, using data from several types of a sources such as historic records, past experiences, industry practices and records, statistical theories, testing, and experiments.

Many quantitative risk analysis methods are currently used by military, nuclear, chemical, financial and other areas. The following selections describe concepts related to quantitative methods.

Many organizations refer to quantitative risk analysis which expresses risk in numeric (e.g. monetary) terms. A quantitative risk analysis is generally performed during a business impact analysis (BIA). The main problem within this process is the valuation of information assets. Different individuals may assign different values to the same asset, depending on the relevance of information to the individual. In the case of technology assets, it is not the cost of the asset that is considered but also the cost of replacement and the value of information processed by that asset.

Q. 4 (c) CHANGEOVER (GO-LIVE OR CUTOVER) TECHNIQUES:

Changeover refers to an approach to shift users from using the application from the existing (old) system to the replacing (new) system. This is appropriate only after testing the new system with respect to its program and relevant dates. This is sometimes called the go-live technique since it enables the start of the new system. This approach is also called the cutover technique since it helps in cutting out from the older system and moving over to the power system.

This technique can be achieved in three different ways.

Parallel Changeover:

This technique includes running the old system, then running both the old and new systems in parallel, and finally fully changing over to the new system after gaining confidence in the working of the new system. With this approach the users will have to use both systems during the period of overlap. This will minimize the risk of using the newer system, and at the same time help in identifying problems, issues or any concerns that the user comes across in the newer system in the beginning. After a period of overlap the user gains confidence and assurance in relying on the newer system. At this point, the use of the older system is

discontinued and the new system becomes totally operational.

Phased Changeover:

In this approach the older system is broken into deliverable modules. Initially, the first module of the older system is phased out using the first module of the newer system. Then, the second module of the older system is phased out, using the second module of the newer system and so forth until reaching the last module. Thus, the changeover from the older system to the newer system takes place in a preplanned, phased manner.

Some of the risk areas that may exist in the phased changeover include:

- Resource challenges (both on the IT side to be able to maintain two unique environment such as hardware, operating systems, databases and code; and on the operations side to be able to maintain user guides, procedures and policies, definitions of system terms, etc.)
- Extension of the project life cycle to cover two systems
- Change management for requirements and customizations to maintain ongoing support of the older system.

Abrupt Changeover:

In this approach the newer system is changed over from the older system on a cutoff date and time, and the older system is discontinued once changeover to the new system takes place.

Changeover to the newer system involves four major steps or activities:

1. Conversion of files and programs; test running on test bed
2. Installation of new hardware, operating system, application system and the migrated data
3. Training employees or users in groups
4. Scheduling operations and test running for go-live or changeover.

Some of the risk areas related to changeover include:

- Asset safeguarding
- Data integrity
- System effectiveness
- System efficiency
- Change management challenges (depending on the configuration items considered)
- Duplicate or missing records (duplicate or erroneous records may exist if data cleaning is not done correctly)

Q. 5 (a) THE EVOLVING IS AUDIT PROCESS:

The IS audit process must continually change to keep pace with innovations in technology. These evolving changes include areas such as automated work papers, integrated auditing

and continuous auditing.

Automated Work Papers:

Increasingly, audit teams are creating their audit work papers (risk analysis, audit programs, results, test evidences, conclusions, reports and other complementary information such as business information) in automated format, using specialized applications designed for this purpose.

Although auditors often use office automation packages such as text/word processors or spreadsheets, standard audit work paper packages are being implemented in more medium to large audit departments, and are proving to be useful and appropriate to help facilitate audit work.

In such cases, rules regarding integrity, confidentiality and availability of audit records should be applied that are equivalent to those required for hard copy or printed documents. Minimum controls that should be addressed include:

- Audit trails-including when a document was changed, who performed the modification, automated update of a document version, when it was changed.
- Automated features to provide and record approvals (e.g., by audit director, managers, etc.) of audit phases (audit program, conclusions, reports).
- Security and integrity controls regarding the operating system, databases and communication channels (e.g., server under audit control, corporate network, exporting documents, exclusive server).
- Backup and restore procedures
- Encryption techniques to provide confidentiality.

Integrated auditing:

Dependence of business processes on information technology has necessitated that traditional financial and operational auditors develop an understanding of IT control structure, and IS auditors develop an understanding of the business control structures. Integrated auditing can be defined as the process whereby appropriate audit disciplines are combined to assess key internal controls over an operation, process or entity.

The integrated approach focuses on risk. A risk analysis assessment aims to understand and identify risks arising from the entity and its environment, including relevant internal controls. At this stage, the role of IT audit is typically to understand and identify risks under topical areas such as information management, IT infrastructure, IT government and IT operations. Other audit specialists will seek to understand the organizational environment, business risks and business controls. A key element of the integrated approach is discussion of the risks arising among the whole audit team, with consideration of impact and likelihood.

Detailed audit work then focuses on the relevant controls in place to manage these risks. IT systems frequently provide a first line of preventive and detective controls, and the integrated audit approach depends on a sound assessment of their efficiency and effectiveness.

The integrated audit process typically involves:

- Identification of risks faced by the organization for the area being audited.
- Identification of relevant key controls.
- Review and understanding of the design of key controls.
- Testing that key controls are supported by the IT system.
- Testing that management controls operate effectively.
- A combined report or opinion on control risk, design and weaknesses.

Continuous Auditing:

The focus on increased effectiveness and efficiency of assurance, internal auditing and control has spurred the development of new studies and examination of new ideas concerning continuous auditing as opposed to more traditional periodic auditing reviews. Several research studies and documents addressing the subject carry different definitions of continuous auditing. All studies, however, recognize that a distinctive character of continuous auditing is the short time lapse between the facts to be audited, the collection of evidence and audit reporting.

Traditional financial reports and the traditional audit style sometime prove to be insufficient because they lack the essential element in today's business environment updated information. Therefore, continuous auditing appears to be gaining more and more followers.

Some of the drivers of continuous auditing are a better monitoring of financial issues within a company, ensuring that real-time transactions also benefit for real-time monitoring, prevention of financial fraud and audit scandal. Continuous auditing involves a large amount of work because the company practicing continuous auditing will not provide one report at the end of a quarter, but will provide financial reports on a more frequent basis.

Continuous auditing has an intrinsic edge over point-in-time or periodic auditing because it captures internal control problems as they occur, preventing negative effects. Implementation can also reduce possible or intrinsic audit inefficiencies such as delays, planning time, inefficiencies of the audit process, overhead due to work segmentation, multiple quality or supervisory reviews, or discussions concerning the validity of findings.

Q. 5 (b) EFFECT OF LAWS AND REGULATIONS ON IS AUDIT PLANNING:

Each organization, regardless of its size or the industry within which it operations, will need to comply with a number of governmental and external requirements related to computer system practices and controls and to the member in which computers, programs and data are stored

and used. Additionally business regulations can impact the way date are processed, transmitted and stored (stock exchange, central banks, etc.)

Special attention should be given to these issues in those industries that, historically, have been closely regulated. For example, the banking industry worldwide has severe penalties for companies and their officers should a company be unable to provide an adequate level of service because of substandard backup and recovery procedures. Also, Internet service providers (ISPs) are subject, in several countries, to specific laws regarding confidentiality and service availability.

IS auditors should review management's privacy policy to ascertain whether it takes into account the requirements of applicable privacy laws and regulations, including transborder data flow requirements such as Safe Harbor and the Organization for Economic Cooperation and Development (OECD) guidelines governing the protection of privacy and transborder flows of personal data.

Several countries, because of growing dependencies on information systems and related technology, are making efforts to establish added layers of regulatory requirements concerning IS audit. The contents of these legal regulations regard:

- Establishment of the regulatory requirements
- Organization of the regulatory requirements
- Responsibilities assigned to the corresponding entities
- Correlation to 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.

THE END