PAPER – 6: INFORMATION SYSTEMS CONTROL AND AUDIT

*Question No. **1** is compulsory.*

*Candidates are required to answer any **four** questions*

*from the remaining **five** questions.*

Question 1

XYZ Limited is involved in trading of high-quality readymade garments. This company has several branches in India as well as in abroad. The company wants to use a system of integrated applications to manage the business and automate many back-office functions related to technology, services, and human resources across its branches. So, the company is planning to implement an ERP system to take care of all such issues. Also, by considering the importance of sensitive databases, there are many control activities involved in maintaining the integrity of the database. In addition, senior management of the company has appointed a high-level IT Steering Committee to discuss IT related issues.

You are appointed as an IT consultant in the company to discuss the implementation of new system. Please answer the following queries raised by management of XYZ Limited.

(a) Describe the key functions of the IT Steering Committee to provide overall direction to the management of the company. ***(6 Marks)***

(b) As an IT consultant of the XYZ Limited, how do you define ERP and convince the management of the company to implement ERP by explaining its components? ***(5 Marks)***

(c) Existence/Backup controls ensure the existence of the database by establishing backup and recovery procedures. Discuss various backup strategies to ensure the existence of the database. ***(3 Marks)***

Answer

(a) The key functions of IT Steering Committee to provide overall direction to the management of the Company are as follows:

- To ensure that long and short-range plans of the IT department are in tune with enterprise goals and objectives.
- To establish size and scope of IT function and sets priorities within the scope.
- To review and approve major IT deployment projects in all their stages.
- To approve and monitor key projects by measuring result of IT projects in terms of return on investment, etc.
- To review the status of Information Systems plans, budgets and overall IT performance.
- To review and approve standards, policies, and procedures.
- To make decisions on all key aspects of IT deployment and implementation.

- To facilitate implementation of IT security within enterprise.
- To facilitate and resolve conflicts in deployment of IT and ensure availability of a viable communication system exists between IT and its users.
- To report to the Board of Directors on IT activities on a regular basis.

(b) **Enterprise Resource Planning (ERP)** is process management software that allows an organization to use a system of integrated applications to manage the business and automate many back-office functions related to technology, services, and human resources.

The components of ERP are as follows:

(i) **Software Component:** The software component is the component that is most visible part and consists of several modules such as Finance, Human Resource, Supply Chain Management, Supplier Relationship Management, Customer Relationship, and Business Intelligence.

(ii) **Process Flow:** It is the model that illustrates the way how information flows among the different modules within an ERP system. By creating this model, it becomes easier to understand how ERP works.

(iii) **Customer mindset:** By implementing ERP system, the old ways for working which user understand and comfortable with, have to be changed and may lead to users' resistance. For example, some users may say that they have spent many years doing an excellence job without help from ERP system. To lead ERP implementation to succeed, the company needs to eliminate negative value or belief that users may carry toward utilizing new system.

(iv) **Change Management:** In ERP implementation, change needs to be managed at several levels - User attitude; resistance to change; and Business process changes.

(c) Various Backup strategies to ensure the existence of the database are as follows:

- **Dual recording of data:** Under this strategy, two complete copies of the database are maintained. The databases are concurrently updated.
- **Periodic dumping of data:** This strategy involves taking a periodic dump of all or part of the database onto some backup storage medium – magnetic tape, removable disk, optical disk etc. The dump may be scheduled.
- **Logging input transactions:** This involves logging the input data transactions which cause changes to the database. Normally, this works in conjunction with a periodic dump.
- **Logging changes to the data:** This involves copying a record each time it is changed by an update action.

Question 2

(a) Being an IT consultant, Management wants your advice by explaining the characteristics of Cloud Computing. Briefly explain any six characteristics of Cloud Computing. ***(6 Marks)***

(b) Feasibility study is carried out by the system analysts so that the most feasible and desirable system can be selected for development. Explain the technical issues usually raised during the feasibility stage of Preliminary Investigation phase of SDLC. ***(5 Marks)***

(c) Which factors related to Legal Considerations and Audit Standards should be considered by an Information System Auditor as a part of his/her Preliminary Review? ***(3 Marks)***

Answer

(a) The characteristics of Cloud Computing are as follows:

- **High Scalability:** Cloud environments enable servicing of business requirements for larger audiences, through high scalability.
- **Agility:** The cloud works in the 'distributed mode' environment. It shares resources among users and tasks, while improving efficiency and agility (responsiveness).
- **High Availability and Reliability:** Availability of servers is supposed to be high and more reliable as the chances of infrastructure failure are minimal.
- **Multi-sharing:** With the cloud working in a distributed and shared mode, multiple users and applications can work more efficiently with cost reductions by sharing common infrastructure.
- **Services in Pay-Per-Use Mode:** Service Level Agreements between the provider and the user must be defined when offering services in pay per use mode. This may be based on the complexity of services offered. Application Programming Interfaces (APIs) may be offered to the users so they can access services on the cloud by using these APIs.
- **Virtualization:** This technology allows servers and storage devices to increasingly share and utilize applications, by easy migration from one physical server to another.
- **Performance:** It is monitored and consistent and loosely coupled architectures are constructed using web services as the system interface.
- **Maintenance:** The Cloud Computing applications are easier because they are not to be installed on each user's computer and can be accessed from different places.

(b) The technical issues usually raised during the feasibility stage of Preliminary Investigation phase of System Development Life Cycle (SDLC) are as follows:

- Does the necessary technology exist to do what is suggested and can it be acquired?
- Does the proposed equipment have the technical capacity to hold the data required to use the new system?

- Can the proposed application be implemented with existing technology?
- Will the proposed system provide adequate responses to inquiries, regardless of the number or location of users?
- Can the system be expanded if developed?
- Are there technical guarantees of accuracy, reliability, ease of access, and data security?

(c) The factors which should be considered by an Information System Auditor related to Legal consideration and Audit standards as a part of his/her Preliminary Review are as follows:

- The auditor should carefully evaluate the legal as well as statutory implications on his/her audit work.
- The Information Systems audit work could be required as part of a statutory requirement in which case he should take into consideration the related stipulations, regulations, and guidelines for conduct of his audit.
- The statutes or regulatory framework may impose stipulations as regards minimum set of control objectives to be achieved by the subject organization. Sometimes, this may also include restrictions on the use of certain types of technologies. For example - freeware, shareware etc.
- The IS Auditor should also consider the Audit Standards applicable to his conduct and performance of audit work. Non-compliance with the mandatory audit standards would not only impact on the violation of the code of professional ethics but also have an adverse impact on the auditor's work.

Question 3

(a) Management of a company wants to collect the information, which is written onto a special audit file - the SCARF master files. As an IS Auditor of the company, briefly explain the types of information, which can be collected using the SCARF technique. ***(6 Marks)***

(b) Program development and implementation is a major phase within the System Development Life Cycle. Explain the various phases, along with their controls, of Program Development Life Cycle. ***(5 Marks)***

(c) Service Strategy of ITIL framework provides guidance on clarification and prioritization of service provider investments in services. Describe any three Service Strategies under ITIL framework. ***(3 Marks)***

Answer

(a) Auditors collect the following types of information using System Control Audit Review File (SCARF) technique:

- **Application System Errors:** SCARF audit routines provide an independent check on the quality of system processing, whether there are any design and programming

errors as well as errors that could creep into the system when it is modified and maintained.

- **Policy and Procedural Variances:** Organizations have to adhere to the policies, procedures and standards of the organization and the industry to which they belong. SCARF audit routines can be used to check when variations from these policies, procedures and standards have occurred.
- **System Exception:** SCARF can be used to monitor different types of application system exceptions. For example - salespersons might be given some leeway in the prices they charge to customers. SCARF can be used to see how frequently salespersons override the standard price.
- **Statistical Sample:** Some embedded audit routines might be statistical sampling routines. SCARF provides a convenient way of collecting all the sample information together on one file and use analytical review tools thereon.
- **Snapshots and Extended Records:** Snapshots and extended records can be written into the SCARF file and printed when required.
- **Profiling Data:** Auditors can use embedded audit routines to collect data to build profiles of system users. Deviations from these profiles indicate that there may be some errors or irregularities.
- **Performance Measurement:** Auditors can use embedded routines to collect data that is useful for measuring or improving the performance of an application system.

(b) Various phases of Program Development Life Cycle along with their controls are as follows:

Phase	Controls
Planning	Techniques like Work Breakdown Structures (WBS), Gantt charts and PERT (Program Evaluation and Review Technique) Charts can be used to monitor progress against plan.
Control	The Control phase has two major purposes: o Task progress in various software life-cycle phases should be monitored against plan and corrective action should be taken in case of any deviations. o Control over software development, acquisition, and implementation tasks should be exercised to ensure software released for production use is authentic, accurate, and complete.
Design	A systematic approach to program design, such as any of the structured design approaches or object-oriented design is adopted.
Coding	Programmers must choose a module implementation and integration strategy (like Top-down, Bottom-up and Threads approach), a coding strategy (that follows the percepts of structured programming), and a

	documentation strategy (to ensure program code is easily readable and understandable).
Testing	Testing ensures that a developed or acquired program achieves its specified requirements. Three types of testing can be undertaken: ○ **Unit Testing** – which focuses on individual program modules. ○ I**ntegration Testing** – which focuses on groups of program modules. ○ **Whole-of-Program Testing** – which focuses on whole program.
Operation and Maintenance	Management establishes formal mechanisms to monitor the status of operational programs so maintenance needs can be identified on a timely basis. Three types of maintenance can be used are as follows: ○ **Repair Maintenance** – in which program errors are corrected. ○ **Adaptive Maintenance** – in which the program is modified to meet changing user requirements. ○ **Perfective Maintenance** - in which the program is tuned to decrease the resource consumption.

(c) The Service strategies under Information Technology Infrastructure Library (ITIL) framework are as follows:

- **IT Service Generation:** IT Service Management (ITSM) refers to the implementation and management of quality information technology services and is performed by IT service providers through People, Process, and Information Technology.
- **Service Portfolio Management:** IT portfolio management is the application of systematic management to the investments, projects, and activities of enterprise Information Technology (IT) departments.
- **Financial Management:** Financial Management for IT Services' aim is to give accurate and cost-effective stewardship of IT assets and resources used in providing IT Services.
- **Demand Management:** Demand management is a planning methodology used to manage and forecast the demand of products and services.
- **Business Relationship Management:** Business Relationship Management is a formal approach to understanding, defining, and supporting a broad spectrum of inter-business activities related to providing and consuming knowledge and services via networks.

Question 4

(a) You are appointed as an IT consultant to assess the potential impacts resulting from various events or incidents in the process of Business Continuity Management. What are the activities that you will perform while making Business Impact Analysis? ***(6 Marks)***

(b) You are appointed to audit the Information Systems of XYZ Limited. Board of Directors of the company desires you to enlighten them on various categories of Information System Audit. What are the points you will cover when you enlighten them? ***(5 Marks)***

(c) Continuous auditing enables auditors to significantly reduce and perhaps to eliminate the time difference between occurrence of the events and the auditor's assurance services thereon. Explain the advantages of Continuous Audit Techniques. ***(3 Marks)***

Answer

(a) The activities that are performed while making the Business Impact Analysis (BIA) are as follows:

- Assess the impacts that would occur if the activity was disrupted over a period of time.
- Identify the maximum time period after the start of a disruption within which the activity needs to be resumed.
- Identify critical business processes.
- Assess the minimum level at which the activity needs to be performed on its resumption.
- Identify the length of time within which normal levels of operation need to be resumed.
- Identify any inter-dependent activities, assets, supporting infrastructure or resources that have also to be maintained continuously or recovered over time.

(b) Information Systems Audit has been categorized into five types:

(i) **Systems and Application:** An audit to verify that systems and applications are appropriate, are efficient, and are adequately controlled to ensure valid, reliable, timely, and secure input, processing, and output at all levels of a system's activity.

(ii) **Information Processing Facilities:** An audit to verify that the processing facility is controlled to ensure timely, accurate, and efficient processing of applications under normal and potentially disruptive conditions.

(iii) **Systems Development:** An audit to verify that the systems under development meet the objectives of the organization and to ensure that the systems are developed in accordance with generally accepted standards for systems development.

(iv) **Management of IT and Enterprise Architecture:** An audit to verify that IT management has developed an organizational structure and procedures to ensure a controlled and efficient environment for information processing.

(v) **Telecommunications, Intranets, and Extranets:** An audit to verify that controls are in place on the client (end point device), server, and on the network connecting the clients and servers.

(c) The advantages of Continuous Audit Techniques are given as under:

- **Timely, Comprehensive and Detailed Auditing:** Evidence would be available more timely and in a comprehensive manner. The entire processing can be evaluated and analysed rather than examining the inputs and the outputs only.
- **Surprise test capability:** As evidence are collected from the system itself by using continuous audit techniques, auditors can gather evidence without the systems staff and application system users being aware that evidence is being collected at that particular moment. This brings in the surprise test advantages.
- **Information to system staff on meeting of objectives:** Continuous audit techniques provide information to systems staff regarding the test vehicle to be used in evaluating whether an application system meets the objectives of asset safeguarding, data integrity, effectiveness, and efficiency.
- **Training for new users:** Using the Integrated Test Facility (ITFs), new users can submit data to the application system, and obtain feedback on any mistakes they make via the system's error reports.

Question 5

(a) The success of the process of ensuring business value from the use of IT can be measured by evaluating the benefits realized from IT enabled investments and services portfolio and how efficiently IT costs, benefits and risk are implemented. Briefly explain the key metrics, which can be used for such evaluation. ***(6 Marks)***

(b) Explain the functions performed by Indian Computer Emergency Response Team in the area of Cyber Security to serve as national agency under Section 70B of IT Act. ***(5 Marks)***

(c) Bring out the differences between the terminologies, Risk, Threat, Attack and Vulnerability with respect to IT Risk Management. ***(3 Marks)***

Answer

(a) Key metrics which can be used for evaluating the benefits realized from IT enabled investments and services portfolio and how efficiently IT costs, benefits and risks are implemented are as follows:

- Percentage of IT enabled investments where benefit realization monitored through full economic life cycle.
- Percentage of IT services where expected benefits realized.
- Percentage of IT enabled investments where claimed benefits met or exceeded.
- Percentage of investment business cases with clearly defined and approved expected IT related costs and benefits.
- Percentage of IT services with clearly defined and approved operational costs and expected benefits.

- Satisfaction survey of key stakeholders regarding the transparency, understanding and accuracy of IT financial information.

(b) According to [Section 70B] of Information Technology Act, 2000; the Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of Cyber Security:

- Collection, analysis, and dissemination of information on cyber incidents.
- Forecast and alerts of cyber security incidents.
- Emergency measures for handling cyber security incidents.
- Coordination of cyber incidents response activities.
- Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents.
- Such other functions relating to cyber security as may be prescribed.

(c) The terminologies are defined as under:

- **Risk:** Risk can be defined as the potential harm caused if a particular threat exploits a particular vulnerability to cause damage to an asset. Information Systems can generate many direct and indirect risks that may lead to a gap between the need to protect systems and the degree of protection applied. Risk areas that could have a significant impact on critical business operations may include external dangers from hackers leading to denial of service and virus attacks, extortion, leakage of corporate information etc.
- **Threat:** Any entity, circumstance, or event with the potential to harm the software system or component through its unauthorized access, destruction, modification, and/or Denial of service is called a Threat. A threat is an action, event, or condition where there is a compromise in the system, its quality and ability to inflict harm to the organization. A threat cannot exist without a target asset and has the capability to attack on a system with intent to harm. Threats are typically prevented by applying some sort of protection to assets.
- **Attack:** An attack is an attempt to gain unauthorized access to the system's services or to compromise the system's dependability. In software terms, an attack is a malicious intentional fault, usually an external fault that has the intent of exploiting vulnerability in the targeted software or system. Basically, it is a set of actions designed to compromise Confidentiality, Integrity or Availability (CIA) or any other desired feature of an information system. Simply, it is the act of trying to defeat IS safeguards. The type of attack and its degree of success determines the consequence of the attack.

- **Vulnerability:** Vulnerability is the weakness in the system safeguards that exposes the system to threats. It may be a weakness in information system/s, cryptographic system or security systems, or other components like system security procedures, hardware design, internal controls, that could be exploited by a threat. Vulnerabilities potentially "allow" a threat to harm or exploit the system. For example, vulnerability could be a poor access control method allowing dishonest employees (the threat) to exploit the system to adjust their own records. In other words, Vulnerability can be referred as the weakness of the software which can be exploited by the attackers. Vulnerabilities can originate from flaws on the software's design, defects in its implementation, or problems in its operation. For example - leaving the front door unlocked makes the house vulnerable to unwanted visitors, and short passwords (less than 6 characters) make the automated information system vulnerable to password cracking or guessing routines.

Question 6

(a) You are appointed as a consultant for maintaining the system aspects of SDLC. Explain different categories of System Maintenance. ***(6 Marks)***

(b) You have been appointed as a manager of a company. What knowledge should be possessed by you as a business manager to operate the company's Information Systems effectively and efficiently? ***(5 Marks)***

(c) Write a short note on the Audit of Security Management Controls. ***(3 Marks)***

OR

Explain the different ways in which organizations can reduce paper consumption under Green IT. ***(3 Marks)***

Answer

(a) The phase of System Maintenance in System Development Life Cycle (SDLC) can be categorized in the following ways:

- **Scheduled Maintenance:** Scheduled maintenance is anticipated and can be planned for operational continuity and avoidance of anticipated risks. For example, the implementation of a new inventory coding scheme can be planned in advance, security checks may be promulgated etc.
- **Rescue Maintenance:** Rescue maintenance refers to previously undetected malfunctions that were not anticipated but require immediate troubleshooting solution. A system that is properly developed and tested should have few occasions of rescue maintenance.
- **Corrective Maintenance:** Corrective maintenance deals with fixing bugs in the code or defects found during the executions. A defect can result from design errors, logic errors coding errors, data processing and system performance errors. The need for

corrective maintenance is usually initiated by bug reports drawn up by the end users. Examples of corrective maintenance include correcting a failure to test for all possible conditions or a failure to process the last record in a file.

- **Adaptive Maintenance:** Adaptive maintenance consists of adapting software to changes in the environment, such as the hardware or the operating system. The term environment in this context refers to the totality of all conditions and influences, which act from outside upon the system. The need for adaptive maintenance can only be recognized by monitoring the environment. For example - business rule, government policies, work patterns, software, and hardware operating platforms.
- **Perfective Maintenance:** Perfective maintenance mainly deals with accommodating to the new or changed user requirements and concerns functional enhancements to the system and activities to increase the system's performance or to enhance its user interface.
- **Preventive Maintenance:** Preventive maintenance concerns with the activities aimed at increasing the system's maintainability, such as updating documentation, adding comments, and improving the modular structure of the system. The long-term effect of corrective, adaptive and perfective changes increase the system's complexity. As a large program is continuously changed, its complexity which reflects deteriorating structure, increases unless work is done to maintain or reduce it. This work is known as preventive change.

(b) As a Business Manager, following knowledge should be possessed to operate Information Systems (IS) effectively and efficiently:

- **Foundation Concepts:** It includes fundamental business, and managerial concepts. For example- 'What are components of a system and their functions', or 'What competitive strategies are required'.
- **Information Technologies (IT):** It includes operation, development and management of hardware, software, data management, networks, and other technologies.
- **Business Applications:** It includes major uses of IT in business steps like - processes, operations, decision making, and strategic and competitive advantage.
- **Development Processes:** It comprises how end users and IS specialists develop and execute business/IT solutions to problems.
- **Management Challenges:** It includes 'how the function and IT resources are maintained' and utilized to attain top performance and build the business strategies.

(c) Audit of Security Management Controls includes the following:

- Auditors must evaluate whether security administrators are conducting ongoing, high-quality security reviews or not.

- Auditors check whether the organizations audited have appropriate, high-quality disaster recovery plan in place.
- Auditors check whether the organizations have opted for an appropriate insurance plan or not.

OR

Different ways in which organizations can reduce paper consumption under Green IT are as follows:

- Reduce paper consumption by use of e-mail and electronic archiving.
- Use of "track changes" feature in electronic documents, rather than redline corrections on paper.
- Use online marketing rather than paper-based marketing; e-mail marketing solutions that are greener, more affordable, flexible, and interactive than direct mail; free and low-cost online invoicing solutions that help cut down on paper waste.
- While printing documents; make sure to use both sides of the paper, recycle regularly, use smaller fonts and margins, and selectively print required pages.