PAPER – 6: INFORMATION SYSTEMS CONTROL AND AUDIT

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

*Candidates are also required to answer any **five** questions*

*from the remaining **six** questions.*

Question 1

ABC Corporation desires to implement an Expert System to manage suspicious transactions, financial forecast, etc. in order to facilitate informed decision making, by various stake holders of the corporation. You have been appointed as IT manager to setup domain-specific and high quality knowledge based system and to enhance internal controls to maintain data integrity and security. Moreover, to help managers in making better decisions, the company decided to develop and implement Information System following System Development Life Cycle (SDLC) approach of system development. The top management of the Corporation is seeking your views on the following issues to be explained in brief:

(a) Some of the business application areas of Expert System.

(b) Knowledge areas required by a business manager to operate Information System in effective and efficient manner.

(c) Interrelated components of internal controls as per COSO (Committee of Sponsoring Organization)

(d) Various evaluation methods in post implementation review in respect to user satisfaction with the Information System. ***(4 x 5 = 20 Marks)***

Answer

(a) Some of the business application areas of Expert Systems are as follows:

- **Accounting and Finance -** It provides tax advice and assistance, helping with credit-authorization decisions, selecting forecasting models, providing investment advice.
- **Marketing -** It provides establishing sales quotas, responding to customer inquiries, referring problems to telemarketing centers, assisting with marketing timing decisions, determining discount policies.
- **Manufacturing -** It helps in determining whether a process is running correctly, analyzing quality and providing corrective measures, maintaining facilities, scheduling job-shop tasks, selecting transportation routes, assisting with product design and faculty layouts.
- **Personnel -** It is useful in assessing applicant qualifications and assisting employees in filling out forms.
- **General Business -** It helps in assisting with project proposals, recommending acquisition strategies, educating trainees, and evaluating performance.

(b) To operate Information Systems (IS) effectively and efficiently, a business manager should have knowledge in the following areas:

- **Foundation Concepts –** It includes fundamental business and managerial concepts e.g. '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 i.e. processes, operations, decision making, and strategic/competitive advantage.
- **Development Processes –** It comprises how end users and Information Systems 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) As per COSO (Committee of Sponsoring Organization), Internal Control is comprised of following five interrelated components:

- **Control Environment:** This includes the elements that establish the control context in which specific accounting systems and control procedures must operate. The control environment is manifested in management's operating style, the ways authority and responsibility are assigned, the functional method of the audit committee, the methods used to plan and monitor performance and so on. For each business process, an organization needs to develop and maintain a control environment including categorizing the criticality and materiality of each business process, plus the owners of the business process.
- **Risk Assessment:** This includes the elements that identify and analyse the risks faced by an organisation and the way the risk can be managed. Both external and internal auditors are concerned with errors or irregularities that cause material losses to an organisation. Each business process comes with various risks. A control environment must include an assessment of the risks associated with each business process.
- **Control Activities:** This includes the elements that operate to ensure transactions are authorized, duties are segregated, adequate documents and records are maintained, assets and records are safeguarded and independent checks on performance and valuation of records. These are called accounting controls. Internal auditors are also concerned with administrative controls to achieve effectiveness and efficiency objectives. Control activities must be developed to manage, mitigate, and reduce the risks associated with each business process. It is unrealistic to expect to eliminate risks completely.

- **Information and Communication:** These are the elements, in which information is identified, captured and exchanged in a timely and appropriate form to allow personnel to discharge their responsibilities. These are associated with control activities regarding information and communication systems of the entity that acts as one of the components of internal accounting system. These enable an organization to capture and exchange the information needed to conduct, manage, and control its business processes.
- **Monitoring:** The internal control process must be continuously monitored with modifications made as warranted by changing conditions. This includes the elements that ensure internal controls operate reliably over time. The best internal controls are worthless if the company does not monitor them and make changes when they are not working.

(d) Various evaluation methods in post-implementation review in respect to user satisfaction with the Information System include the following:

- **Development Evaluation:** Evaluation of the development process is primarily concerned with whether the system was developed on schedule and within budget. It requires schedules and budgets to be established in advance and that record of actual performance and cost be maintained. However, it may be noted that very few information systems have been developed on schedule and within budget. In fact, many information systems are developed without clearly defined schedules or budgets. Due to the uncertainty and mystique associated with system development, they are not subjected to traditional management control procedures.
- **Operational Evaluation:** The evaluation of the information system's operation pertains to whether the hardware, software and personnel are capable to perform their duties. It tries to answer the questions related to functional aspects of the system. Such an evaluation is relatively straightforward if evaluation criteria are established in advance. For example, if the systems analyst lays down the criterion that a system, which can support one hundred terminals should give response time of less than two seconds, evaluation of this aspect of system operation can be done easily after the system becomes operational.
- **Information Evaluation:** An information system should also be evaluated in terms of information it provides or generates. This aspect of system evaluation is difficult and it cannot be conducted in a quantitative manner, as is the case with development and operational evaluations. The objective of an information system is to provide information to a considerable extent to support the organizational decision system. Therefore, the extent to which information provided by the system is supportive to decision making is the area of concern in evaluating the system.

Question 2

(a) You have been appointed as the IS Auditor of a Company. Can you please explain the different steps involved in the conduct of your Information System Audit. ***(6 Marks)***

(b) What are the ways in which remote and distributed data processing applications can be controlled in relation to issues and revelations related to logical access? ***(6 Marks)***

(c) As an IS Auditor, what are the key areas you would verify during review of BCM arrangement of an Enterprise? Write any four. ***(4 Marks)***

Answer

(a) The different steps involved in the conduct of Information Systems Audit are as follows:

(i) **Scoping and pre-audit survey:** Auditors determine the main area/s of focus and any areas that are explicitly out-of-scope, based on the scope-definitions agreed with management. Information sources at this stage include background reading and web browsing, previous audit reports, pre-audit interview, observations and, sometimes, subjective impressions that simply deserve further investigation.

(ii) **Planning and preparation:** During which the scope is broken down into greater levels of detail, usually involving the generation of an audit work plan or risk-control-matrix.

(iii) **Fieldwork:** This step involves gathering of evidence by interviewing staff and managers, reviewing documents, and observing processes etc.

(iv) **Analysis:** This step involves desperately sorting out, reviewing and trying to make sense of all that evidence gathered earlier. SWOT (Strengths, Weaknesses, Opportunities, and Threats) or PEST (Political, Economic, Social, and Technological) techniques can be used for analysis.

(v) **Reporting:** Reporting to the management is done after analysis of evidence is gathered and analysed. Analysis and reporting may involve the use of automated data analysis tools such as ACL, IDEA, Excel, Access and hand-crafted SQL queries.

(vi) **Closure:** Closure involves preparing notes for future audits and follow up with management to complete the actions they promised after previous audits.

(b) The ways in which remote and distributed data processing applications can be controlled in relation to issues and revelations related to logical access are as follows:

- Remote access to computer and data files through the network should be implemented.
- Having a terminal lock can assure physical security to some extent.
- Applications that can be remotely accessed via modems and other devices should be controlled appropriately.

- Terminal and computer operations at remote locations should be monitored carefully and frequently for violations.
- To prevent the unauthorized user's access to the system, there should be proper control mechanisms over system documentation and manuals.
- Data transmission over remote locations should be controlled. The location which sends data should attach needed control information that helps the receiving location to verify the genuineness and integrity.
- When replicated copies of files exist at multiple locations, it must be ensured that all are identical copies contain the same information and checks are also done to ensure that duplicate data does not exist.

(c) As an Information Systems (IS) Auditor, the key areas that would be verified during review of BCM arrangement of an enterprise are as follows:

- All key products and services and their supporting critical activities and resources have been identified and included in the enterprise's BCM strategy;
- The enterprise's BCM policy, strategies, framework and plans accurately reflect its priorities and requirements (the enterprise's objectives);
- The enterprise' BCM competence and its BCM capability are effective and fit-for-purpose and will permit management, command, control and coordination of an incident;
- The enterprise's BCM solutions are effective, up-to-date and fit-for-purpose and appropriate to the level of risk faced by the enterprise;
- The enterprise's BCM maintenance and exercising programs have been effectively implemented;
- BCM strategies and plans incorporate improvements identified during incidents and exercises and in the maintenance program;
- The enterprise has an ongoing program for BCM training and awareness;
- BCM procedures have been effectively communicated to relevant staff and that those staff understand their roles and responsibilities; and
- Change control processes are in place and operate effectively.

Question 3

(a) What are the benefits of COBIT 5? ***(6 Marks)***

(b) Integrated Test Facility (ITF) is one of the continuous audit tool. Explain how ITF is used in continuous audit by an auditor. ***(6 Marks)***

(c) Describe the provision related to 'Compensation for failure to protect data' under Section 43A and 'Penalty for failure to furnish information return, etc.' under Section 44 of the Information Technology Act, 2000. ***(4 Marks)***

Answer

(a) COBIT 5 frameworks can be implemented in all sizes of enterprises and have the following benefits:

- A comprehensive framework such as COBIT 5 enables enterprises in achieving their objectives for the governance and management of enterprise IT.
- The best practices of COBIT 5 help enterprises to create optimal value from IT by maintaining a balance between realizing benefits and optimizing risk levels and resource use.
- COBIT 5 enables IT to be governed and managed in a holistic manner for the entire enterprise, taking in the full end-to-end business and IT functional areas of responsibility, considering the IT related interests of internal and external stakeholders.
- COBIT 5 helps enterprises to manage IT related risk and ensures compliance, continuity, security and privacy.
- COBIT 5 enables clear policy development and good practice for IT management including increased business user satisfaction.
- The key advantage in using a generic framework such as COBIT 5 is that it is useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector.
- COBIT 5 supports compliance with relevant laws, regulations, contractual agreements and policies.

(b) Following are the ways through which an auditor may use Integrated Test Facility (ITF) as a continuous audit tool:

- **Methods of Entering Test Data:** The transactions to be tested must be tagged. The application system should be programmed to recognize the tagged transactions and have them invoke two updates - one to the application system master file record and one to the ITF dummy entity. Auditors can also embed audit software modules in the application system programs to recognize transactions having certain characteristics as ITF transactions.

  The auditors may also use test data that is specially prepared. Test transactions would be entered along with the production input into the application system. In this approach, the test data is likely to achieve more complete coverage of the execution paths in the application system to be tested than selected production data and the application system does not have to be modified to tag the ITF transactions and to treat them in a special way.

- **Methods of Removing the Effects of ITF Transactions:** The presence of ITF transactions within an application system affects the output results obtained. The effects of these transactions must be removed. The application system may be programmed to recognize ITF transactions and to ignore them in terms of any processing that might affect users. Another method would be the removal of effects of ITF transactions by submitting additional inputs that reverse the effects of the ITF transactions. Another less used approach is to submit trivial entries so that the effects of the ITF transactions on the output are minimal. The effects of the transactions are not really removed.

(c) Section 43A of Information Technology Act, 2000 is as follows:

[Section 43A] Compensation for failure to protect data

Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, to the person so affected.

Section 44 of Information Technology Act, 2000 is as follows:

[Section 44] Penalty for failure to furnish information return etc.

If any person who is required under this Act or any rules or regulations made there under to -

(a) furnish any document, return or report to the Controller or the Certifying Authority, fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure;

(b) file any return or furnish any information, books or other documents within the time specified therefore in the regulations fails to file return or furnish the same within the time specified therefore in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues;

(c) Maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

Question 4

(a) What are the key management practices to implement risk management? ***(6 Marks)***

(b) Briefly describe the audit issues relating to operational layer with respect to the application security control auditing, ***(6 Marks)***

(c) State the advantages and disadvantages of Full Backup type. ***(4 Marks)***

Answer

(a) The key management practices for implementing risk management are as follows:

- **Collect Data:** Identify and collect relevant data to enable effective IT related risk identification, analysis and reporting.

- **Analyze Risk:** Develop useful information to support risk decisions that consider the business relevance of risk factors.
- **Maintain a Risk Profile:** Maintain an inventory of known risks and risk attributes including expected frequency, potential impact, and responses, and of related resources, capabilities, and current control activities.
- **Articulate Risk:** Provide information on the current state of IT- related exposures and opportunities in a timely manner to all required stakeholders for appropriate response.
- **Define a Risk Management Action Portfolio:** Manage opportunities and reduce risk to an acceptable level as a portfolio.
- **Respond to Risk:** Respond in a timely manner with effective measures to limit the magnitude of loss from IT related events.

(b) The audit issues relating to the Operational Layer with respect to the application security control auditing are provided below. Auditor needs to check that there is no violation of the below mentioned principles as any violation of these may have serious repercussions.

- **User Accounts and Access Rights:** This includes defining unique user accounts and providing them access rights appropriate to their roles and responsibilities. Auditor needs to always ensure the use of unique user IDs, and these needs to be traceable to individual for whom created. In case, guest IDs are used, then test of same should also be there. Likewise, vendor accounts and third-party accounts should be reviewed. Users and applications should be uniquely identifiable.
- **Password Controls:** In general; password strength, password minimum length, password age, password non-repetition and automated lockout after three attempts should be set as a minimum. Auditor needs to check whether there are applications where password controls are weak. In case such instances are found, then auditor may look for compensating controls against such issues.
- **Segregation of Duties:** As frauds, due to collusions / lack of segregations increase across the world, importance of the Segregation of Duties also increases. Segregation of duties is a basic internal control that prevents or detects errors and irregularities by assigning to separate individuals' responsibility for initiating and recording transactions and custody of assets to separate individuals. Example to illustrate:
  - Record keeper of asset must not be asset keeper.
  - Cashier who creates a cash voucher in system, must not have right to authorize payments.
  - Maker must not be checker.

(c) Advantages of Full Backup type are as follows:

- Restores are fast and easy to manage as the entire list of files and folders are in one backup set.
- Easy to maintain and restore different versions.

Disadvantages of Full Backup type are as follows:

- Backups can take very long as each file is backed up again every time the full backup is run.
- Consumes the most storage space compared to incremental and differential backups. The exact same files are stored repeatedly resulting in inefficient use of storage.

Question 5

(a) What are the major data integrity policies followed by an organization? ***(6 Marks)***

(b) What is Mobile Computing? Describe the main components of mobile computing technology. ***(6 Marks)***

(c) List out the valid consideration for acquisition of both hardware and software when Request For Proposal is called from vendors. ***(4 Marks)***

Answer

(a) Major Data integrity policies followed by an organization are as under:

- **Virus-Signature Updating:** Virus signatures must be updated automatically when they are made available from the vendor through enabling of automatic updates.
- **Software Testing:** All software must be tested in a suitable test environment before installation on production systems.
- **Division of Environments:** The division of environments into Development, Test, and Production is required for critical systems.
- **Offsite Backup Storage:** Backups older than one month must be sent offsite for permanent storage.
- **Quarter-End and Year-End Backups:** Quarter-end and year-end backups must be done separately from the normal schedule for accounting purposes.
- **Disaster Recovery:** A comprehensive disaster-recovery plan must be used to ensure continuity of the corporate business in the event of an outage.

(b) **Mobile Computing:** Mobile Computing refers to the technology that allows transmission of data via a computer without having to be connected to a fixed physical link. Mobile voice communication has very rapid increase in the number of subscribers to the various cellular networks over the last few years. An extension of this technology is the ability to send and receive data across these cellular networks. This is the fundamental principle of mobile computing. Mobile data communication allows users to transmit data from remote locations to other remote or fixed locations.

The main components of Mobile Computing are as follows:

- **Mobile Communication:** This refers to the infrastructure put in place to ensure that seamless and reliable communication goes on. This would include communication properties, protocols, data formats and concrete technologies.
- **Mobile Hardware:** This includes mobile devices or device components that receive or access the service of mobility. They would range from Portable laptops, Smart Phones, Tablet PCs, and Personal Digital Assistants (PDA) that use an existing and established network to operate on. At the back end, there are various servers like Application Servers, Database Servers and Servers with wireless support, WAP gateway, a Communications Server and/or MCSS (Mobile Communications Server Switch) or a wireless gateway embedded in wireless carrier's network. The characteristics of mobile computing hardware are defined by the size and form factor, weight, microprocessor, primary storage, secondary storage, screen size and type, means of input, means of output, battery life, communications capabilities, expandability and durability of the device.
- **Mobile Software:** Mobile Software is the actual programme that runs on the mobile hardware and deals with the characteristics and requirements of mobile applications. It is the operating system of that appliance and is the essential component that makes the mobile device operates. Mobile applications popularly called Apps are being developed by organizations for use by customers but these apps could represent risks, in terms of flow of data as well as personal identification risks, introduction of malware and access to personal information of mobile owner.

(c) The following considerations are valid for acquisition of both hardware and software when Request for Proposal (RFP) is called from vendors:

- **Vendor Selection:** Vendor selection is to be done prior to sending RFP and is a critical step for success of process of acquisition of systems. The result of this process is that 'RFP are sent only to selected vendors'. For vendor selection, the things that are kept in mind include the background and location advantage of the vendor, the financial stability of vendor, the market feedback of vendor performance, in terms of price, services etc.
- **Geographical Location of Vendor:** This is regarding the issue to look for whether the vendor has local support persons or not? Otherwise, the proposals submitted by vendor not as per RFP requirements need to rejected, with no further discussion on such rejected proposals. This stage may be referred to as 'technical validation', that is to check the proposals submitted by vendors, are technically complying with RFP requirements.
- **Presentation by Selected Vendors:** All vendors, whose proposals are accepted

after "technical validation", are allowed to make presentation to the System Acquisition Team. The team evaluates the vendor's proposals by using techniques.

- **Evaluation of Users' Feedback:** The best way to understand the vendor systems is to analyze the feedback from present users. Present users can provide valuable feedback on system, operations, problems, vendor response to support calls.

Question 6

(a) Which aspects of environmental controls should be physically inspected by an information system auditor, while auditing environmental controls? Write any six. ***(6 Marks)***

(b) As an IT consultant, your client is seeking your advice whether to go for ISO 27001. Explain the reasons for which company may adopt ISO 27001. ***(6 Marks)***

(c) What are the objectives of performing BCP tests? ***(4 Marks)***

Answer

(a) Following aspects of environmental controls should be physically inspected by an Information System Auditor, while auditing environmental controls: The Auditor should verify:

- The IPF (Infrastructure Planning and Facilities) and the construction about the type of materials used for construction;
- The presence of water and smoke detectors, power supply arrangements to such devices, and testing logs;
- The location of fire extinguishers, firefighting equipment and refilling date of fire extinguishers;
- Emergency procedures, evacuation plans and marking of fire exists. There should be half-yearly Fire drill to test the preparedness;
- Documents for compliance with legal and regulatory requirements with regards to fire safety equipment, external inspection certificate and shortcomings pointed out by other inspectors/auditors;
- Power sources and conduct tests to assure the quality of power, effectiveness of the power conditioning equipment and generators. Also, the power supply interruptions must be checked to test the effectiveness of the back-up power;
- Environmental control equipment such as air-conditioning, dehumidifiers, heaters, ionizers etc.;
- Compliant logs and maintenance logs to assess if MTBF (Mean Time Between Failures) and MTTR (Mean Time To Repair) are within acceptable levels; and
- Identify undesired activities such as smoking, consumption of eatables etc.

(b) A company may adopt ISO 27001 for the following reasons:

- It is suitable for protecting critical and sensitive information.

- It provides a holistic, risk-based approach to secure information and compliance.
- Demonstrates credibility, trust, satisfaction and confidence with stakeholders, partners, citizens and customers.
- Demonstrates security status according to internationally accepted criteria.
- Creates a market differentiation due to prestige, image and external goodwill.
- If a company is certified once, it is accepted globally.

(c) In case of Development of BCP, the objectives of performing BCP tests are to ensure that:

- The recovery procedures are complete and workable.
- The competence of personnel in their performance of recovery procedures can be evaluated.
- The resources such as business processes, systems, personnel, facilities and data are obtainable and operational to perform recovery processes.
- The manual recovery procedures and IT backup system/s are current and can either be operational or restored.
- The success or failure of the business continuity training program is monitored.

Question 7

Write short notes on any ***four*** *of the following:*

(a) Misconceptions about MIS

(b) Characteristics of Public Cloud

(c) Trojan Horse

(d) Metrics of Risk Management

(e) Types of System Testing ***(4 x 4 = 16 Marks)***

Answer

(a) Following are the major misconceptions about Management Information Systems (MIS):

- Any computer based information system is a MIS.
- Any reporting system is MIS.
- MIS is a management technique.
- MIS is a bunch of technologies.
- MIS is an implementation of organizational systems and procedures. It is a file structure.
- The study of MIS is about use of computers.
- More data in generated reports refers more information to managers.

- o Accuracy plays vital role in reporting.

(b) Characteristics of Public Cloud are as follows:

- **Highly Scalable:** The resources in the public cloud are large in number and the service providers make sure that all requests are granted. Hence public clouds are scalable.
- **Affordable:** The cloud is offered to the public on a pay-as-you-go basis; hence the user must pay only for what he or she is using (using on a per-hour basis). This does not involve any cost related to the deployment.
- **Less Secure:** Since it is offered by a third party and they have full control over the cloud, the public cloud is less secure out of all the other deployment models.
- **Highly Available:** It is highly available because anybody from any part of the world can access the public cloud with proper permission, and this is not possible in other models as geographical or other access restrictions might be there.
- **Stringent Service-Level Agreements (SLAs):** As the service provider's business reputation and customer strength are totally dependent on the cloud services, they follow the SLAs strictly and violations are avoided.

(c) **Trojan Horse:** These are malicious programs that are hidden under any authorized program. Typically, a Trojan horse is an illicit coding contained in a legitimate program, and causes an illegitimate action. A Trojan may:

- Change or steal the password; or
- May modify records in protected files; or
- May allow illicit users to use the systems.

Trojan Horses hide in a host and generally do not damage the host program. Trojans cannot copy themselves to other software in the same or other systems. The Trojan may get activated only if the illicit program is called explicitly. It can be transferred to other system only if an unsuspecting user copies the Trojan program. Christmas card is a well-known example of Trojan.

(d) Some of the key metrics of IT Risk Management are as follows:

- Percentage of critical business processes, IT services and IT-enabled business programs covered by risk assessment;
- Number of significant IT related incidents that were not identified in risk assessment;
- Percentage of enterprise risk assessments including IT related risks; and
- Frequency of updating the risk profile based on status of assessment of risks.

(e) Different types of System Testing are as follows:

- **Recovery Testing:** This is the activity of testing 'how well the application is able to recover from crashes, hardware failures and other similar problems'. Recovery testing is the forced failure of the software in a variety of ways to verify that recovery is liable to be properly performed, in actual failures.
- **Security Testing:** This is the process to determine that an Information System protects data and maintains functionality as intended or not. The six basic security concepts that need to be covered by security testing are – Confidentiality, Integrity, Availability, Authentication, Authorization and Non-repudiation. This testing technique also ensures the existence and proper execution of access controls in the new system.
- **Stress or Volume Testing:** Stress testing is a form of testing that is used to determine the stability of a given system or entity. It involves testing beyond normal operational capacity, often to a breaking point, in order to observe the results. Stress testing may be performed by testing the application with large quantity of data during peak hours to test its performance.
- **Performance Testing:** In the computer industry, software performance testing is used to determine the speed or effectiveness of a computer, network, software program or device. This testing technique compares the new system's performance with that of similar systems using well defined benchmarks.