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

NXN Inc. is an insurance company having its head office in Texas US, and operations in other countries across the world. With the aim to expand their business they started a subsidiary in India and obtained the license from IRDA. Now they want to open their branches across India and also to appoint agents to sell their different insurance products. The company also wants to sell their products online. For this they wish to develop a website and a mobile application to market their products and enable their customers to pay the premium online. The company wants to use latest technologies and to establish an IT department with full IS security. The management of the company wants to follow the best practices in the area of governance. To fulfil their IT governance responsibilities the management wants to implement COBIT 5 framework in the organization.

You have been appointed as a consultant by the management of the company to assist them in this entire process. Kindly address the following queries raised by the management in this regard.

(a) Management wants to know as to what are the benefits the company would derive by implementing COBIT 5 framework? ***(6 Marks)***

(b) What is the information that an IS auditor is expected to obtain at the audit location before proceeding with the IS audit as per the provisions of IRDA? ***(5 Marks)***

(c) What is the set of skills that is generally expected to be with an IS? ***(3 Marks)***

Answer

(a) Some benefits that the Insurance company NXN Inc. would drive by implementing COBIT 5 framework are as follows:

- 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) As per the provisions of Insurance Regulatory and Development Authority of India (IRDA), an IS auditor is expected to obtain the following information at the audit location before proceeding with the IS audit:

- Location(s) from where Investment activity is conducted.
- IT Applications used to manage the Insurer's Investment Portfolio.
- Obtain the system layout of the IT and network infrastructure including Server details, database details, type of network connectivity, firewalls and other facilities/utilities.
- Check whether the systems and applications are hosted at a central location or hosted at different offices.
- Obtain Previous Audit reports and open issues/details of unresolved issues from Internal Audit, Statutory Audit, and IRDA Inspection/Audit.
- Internal circulars and guidelines of the Insurer.
- Standard Operating Procedures (SOP).
- List of new Products/funds introduced during the period under review along with IRDA approvals for the same.
- Scrip wise lists of all investments, fund wise, classified as per IRDA Guidelines, held on date.
- IRDA Correspondence files, circulars and notifications issued by IRDA.
- IT Security Policy.
- Business Continuity Plans.
- Network Security Reports pertaining to IT Assets.

(c) The skillset that is generally expected to be with an Information Systems auditor includes the following:

- Sound knowledge of business operations, practices and compliance requirements;

- Should possess the requisite professional technical qualification and certifications;
- A good understanding of information risks and controls;
- Knowledge of IT strategies, policy and procedural controls;
- Ability to understand technical and manual controls relating to business continuity; and
- Good knowledge of Professional Standards and Best Practices of IT controls and security.

Question 2

(a) A Pharma company has chain of distributors and stockist at various cities of India. The company is having "Distributed data processing facilities" so that distributors, stockist, and members of sales team can access the application remotely. Being an IS auditor, suggest various ways for controlling remote and distributed data processing application.

(6 Marks)

(b) During COVID 19, the management of a hospital wish to get developed an application software for online consultations. The proposed software can be used by public for general medical emergency including expected COVID situations. Suggest, what properties this potential application should possess to qualify for Expert System? ***(5 Marks)***

(c) What are the provisions related to penalty for publishing Electronic Signature Certificate false in certain particulars as under section 73 of IT Act 2000? ***(3 Marks)***

Answer

(a) Some ways in which remote and distributed data processing applications can be controlled 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.
- In order 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.

(b) The properties that potential applications should possess to qualify for Expert Systems are as follows:

- **Availability** – One or more experts are capable of communicating 'how they go about solving the problems to which the Expert System will be applied.'
- **Complexity** – Solution of the problem for which the Expert System will be used, is a complex task that requires logical inference processing, which would not be easily handled by conventional information processing.
- **Domain** – The domain or subject area of the problem for which the Expert system is applicable, is relatively small and limited to a relatively well-defined problem area.
- **Expertise** – Solutions to the complex problem require the efforts of experts. That is, only a few possess the knowledge, techniques, and intuition needed.
- **Structure** – The solution process must be able to cope with ill-structured, uncertain, missing, and conflicting data, and a dynamic problem-solving situation.

(c) The provisions related to Penalty for publishing Electronic Signature Certificate false in certain particulars as under Section 73 of the Information Technology Act 2000 is as follows:

(1) No person shall publish an Electronic Signature Certificate or otherwise make it available to any other person with the knowledge that -

- the Certifying Authority listed in the certificate has not issued it; or
- the subscriber listed in the certificate has not accepted it; or
- the certificate has been revoked or suspended,

unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.

(2) Any person contravenes the provisions of sub-section (1) shall be punished with imprisonment for term which may be extend to two years, or with fine which may be extend to one lakh rupees, or both.

Question 3

(a) As a BCP auditor, while reviewing the disaster recovery/business resumption plan that exist in the organization was developed using sound methodology. Which aspects should be reviewed by you as an auditor? ***(6 Marks)***

(b) "The management of Risk is now being understood as an effective part of IT governance". In the light of above statement, describe the various Risk Management Strategies.

(5 Marks)

(c) What are the characteristics of private cloud? ***(3 Marks)***

Answer

(a) As a BCP Auditor, while reviewing whether the disaster recovery/business resumption plan that exists in an organization was developed using a sound methodology or not, following aspects should be reviewed:

- Identification and prioritization of the activities, which are essential to continue functioning.
- The plan is based upon a business impact analysis that considers the impact of the loss of essential functions.
- Operations managers and key employees participated in the development of the plan.
- The plan identifies the resources that will likely be needed for recovery and the location of their availability.
- The plan is simple and easily understood so that it will be effective when it is needed.
- The plan is realistic in its assumptions.

(b) Various Risk Management strategies used in IT Governance are as follows:

- **Tolerate/Accept the risk.** One of the primary functions of management is managing risk. Some risks may be considered minor because their impact and probability of occurrence is low. In this case, consciously accepting the risk as a cost of doing business is appropriate, as well as periodically reviewing the risk to ensure its impact remains low.
- **Terminate/Eliminate the risk.** It is possible for a risk to be associated with the use of a particular technology, supplier, or vendor. The risk can be eliminated by replacing the technology with more robust products and by seeking more capable suppliers and vendors.
- **Transfer/Share the risk.** Risk mitigation approaches can be shared with trading partners and suppliers. A good example is outsourcing infrastructure management. In such a case, the supplier mitigates the risks associated with managing the IT infrastructure by being more capable and having access to more highly skilled staff than the primary organization. Risk also may be mitigated by transferring the cost of realized risk to an insurance provider.

- **Treat/mitigate the risk.** Where other options have been eliminated, suitable controls must be devised and implemented to prevent the risk from manifesting itself or to minimize its effects.
- **Turn back.** Where the probability or impact of the risk is very low, then management may decide to ignore the risk.

(c) Various characteristics of Private Cloud are as follows:

- **Secure:** The private cloud is secure as it is deployed and managed by the organization itself, and hence there is least chance of data being leaked out of the cloud.
- **Central Control:** As usual, the private cloud is managed by the organization itself, there is no need for the organization to rely on anybody and it's controlled by the organization itself.
- **Weak Service Level Agreements (SLAs):** SLAs play a very important role in any cloud service deployment model as they are defined as agreements between the user and the service provider in private cloud. In private cloud, either Formal SLAs do not exist or are weak as it is between the organization and user of the same organization. Thus, high availability and good service may or may not be available.

Question 4

(a) "When properly implemented, audit trails provide an important detective control to help accomplish security policy objectives." In light of the above statement, list out the ways in which audit trails can be used to Support security objectives. ***(6 Marks)***

(b) Briefly describe the various ways to implement application and monitoring system access control pertaining to logical access control. ***(5 Marks)***

(c) Define the following terms as provided in the Information Technology Act:

(i) Access

(ii) Intermediary

(iii) Asymmetric Crypto System ***(3 Marks)***

Answer

(a) Audit trails can be used to support Information Systems' security objectives in following three ways:

- **Detecting Unauthorized Access:** Detecting unauthorized access can occur in real time or after the fact. The primary objective of real-time detection is to protect the system from outsiders who are attempting to breach system control. A real-time audit trail can also be used to report on changes in system performance that may indicate infestation by a virus or worm. Depending upon how much activity is being logged and reviewed; real-time detection can impose a significant overhead on the operating

system, which can degrade operational performance. After-the-fact, detection logs can be stored electronically and reviewed periodically or as needed. When properly designed, they can be used to determine if unauthorized access was accomplished, or attempted and failed.

- **Reconstructing Events:** Audit analysis can be used to reconstruct the steps that led to events such as system failures, security violations by individuals, or application processing errors. Knowledge of the conditions that existed at the time of a system failure can be used to assign responsibility and to avoid similar situations in the future. Audit trail analysis also plays an important role in accounting control. For example - by maintaining a record of all changes to account balances, the audit trail can be used to reconstruct accounting data files that were corrupted by a system failure.
- **Promoting Personal Accountability:** Audit trails can be used to monitor user activity at the lowest level of detail. This capability is a preventive control that can be used to influence behavior. Individuals are likely to violate an organization's security policy if they know that their actions are not recorded in an audit log.

(b) Various ways to implement application and monitoring system access control pertaining to Logical Access Controls are as follows:

- **Information access restriction:** The access to information is prevented by application specific menu interfaces, which limit access to system function. A user is allowed to access only those items, s/he is authorized to access. Controls are implemented on the access rights of users, for example - read, write, delete and execute and ensure that sensitive output is sent only to authorized terminals and locations.
- **Sensitive system isolation:** Based on the critical constitution of a system in an enterprise, it may even be necessary to run the system in an isolated environment. Monitoring system access and use is a detective control, to check if preventive controls discussed so far are working. If not, this control will detect and report any unauthorized activities.
- **Event logging:** In Computer systems, it is easy and viable to maintain extensive logs for all types of events. It is necessary to review if logging is enabled and the logs are archived properly. An intruder may penetrate the system by trying different passwords and user ID combinations. All incoming and outgoing requests along with attempted access should be recorded in a transaction log. The log should record the user ID, the time of the access and the terminal location from where the request has been originated.
- **Monitor system use:** Based on the risk assessment, a constant monitoring of some critical systems is essential. Define the details of types of accesses, operations, events and alerts that will be monitored. The extent of detail and the frequency of the

review would be based on criticality of operation and risk factors. The log files are to be reviewed periodically and attention should be given to any gaps in these logs.

- **Clock synchronization:** Event logs maintained across an enterprise network plays a significant role in correlating an event and generating report on it. Hence, the need for synchronizing clock time across the network as per a standard time is mandatory.

(c) As per the Information Technology Act 2000, the requisite definitions are as follows:

(i) **"Access"** with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network.

(ii) **"Intermediary"** with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes.

(iii) **"Asymmetric Crypto System"** means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature.

Question 5

(a) The characterizing features of Waterfall Model have influenced the software development community in big way. As a system developer, state three key characteristics and three strengths of Waterfall Model. ***(6 Marks)***

(b) What are the important implications of information system in a business? Explain. ***(5 Marks)***

(c) Briefly explain any three applications fields of Web 2.0. ***(3 Marks)***

Answer

(a) Following are some key characteristics of the Waterfall Model:

- Project is divided into sequential phases with some overlap and splash back acceptable between phases.
- Emphasis is on planning, time schedules, target dates, budgets and implementation of an entire system at one time.
- Tight control is maintained over the life of the project through the use of extensive written documentation, as well as through formal reviews and approval/signoff by the user and information technology management occurring at the end of most phases before beginning the next phase.

The strengths of the Waterfall Model are as follows:

- It is ideal for supporting less experienced project teams and project managers or project teams, whose composition fluctuates.
- The orderly sequence of development steps and design reviews helps to ensure the quality, reliability, adequacy and maintainability of the developed software.
- Progress of system development is measurable.
- It enables us to conserve resources.

(b) The important implications of Information Systems in business are as follows:

- Information Systems helps managers in efficient decision-making to achieve the organizational goals.
- An organization will be able to survive and thrive in a highly competitive environment on the strength of well-designed Information systems.
- Information systems help in making right decision at the right time i.e., just on time.
- Good information systems may help in generating innovative ideas for solving critical problems.
- Knowledge gathered though Information systems may be utilized by managers in unusual situations.
- Information Systems are viewed as a process which can be integrated to formulate a strategy of action or operation.

(c) The application fields of Web 2.0 are as follows:

- **Social Media:** Social Media/Social Network is an important application of web 2.0 as it provides a fundamental shift in the way people communicate and share information. The social web offers number of online tools and platforms that could be used by the users to share their data, perspectives, and opinions among other user communities.
- **Marketing:** Web 2.0 offers excellent opportunities for marketing by engaging customers in various stages of the product development cycle. It allows the marketers to collaborate with consumers on various aspects such as product development, service enhancement, and promotion. Collaboration with the business partners and consumers can be improved by the companies by utilizing the tools provided by Web 2.0 paradigm. Consumer-oriented companies use networks such as Twitter and Facebook as common elements of multichannel promotion of their products.
- **Education:** Web 2.0 technologies can help the education scenario by providing students and faculty with more opportunities to interact and collaborate with their peers. By utilizing the tools of Web 2.0, the students get the opportunity to share what they learn with other peers by collaborating with them.

Question 6

(a) There are many aspects to the application controls that are reviewed as a part of any application audit but out of these, application security is one of the most important controls. Describe the audit issues relating to operational layer with respect to the audit of application security control. ***(6 Marks)***

(b) Describe the various categories of tests that a programmer typically performs on a program unit. ***(5 Marks)***

(c) Briefly describe the control procedures over source documents which an organization must implement to account for each document to control the frauds. ***(3 Marks)***

OR

Explain, how a physical component 'Modem' in a network communication can affect the reliability of communication system. ***(3 Marks)***

Answer

(a) The Operational Layer audit issues w.r.t Application Security audit include the following:

- **User Accounts and Access Rights:** This includes defining unique user accounts and providing them with access rights appropriate to their roles and responsibilities. An auditor needs to always ensure the use of unique user IDs and these need to be traceable to individuals for whom they are 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. In essence, 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 (SoD):** As frauds due to collusions/lack of segregations increase across the world, importance of the SoD also increases. SoD 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. Some examples to illustrate this are that record keeper of asset must not be asset keeper; cashier who creates a cash voucher in system must not have right to authorize payments and maker must not be checker. The auditor needs to check that there is no violation of these principles. Any violation may have serious repercussions, the same need to be immediately communicated to those charged with governance.

(b) The five categories of tests that a programmer typically performs on a program unit are as follows:

- **Functional Tests:** Functional Tests check "whether programs do, what they are supposed to do or not". The test plan specifies operating conditions, input values, and expected results, and as per this plan, programmer checks by inputting the values to see whether the actual result and expected result match.
- **Performance Tests:** Performance Tests should be designed to verify the response time, the execution time, the throughput, primary and secondary memory utilization and the traffic rates on data channels and communication links.
- **Stress Tests:** 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. These tests are designed to overload a program in various ways. The purpose of a stress test is to determine the limitations of the program. For example, during a sort operation, the available memory can be reduced to find out whether the program is able to handle the situation.
- **Structural Tests:** Structural Tests are concerned with examining the internal processing logic of a software system. For example, if a function is responsible for tax calculation, the verification of the logic is a structural test.
- **Parallel Tests:** In Parallel Tests, the same test data is used in the new and old system and the output results are then compared.

(c) The control procedures that an organization must implement over source documents to account for each document are described below:

- **Use pre-numbered source documents:** Source documents should come pre-numbered from the printer with a unique sequential number on each document. Source document numbers enable accurate accounting of document usage and provide an audit trail for tracing transactions through accounting records.
- **Use source documents in sequence:** Source documents should be distributed to the users and used in sequence. This requires adequate physical security be maintained over the source document inventory at the user site. When not in use, documents should be kept under lock and key and access to source documents should be limited to authorized persons.
- **Periodically audit source documents:** Missing source documents should be identified by reconciling document sequence numbers. Periodically, the auditor should compare the numbers of documents used to date with those remaining in inventory plus those voided due to errors. Documents not accounted for should be reported to management.

OR

Modem in a network Communication can affect the reliability of communication system as follows:

- Increases the speed with which data can be transmitted over a communication line.
- Reduces the number of line errors that arise through distortion if they use a process called equalization.
- Reduces the number of line errors that arise through noise.