6

Auditing of Information Systems

Basic Concepts

1. Need for Audit of Information Systems: Factors influencing an organization toward controls and audit of computers and the impact of the information systems audit function on organizations are depicted in the Fig. 6.1.

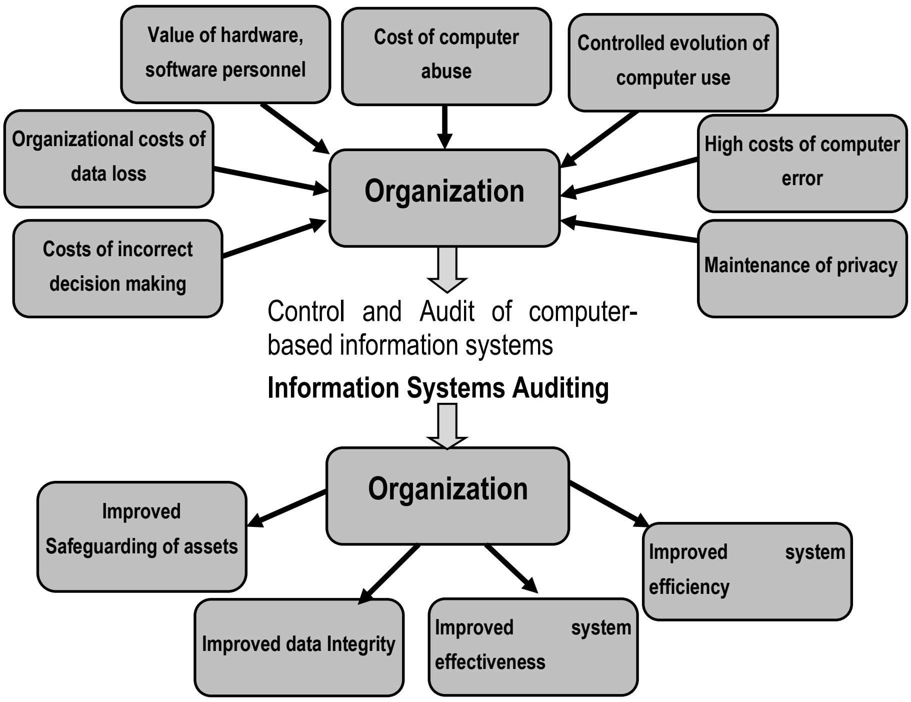
Value of hardware, software personnel
Cost of computer abuse
Controlled evolution of computer use
Organizational costs of data loss
Organization
High costs of computer error
Costs of incorrect decision making
Maintenance of privacy
Control and Audit of computer-based information systems
Information Systems Auditing
Organization
Improved Safeguarding of assets
Improved system efficiency
Improved data Integrity
Improved system effectiveness

Fig. 6.1: Impact of Controls and Auditing influencing an Organization

These are: *Organisational Costs of Data Loss, Incorrect Decision Making, Costs of Computer Abuse, Value of Computer Hardware, Software and Personnel*, *High Costs of Computer Error*, *Maintenance of Privacy, Controlled evolution of computer Use*, *Information Systems Auditing*, *Asset Safeguarding Objectives*, *Data Integrity Objectives*, *System Effectiveness Objectives* and *System Efficiency Objectives*.

2. **Effect of Computers on Internal Audit:** To cope up with the new technology usage in an enterprise, the auditor should be competent to provide independent evaluation as to whether the business process activities are recorded and reported according to established standards or criteria. Two basic functions carried out to examine these changes are:

(i) **Changes to Evidence Collection:** The performance of evidence collection and understanding the reliability of controls involves issues like- *Data retention and storage, Absence of input documents*, *Non-availability of audit trail, Lack of availability of output, Audit evidence* and *Legal issues*.

(ii) **Changes to Evidence Evaluation:** Evaluation of audit trail and evidence is to trace consequences of control's strength and weakness throughout the system. Major issues are: *System generated transactions, Automated transaction processin*g/generation *systems* and Systemic errors.

3. **Responsibility for Controls:** Management is responsible for establishing and maintaining control to achieve the objectives of effective and efficient operations, and reliable information systems.

4. **IS Audit:** The IS Audit of an Information System environment may include one or both following:

- Assessment of internal controls within the IS environment to assure validity, reliability, and security of information and information systems.
- Assessment of the efficiency and effectiveness of the IS environment.

5. **Functions of IS Auditor:** IS Auditors review risks relating to IT systems and processes; some of them are: *Inadequate information security controls, Inefficient use of resources, or poor governance, Ineffective IT strategies, policies and practices and IT-related frauds.*

6. **Categories of IS Audits:** IS Audits has been categorized into five types: *Systems and Application, Information Processing Facilities*, *Systems Development*, *Management of IT and Enterprise Architecture* and *Telecommunications, Intranets, and Extranets*.

7. **Steps in Information System Audit:** Different audit organizations go about IS auditing in different ways and individual auditors have their own favorite ways of working. However, it can be categorized into six stages, which are: *Scoping and pre-audit survey, Planning and preparation, Fieldwork, Analysis, Reporting and Closure.*

8. **Audit Standards and Best Practices:** These are: *IS auditing standards*, *IS auditing guidelines*, *IS auditing procedures & COBIT (Control objectives for information and related technology) of ISACA (Information Systems Audit and Control Association), ISO 27001, Internal Audit Standards, Standards on Internal Audit issued by ICAI and ITIL.*

9. **Performing IS Audit:** Various steps are given as follows:

(i) **Basic Plan:** Planning is one of the primary and important phase in an Information System Audit, which ensures that the audit is performed in an effective manner. Adequate planning of the audit work helps to ensure that appropriate attention is devoted to important areas of the audit, potential problems are identified and that the work is completed expeditiously.

(ii) Preliminary Review: Some of the critical factors, which should be considered by an IS auditor as part of his/her preliminary review are: *Knowledge of the Business, Understanding the Technology, Understanding Internal Control Systems, Legal Considerations and Audit Standards and Risk Assessment and Materiality.* Risks are categorized as: *Inherent Risk, Control Risk and Detection Risk*.

10. Concurrent or Continuous Audit: Continuous auditing enables auditors to significantly reduce and perhaps to eliminate the time between occurrence of the events at the client and the auditor's assurance services thereon. Continuous auditing techniques use two bases for collecting audit evidence. One is the use of embedded modules in the system to collect, process, and print audit evidence and the other is special audit records used to store the audit evidence collected.

Types of Audit Tools: Some of the well-known tools are as follows:

(i) Snapshots: Tracing a transaction in a computerized system can be performed with the help of snapshots or extended records. The snapshot software is built into the system at those points where material processing occurs which takes images of the flow of any transaction as it moves through the application.

(ii) Integrated Test Facility (ITF): The ITF technique involves the creation of a dummy entity in the application system files and the processing of audit test data against the entity as a means of verifying processing authenticity, accuracy, and completeness.

(iii) System Control Audit Review File (SCARF): The SCARF technique involves embedding audit software modules within a host application system to provide continuous monitoring of the system's transactions. The information collected is written onto a special audit file- the SCARF master files. Auditors might use SCARF to collect the different types of information such as *Application System Errors*, *Policy and Procedural Variances*, *System Exception*, *Statistical Sample*, *Snapshots and Extended Records*, *Profiling Data* and *Performance Measurement*.

(iv) Continuous and Intermittent Simulation (CIS): This is a variation of the SCARF continuous audit technique. This technique can be used to trap exceptions whenever the application system uses a database management system.

Some of the advantages of continuous audit techniques are: *Timely, Comprehensive and Detailed Auditing*, *Surprise test capability*, *Information to system staff on meeting of objectives and Training for new users*.

(v) Audit Hooks: There are audit routines that flag suspicious transactions. For example, Internal auditors at Insurance Company determined that their policyholder system was vulnerable to fraud every time a policyholder changed his or her name or address and then subsequently withdrew funds from the policy. They devised a system of audit hooks to tag records with a name or address change. The internal audit department will investigate these tagged records for detecting fraud. When audit hooks are employed, auditors can be informed of questionable transactions as soon as they occur. This approach of real-time notification displays a message on the auditor's terminal.

11. Audit Trail Objectives: Audit trails can be used to support security objectives in three ways: *Detecting unauthorized access to the system, Facilitating the reconstruction of events, and Promoting personal accountability.*

12. Role of IS Auditor in Physical Access Controls: Auditing physical access requires the auditor to review the physical access risk and controls to form an opinion on the effectiveness of the physical access controls. This involves: *Risk Assessment*, *Controls Assessment* and *Review of Documents*.

13. Role of IS Auditor in Environmental Controls: Audit of environmental controls should form a critical part of every IS audit plan. The IS auditor should satisfy not only the effectiveness of various technical controls but also the overall controls safeguarding the business against environmental risks. Documentation of Auditing of environmental controls activities is a critical part.

14. Application Controls and their Audit Trail: These are categorized in the following types:

- **Boundary Controls:** IT ensures that those who are using system are authentic users.
- **Input Controls:** Responsible for bringing the data and instructions in to the information system.
- **Communication Controls:** Responsible for controls over physical components, communication line errors, flows, and links, topological controls, channel access controls, controls over subversive attacks, internetworking controls, communication architecture controls, audit trail controls, and existence controls.
- **Processing Controls:** Responsible for computing, sorting, classifying and summarizing data. It maintains the chronology of events from the time data is received from input or communication systems to the time data is stored into the database or output as results.
- **Database Controls:** Responsible to provide functions to define, create, modify, delete and read data in an information system. It maintains procedural data-set of rules to perform operations on the data to help a manager to take decisions.
- **Output Controls:** To provide functions that determine the data content available to users, data format, timeliness of data and how data is prepared and routed to users.

15. Review of Controls at various Layers: For application security audit, a layered approach is used based on the functions and approach of each layer. This approach is in line with management structure, which follows top-down approach. Various layers are:

- **Operational Layer:** The basic layer, where user access decisions are generally put in place.
- **Tactical Layer:** The next is management layer, which includes supporting functions such as security administration, IT risk management and patch management.
- **Strategic Layer:** This is the layer used by top management. It includes the overall information security governance, security awareness, supporting information security policies and standards, and the overarching an application security perspective.

Various aspects relating to each aforementioned layer are given as follows:

- **Operational Layer:** The operational layer audit issues include: *User Accounts and Access Rights, Password Controls and Segregation of Duties.*
- **Tactical Layer**: At the tactical layer, security administration is put in place. This includes: *Timely updates to user profiles, like creating/deleting and changing of user accounts, IT Risk Management, Interface Security and Audit Logging and Monitoring.*
- **Strategic Layer:** At this layer, the top management acts, in form of drawing up security policy, security training, security guideline and reporting. A comprehensive information security programme fully supported by top management and communicated well to the organization is of paramount importance to succeed in information security. The security policy should be supported and supplemented by detailed standards and guidelines. These guidelines shall be used at the appropriate level of security at the application, database and operating system layers.

  Based on the key controls described previously, the risk assessment of failure/weakness in the operating effectiveness of key application security controls shall be made and acted upon by auditor.

Question 1

Compared to traditional audit, evidence collection has become more challenging with the use of computers to the auditors. What are the issues which affect evidence collection and understanding the reliability of controls in financial audit?

Or

The advent of computer has drastically transformed the mode of evidence collection by an auditor. Discuss the various issues involved in the performance of evidence collection and understanding the reliability of controls.

Answer

The performance of evidence collection and understanding the reliability of controls involves the following major issues:

- **Data retention and storage:** A client's storage capabilities may restrict the amount of historical data that can be retained "on-line" and readily accessible to the auditor. If the client has insufficient data retention capacities the auditor may not be able to review a whole reporting period transactions on the computer system. For example, the client's computer system may save data on detachable storage device by summarizing transactions into monthly, weekly or period end balances.
- **Absence of input documents:** Transaction data may be entered into the computer directly without the presence of supporting documentation e.g. input of telephone orders into a telesales system. The increasing use of EDI will result in less paperwork being available for audit examination.
- **Non-availability of audit trail:** The audit trails in some computer systems may exist for only a short period of time. The absence of an audit trail will make the auditor's job very difficult and may call for an audit approach which involves auditing around the computer system by seeking other sources of evidence to provide assurance that the computer input has been correctly processed and output.
- **Lack of availability of output:** The results of transaction processing may not produce a hard copy form of output, i.e. a printed record. In the absence of physical output it may be necessary for the auditor to directly access the electronic data retained on the client's computer. This is normally achieved by having the client provide a computer terminal and being granted "read-only" access to the required data files.
- **Audit evidence.** Certain transactions may be generated automatically by the computer system. For example, a fixed asset system may automatically calculate depreciation on assets at the end of each calendar month. The depreciation charge may be automatically transferred (journalized) from the fixed assets register to the depreciation account and hence to the client's income and expenditure account.
- **Legal issues:** The use of computers to carry out trading activities is also increasing. More organizations in both the public and private sector intend to make use of EDI and electronic trading over the Internet. This can create problems with contracts, e.g. when is the contract made, where is it made (legal jurisdiction), what are the terms of the contract and who are the parties to the contract.

Question 2

Explain the set of skills that is generally expected of an IS auditor.

Or

ABC Ltd. is looking for a suitable IS Auditor. Please send an introductory note to ABC Ltd. explaining your suitability by describing the skill set and competence you possess for the job other than your qualification.

Answer

The set of skills that is generally expected of an IS auditor includes:

- 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.
- Knowledge of various technologies and their advantages and limitations is a critical competence requirement for the auditor. For example, authentication risks relating to e-mail systems.

Question 3

Explain major types of IS Audits in brief.

Answer

Major types of IS Audits are given as follows:

(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.

Question 4

Different auditors go about IS auditing in different ways. Despite this, IS audit process can be categorized into broad categories. Discuss the statement explaining broad steps involved in the process.

Or

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?

Answer

Different audit organizations go about IS auditing in different ways and individual auditors have their own favourite ways of working. However, it can be categorized into the following major stages:

(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:** Gathering 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 the evidence gathered earlier. SWOT (Strengths, Weaknesses, Opportunities, Threats) or PEST (Political, Economic, Social, Technological) techniques can be used for analysis.

(v) **Reporting:** Reporting to the management is done after analysis of evidence gathered and analysed.

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

Question 5

An important task for the auditor as a part of the preliminary evaluation is to gain a good understanding of the technology environment and related control issues. As the company auditor, which aspects you will include in your consideration to understand the technology?

Answer

Major aspects to be considered in the afore mention exercise are given as follows:

- Analysis of business processes and level of automation,

- Assessing the extent of dependence of the enterprise on Information Technology to carry on its businesses i.e. Role of IT in the success and survival of business,
- Understanding technology architecture which could be quite diverse such as a distributed architecture or a centralized architecture or a hybrid architecture,
- Studying network diagrams to understand physical and logical network connectivity,
- Understanding extended enterprise architecture wherein the organization systems connect seamlessly with other stakeholders such as vendors (SCM), customers (CRM), employees and the government,
- Knowledge of various technologies and their advantages and limitations is a critical competence requirement for the auditor. For example, authentication risks relating to e-mail systems, and
- Finally, Studying Information Technology policies, standards, guidelines and procedures.

Question 6

What are the key steps that can be followed for a risk-based approach to make an audit plan? Explain in brief.

Answer

The steps that can be followed for a risk-based approach to make an audit plan are given as follows:

- Inventory the information systems in use in the organization and categorize them.
- Determine which of the systems impact critical functions or assets, such as money, materials, customers, decision making, and how close to real time they operate.
- Assess what risks affect these systems and the likelihood and severity of the impact on the business.
- Based on the above assessment, decide the audit priority, resources, schedule and frequency.

Question 7

Write short notes on the following:

(i) Snapshots

(ii) Audit Hooks

(iii) Effect of Computers on Evidence Collection for audit

(iv) Objectives of IS Audit

(v) ISO 27001

Answer

(i) **Snapshots:** Tracing a transaction in a computerized system can be performed with the help of snapshots or extended records. The snapshot software is built into the system at those points where material processing occurs which takes images of the flow of any transaction as it moves through the application. These images can be utilized to assess the authenticity, accuracy, and completeness of the processing carried out on the transaction. The main areas to dwell upon while involving such a system are to locate the snapshot points based on materiality of transactions when the snapshot will be captured and the reporting system design and implementation to present data in a meaningful way.

(ii) **Audit Hooks:** There are audit routines that flag suspicious transactions. For example, internal auditors at Insurance Company determined that their policyholder system was vulnerable to fraud every time a policyholder changed his or her name or address and then subsequently withdrew funds from the policy. They devised a system of audit hooks to tag records with a name or address change. The internal audit department will investigate these tagged records for detecting fraud. When audit hooks are employed, auditors can be informed of questionable transactions as soon as they occur. This approach of real-time notification may display a message on the auditor's terminal.

(iii) **Effects of Computers on Evidence Collection for Audit:** The performance of evidence collection and understanding the reliability of controls involves issues like -

- **Data retention and storage:** A client's storage capabilities may restrict the amount of historical data that can be retained "on-line" and readily accessible to the auditor due to which the auditor may not be able to review a whole reporting period transactions on the computer system.
- **Absence of input documents:** Transaction data may be entered into the computer directly without the presence of supporting documentation resulting in less paperwork being available for audit examination.
- **Non-availability of audit trail:** The audit trails in some computer systems may exist for only a short period of time; thus making the auditor's job very difficult.
- **Lack of availability of printed output:** In the absence of physical output, it may be necessary for the auditor to directly access the electronic data retained on the client's computer.
- **Audit evidence:** Certain transactions may be generated automatically by the computer system.
- **Legal issues:** Making use of Electronic Data Interchange (EDI) and electronic trading over the Internet can create problems with contracts, e.g. when is the contract made, where is it made (legal jurisdiction), what are the terms of the contract and are the parties to the contract.

(iv) The major objectives of Information System Audit, are as follows:

- **Asset Safeguarding Objectives:** The information system assets (hardware, software, data information etc.) must be protected by a system of internal controls from unauthorised access.
- **Data Integrity Objectives:** It is a fundamental attribute of IS Auditing. The importance to maintain integrity of data of an organisation requires all the time. It is also important from the business perspective of the decision maker, competition and the market environment.
- **System Effectiveness Objectives:** Effectiveness of a system is evaluated by auditing the characteristics and objective of the system to meet business and user requirements.
- **System Efficiency Objectives:** To optimize the use of various information system resources (machine time, peripherals, system software and labour) along with the impact on its computing environment.

(v) ISO 27001: ISO 27001 is the international best practice and certification standard for an Information Security Management System (ISMS). An ISMS is a systematic approach to manage Information security in an IS environment through which an organization identifies, analyzes and addresses its information security risks. It encompasses people, processes and IT Systems. ISO 27001 defines how to organise information security in any kind of organization, profit or non-profit, private or state-owned, small or large. This standard is the foundation of information security management that enables an organization to get certified, which means that an independent certification body has confirmed that information security has been implemented in the organisation as defined policies and procedures.

The ISO 27001 can act as the extension of the current quality system to include security; provides an opportunity to identify and manage risks to key information and systems assets; provides confidence and assurance to trading partners and clients; acts as a marketing tool and allows an independent review and assurance to you on information security practices.

Question 8

As an IS Auditor of a company, you want to use SCARF technique for collecting some information, which you want to utilize for discharging some of your functions Briefly describe the type of information that can be collected using SCARF technique.

Answer

System Control Audit Review File (SCARF): The SCARF technique involves embedding audit software modules within a host application system to provide continuous monitoring of the system's transactions. The information collected is written on a special audit file- the SCARF master files. Auditors then examine the information contained on this file to see if some aspect of the application system needs follow-up. In many ways, the SCARF technique is like the snapshot technique along with other data collection capabilities.

Auditors might use SCARF technique to collect the following types of information:

- **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 must 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.

Question 9

Describe major advantages of continuous audit techniques.

Answer

Major advantages of continuous audit techniques are given as follows:

- **Timely, Comprehensive and Detailed Auditing –** Evidence would be available more timely and in a comprehensive manner. The entire processing can be evaluated and analyzed rather than examining the inputs and the outputs only.
- **Surprise test capability –** As evidences 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 provides 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 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 10

Describe major disadvantages and limitations of Continuous Audit techniques.

Answer

Major disadvantages and limitations of continuous audit techniques are given as follows:

- Auditors should be able to obtain resources required from the organization to support development, implementation, operation, and maintenance of continuous audit techniques.
- Continuous audit techniques are more likely to be used if auditors are involved in the development work associated with a new application system.
- Auditors need the knowledge and experience of working with computer systems to be able to use continuous audit techniques effectively and efficiently.
- Continuous auditing techniques are more likely to be used where the audit trail is less visible and the costs of errors and irregularities are high.
- Continuous audit techniques are unlikely to be effective unless they are implemented in an application system that is relatively stable.

Question 11

Explain three major ways by which audit trails can be used to support security objectives.

Answer

Audit trails can be used to support security objectives in the 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 controls. 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 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.

- **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.

Question 12

Briefly describe the audit issues relating to operational layer with respect to the application security control auditing,

Answer

Major audit issues of operational layer regarding application security audit are given as follows:

- **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 individuals for whom they are created. In case, guest IDs are used, then these should be tested. 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:** As frauds due to lack of segregations increase across the world, importance of the Segregation of Duties also increases. As defined earlier, Segregation of duties is a basic internal control that prevents or detects errors and irregularities by assigning to the 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.

Auditor needs to check that there is no violation of above principle. Any violation may have serious repercussions, the same needs to be immediately communicated to those charged with governance.

Question 13

Discuss Managerial Controls and their Audit Trails.

Or

With respect to Top Management and in IS management control, the major activities that the senior management must perform are: Planning, Organising, Leading and Controlling in the Information System functions. Explain the role of the IS auditor in any three of the above-mentioned activities.

Answer

The Managerial controls and their Audit trails are as follows:

(a) **Top Management and Information Systems Management Controls:** The major activities that senior management must perform are – Planning, Organizing, Controlling and Leading.

- **Planning:** Auditors evaluate whether top management has formulated a high-quality information system's plan that is appropriate to the needs of an organization or not.
- **Organizing:** Auditors should be concerned about how well top management acquires and manage staff resources.
- **Leading:** Generally, the auditors examine variables that often indicate when motivation problems exist or suggest poor leadership – for example, staff turnover statistics, frequent failure of projects to meet their budget and absenteeism level to evaluate the leading function.
- **Controlling:** Auditors must evaluate whether top management's choice to the means of control over the users of Information System services is likely to be effective or not.

(b) **System Development Management Controls:** Three different types of audits may be conducted during system development process as follows:

- **Concurrent Audit:** Auditors are members of the system development team. They assist the team in improving the quality of systems development for the specific system they are building and implementing.
- **Post -implementation Audit:** Auditors seek to help an organization learn from its experiences in the development of a specific application system. In addition, they might be evaluating whether the system needs to be scrapped, continued, or modified in some way.
- **General Audit:** Auditors evaluate systems development controls overall. They seek to determine whether they can reduce the extent of substantive testing needed to form an audit opinion about management's assertions relating to the financial statements for systems effectiveness and efficiency.

(c) **Programming Management Controls:** Some of the major concerns that an Auditor should address under different activities are as under:

- **Planning:** They should evaluate whether the nature of and extent of planning are appropriate to the different types of software that are developed or acquired and how well the planning work is being undertaken.
- **Control:** They must evaluate whether the nature of an extent of control activities undertaken are appropriate for the different types of software that are developed or acquired. They must gather evidence on whether the control procedures are operating reliably.
- **Design:** Auditors should find out whether programmers use some type of systematic approach to design. Auditors can obtain evidence of the design practices used by undertaking interviews, observations, and reviews of documentation.
- **Coding:** Auditors should seek evidence on the level of care exercised by programming management in choosing a module implementation and integration strategy. Auditors determine whether programming management ensures that programmers follow structured programming conventions.
- **Testing:** Auditors can use interviews, observations, and examination of documentation to evaluate how well unit testing is conducted. They are concerned primarily with the quality of integration testing work carried out by information systems professionals rather than end users.
- **Operation and Maintenance:** Auditors need to ensure effectively and timely reporting of maintenance needs occurs and maintenance is carried out in a well-controlled manner. Auditors should ensure that management has implemented a review system and assigned responsibility for monitoring the status of operational programs

(d) **Data Resource Management Controls:** Auditors should determine what controls are exercised to maintain data integrity. They might also interview database users to determine their level of awareness of these controls. Auditors might employ test data to evaluate whether access controls and update controls are working.

(e) **Quality Assurance Management Controls:** Auditors might use interviews, observations and reviews of documentation to evaluate how well Quality Assurance (QA) personnel perform their monitoring role. Auditors might evaluate how well QA personnel make recommendations for improved standards or processes through interviews, observations, and reviews of documentation.

(f) **Security Management Controls:** Auditors must evaluate whether security administrators are conducting ongoing, high-quality security reviews or not; check whether the organizations audited have appropriate, high-quality disaster recovery plan in place; and check whether the organizations have opted for an appropriate insurance plan or not.

(g) **Operations Management Controls:** Auditors should pay concern to see whether the documentation is maintained securely and that it is issued only to authorized personnel. Auditors can use interviews, observations, and review of documentation to evaluate the activities of documentation librarians; how well operations management undertakes the capacity planning and performance monitoring function; the reliability of outsourcing vendor controls; whether operations management is monitoring compliance with the outsourcing contract; and Whether operations management regularly assesses the financial viability of any outsourcing vendors that an organization uses.

Question 14

As an IS auditor, what are the risks reviewed by you relating to IT systems and processes as part of your functions?

Answer

IS (Information Systems) Auditors review risks relating to IT systems and processes; some of them are as follows:

- Inadequate information security controls (e.g. missing or out of date antivirus controls, open ports, open systems without password or weak passwords etc.)
- Inefficient use of resources, or poor governance (e.g. huge spending on unnecessary IT projects like printing resources, storage devices, high power servers and workstations etc.)
- Ineffective IT strategies, policies and practices (including a lack of policy for use of
- Information and Communication Technology (ICT) resources, Internet usage policies, Security practices etc.).
- IT-related frauds (including phishing, hacking etc).

Question 15

You are appointed to audit the Information Systems of ABC Limited. As a part of preliminary evaluation, list the major aspects which you would study to gain a good understanding of the technology environment and the related control issues.

Answer

As a part of preliminary evaluation, the major aspects which should be studied to gain a good understanding of the technology environment and related control issues are as follows:

- Analysis of business processes and level of automation,
- Assessing the extent of dependence of the enterprise on Information Technology to carry on its businesses i.e. Role of IT in the success and survival of business,
- Understanding technology architecture which could be quite diverse such as a distributed architecture or a centralized architecture or a hybrid architecture,
- Studying network diagrams to understand physical and logical network connectivity,

- Understanding extended enterprise architecture wherein the organization systems connect seamlessly with other stakeholders such as vendors (SCM), customers (CRM), employees (ERM) and the government,
- Knowledge of various technologies and their advantages and limitations is a critical competence requirement for the auditor. For example, authentication risks relating to e-mail systems,
- And finally, studying Information Technology policies, standards, guidelines and procedures.

Question 16

What are the various types of application controls? Explain each control with reference to their performance and the reliability.

Answer

The Application Controls are categorized as below:

- **Boundary Controls:** Establishes interface between the user of the system and the system itself. The system must ensure that it has an authentic user. Users allowed using resources in restricted ways.
- **Input Controls:** These are responsible for bringing both the data and instructions in to the information system. Input Controls are validation and error detection of data input into the system.
- **Communication Controls:** These are responsible for controls over physical components, communication line errors, flows, and links, topological controls, channel access controls, controls over subversive attacks, internetworking controls, communication architecture controls, audit trail controls, and existence controls.
- **Processing Controls:** These are responsible for computing, sorting, classifying and summarizing data. It maintains the chronology of events from the time data is received from input or communication systems to the time data is stored into the database or output as results.
- **Output Controls:** These are the controls to provide functions that determine the data content available to users, data format, timeliness of data and how data is prepared and routed to users.
- **Database Controls:** These are responsible to provide functions to define, create, modify, delete and read data in an information system. It maintains procedural data-set of rules to perform operations on the data to help a manager to take decisions.

The following two types of Audit Trail controls should exist in each application control:

- An Accounting Audit Trail to maintain a record of events within the subsystem; and

- An Operations Audit Trail to maintain a record of the resource consumption associated with each event in the subsystem.

Question 17

What are the factors influencing an organization towards control and audit of computers?

Answer

The factors influencing an organization towards controls and audit of computers are as follows:

- **Organisational Costs of Data Loss:** Data is a critical resource of an organisation for its present and future process and its ability to adapt and survive in a changing environment.
- **Cost of Incorrect Decision Making:** Management and operational controls taken by managers involve detection, investigations and correction of the processes. These high-level decisions require accurate data to make quality decision rules.
- **Costs of Computer Abuse:** Unauthorised access to computer systems, malwares, unauthorised physical access to computer facilities and unauthorised copies of sensitive data can lead to destruction of assets (hardware, software, data, information etc.)
- **Value of Computer Hardware, Software and Personnel:** These are critical resources of an organisation, which has a credible impact on its infrastructure and business competitiveness.
- **High Costs of Computer Error:** In a computerised enterprise environment where many critical business processes are performed, a data error during entry or process would cause great damage.
- **Maintenance of Privacy:** Today, data collected in a business process contains private information about an individual too. These data were also collected before computers but now, there is a fear that privacy has eroded beyond acceptable levels.
- **Controlled evolution of computer Use:** Use of Technology and reliability of complex computer systems cannot be guaranteed and the consequences of using unreliable systems can be destructive.

Question 18

As an IS Auditor, what are the environmental controls verified by you, while conducting physical inspections?

Or

Which aspects of environmental controls should be physically inspected by an information system auditor, while auditing environmental controls? Write any six.

Answer

Audit of environmental controls requires the Information Systems 'auditor to conduct physical inspections and observe practices. The Auditor should verify:

- The IPF (Infrastructure Planning and Facilities) and the construction with regard to 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 exits. 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.

Question 19

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

Answer

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

- ***<u>Methods of Entering Test Data:</u> 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.

- *<u>Methods of Removing the Effects of ITF Transactions:</u> 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*.

Question 20

Define and elaborate categories of risks that affect a system and taken into consideration at the time of assessment or audit of information systems.

Answer

Risks that affect a system and are taken into consideration at the time of assessment or audit of information systems can be differentiated as Inherent risk, Control Risk and Detection Risk. They are as follows:

- *<u>Inherent Risk:</u> Inherent risk is the susceptibility of information resources or resources controlled by the information system to material theft, destruction, disclosure, unauthorized modification, or other impairment, if there are no related internal controls. Inherent risk is the measure of auditor's assessment that there may or may not be material vulnerabilities or gaps in the audit subject exposing it to high risk before considering the effectiveness of internal controls. If the auditor concludes that there is a high likelihood of risk exposure, ignoring internal controls, the auditor would conclude that the inherent risk is high. For example, inherent risk would be high in case of auditing internet banking in comparison to branch banking or inherent risk would be high if the audit subject is an off-site. ATM in an example of the same. Internal controls are ignored in setting inherent risk because they are considered separately in the audit risk model as control risk. It is often an area of professional judgment on the part of an auditor.*
- *<u>Control Risk:</u> Control risk is the risk that could occur in an audit area, and which could be material, individually or in combination with other errors, will not be prevented or detected and corrected on a timely basis by the internal control system. Control risk is a measure of the auditor's assessment of the likelihood that risk exceeding a tolerable level and will not be prevented or detected by the client's internal control system. This assessment includes an assessment of whether a client's internal controls are effective for preventing or detecting gaps and the*

auditor's intention to make that assessment at a level below the maximum (100 percent) as a part of the audit plan.

- *Detection Risk: Detection risk is the risk that the IT auditor's substantive procedures will not detect an error which could be material, individually or in combination with other errors. For example, the detection risk associated with identifying breaches of security in an application system is ordinarily high because logs for the whole period of the audit are not available at the time of the audit. The detection risk associated with lack of identification of disaster recovery plans is ordinarily low since existence is easily verified.*

Question 21

Proper assessment of the degree of risk is critical to the effectiveness of the audit. Discuss some of the critical factors to be considered by an IS Auditor as part of his/her preliminary review.

Answer

Proper assessment of the degree of risk is critical to the effectiveness of the audit. The following are some of the critical factors to be considered by an IS auditor as part of his/her preliminary review.

(i) Knowledge of the Business: Related aspects are General economic factors and industry conditions affecting the entity's business; Nature of Business, its products and services; General exposure to business; Its clientele, vendors and most importantly, strategic business partners/associates to whom critical processes have been outsourced; Level of competence of the Top management and IT Management, and finally, Set up and organization of IT department.

(ii) Understanding the Technology: This includes the process to gain a good understanding of the technology environment and related control issues. This could include consideration of analysis of business processes and level of automation; Role of IT in the success and survival of business; Understanding technology architecture which could be quite diverse such as a distributed architecture or a centralized architecture or a hybrid architecture; Studying network diagrams to understand physical and logical network connectivity; Understanding extended enterprise architecture wherein the organization systems connect seamlessly with other stakeholders such as vendors (SCM), customers (CRM), employees (ERM) and the government; Knowledge of various technologies and their advantages and limitations is a critical competence requirement for the auditor and finally, Studying IT policies, standards, guidelines and procedures.

(iii) Understanding Internal Control Systems: For gaining understanding of Internal Controls emphasis is to be placed on compliance and substantive testing.

(iv) Legal Considerations and Audit Standards: 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 about 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 e.g. 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.

(v) Risk Assessment and Materiality: Risk Assessment is a critical and inherent part of the Information Systems Auditor's planning and audit implementation. It implies the process of identifying the risk, assessing the risk, and recommending controls to reduce the risk to an acceptable level, considering both the probability and the impact of occurrence. Risk assessment allows the auditor to determine the scope of the audit and assess the level of audit risk and error risk (the risk of errors occurring in the area being audited).

Question 22

Write a short note on the following:

(a) Inherent limitations of IS Audit

(b) Role of IS Auditor in Physical Access Control

Answer

(a) Inherent Limitations of Information Systems (IS) Audit are as follows:

- *The nature of financial reporting;*
- *The nature of audit procedures;*
- *The need for the audit to be conducted within a reasonable period of time and at a reasonable cost.*
- *The matter of difficulty, time, or cost involved is not in itself a valid basis for the auditor to omit an audit procedure for which there is no alternative or to be satisfied with audit evidence that is less than persuasive.*
- *Fraud, particularly fraud involving senior management or collusion.*
- *The existence and completeness of related party relationships and transactions.*
- *The occurrence of non-compliance with laws and regulations.*
- *Future events or conditions that may cause an entity to cease to continue as a going concern.*

(b) ***Auditing physical access requires the auditor to review the physical access risk and controls to form an opinion on the effectiveness of the physical access controls. This involves the following:***

- ***Risk Assessment:*** ***The auditor must satisfy him/herself that the risk assessment procedure adequately covers periodic and timely assessment of all assets, physical access threats, vulnerabilities of safeguards and exposures there from.***
- ***Controls Assessment:*** ***The auditor based on the risk profile evaluates whether the physical access controls are in place and adequate to protect the IS assets against the risks.***
- ***Review of Documents:*** ***It requires examination of relevant documentation such as the security policy and procedures, premises plans, building plans, inventory list and cabling diagrams.***

Exercise

1. *What are the factors that influence an organization towards controls and audit of computers?*
2. *Discuss the points relating to 'Legal Considerations and Audit Standards' to be considered by an IS auditor as a part of his/her preliminary review.*
3. *Discuss Integrated Test Facility (ITF) technique of continuous audit in detail with the help of examples.*
4. *What are the major aspects that should be thoroughly examined by an IS Auditor during the audit of Environmental Controls? Explain in brief.*
5. *Discuss audit trails of the following with reference to Application Controls in brief.*

   (a) Input Controls

   (b) Output controls

   (c) Communication Controls

   (d) Database Controls

   (e) Boundary Controls

   (f) Processing Controls
6. *Discuss major audit issues of Tactical Layer with reference to Application Security Audit.*
7. *Write short notes on the following:*

   (i) Basic Plan regarding IS Audit

   (ii) Continuous Auditing

   (iii) Continuous and Intermittent Simulation (CIS) technique

   (iv) Strategic Layer regarding application security audit