4. INFORMATION SYSTEMS AUDITING

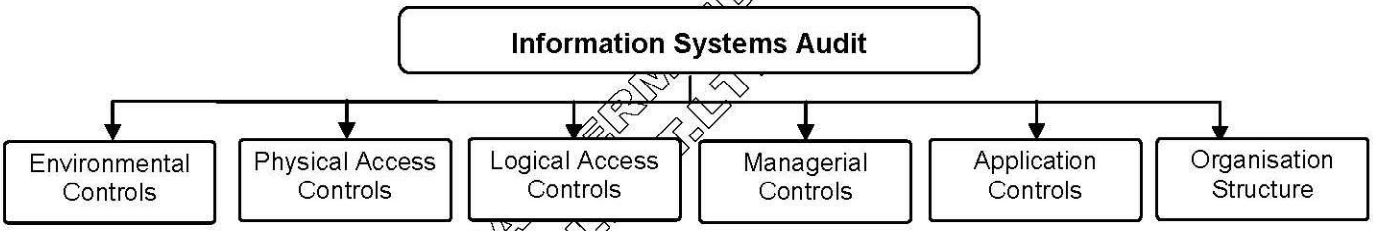
QUESTION WISE ANALYSIS OF PREVIOUS EXAMINATIONS

No.	M-14	N-14	M-15	N-15	M-16	N-16	M-17	N-17	M-18 (O)	M-18 (N)	N-18 (O)	N-18 (N)	M-19 (O)	M-19 (N)	N-19 (O)	N-19 (N)	N-20 (O)	N-20 (N)
THEORY QUESTIONS FOR CLASSROOM DISCUSSION																		
1.	-	-	-	-	-	-	-	-	-	4	-	-	-	-	-	-	-	-
13.																		

CHAPTER OVERVIEW

SECTION	TOPIC	STARTING PAGE NO.
1.	THEORY FOR CLASSROOM DISCUSSION	4.1

SECTION 1: THEORY FOR CLASSROOM DISCUSSION



PART 1: INTRODUCTION

Q.No.1. What is Information Systems Auditing and explain its objectives? (A) (M18 (N) - 4M)

IS Auditing is defined as the process of attesting objectives (those of the external auditor) that focus on asset safeguarding, data integrity and management objectives (those of the internal auditor) that include effectiveness and efficiency both.

This enables organizations to better achieve four major objectives that are as follows:

1) **ASSET SAFEGUARDING OBJECTIVES:** The information system assets (hardware, software, data information etc.) must be protected by a system of internal controls from unauthorized access.
2) **DATA INTEGRITY OBJECTIVES:** It is a fundamental attribute of IS Auditing. The importance to maintain integrity of data of an organization requires all the time.
3) **SYSTEM EFFECTIVENESS OBJECTIVES:** it is evaluated by auditing the characteristics and objective of the system to meet business and user requirements.
4) **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.

SIMILAR QUESTION:

1. The effectiveness of an information system's controls is evaluated through an information systems audit. It is a part of a more general financial audit that verifies an organization's accounting records and financial statements. Information systems are designed so that every financial transaction can be traced. In this context as an IS auditor can you define IS audit along with its objectives.

A. Refer above answer.

Q.No.2. Explain the Need for Audit of Information Systems? (or) Explain about the impact of controls and audit influencing an organization? (A)

1) **ORGANIZATIONAL COSTS OF DATA LOSS:** Data is a critical resource of an organisation for its present and future process and for its ability to adapt and survive in a changing environment.
2) **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.
3) **COSTS OF COMPUTER ABUSE:** Unauthorized access to computer systems, malwares, unauthorised physical access to computer facilities and unauthorized copies of sensitive data can lead to destruction of assets (hardware, software, data, information etc.)
4) **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.
5) **HIGH COSTS OF COMPUTER ERROR:** In a computerized enterprise environment where many critical business processes are performed, a data error during entry or process would cause great damage.
6) **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.
7) **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.

SIMILAR QUESTION:

1. An information systems audit is important because it gives assurance that the IT systems are adequately protected, provide reliable information to users, and are properly managed to achieve their intended benefits. It also reduces the risk data tampering, data loss or leakage, service disruption and poor management of IT systems. In this context can you explore further the need of IS audit for an organization?

A. Refer above answer.

Q.No.3. What is Concurrent or Continuous Audit? Explain different Types of Audit Tools? (A) (RTP M18 (N))

Today, organizations produce information on a real-time, online basis. Real-time recordings need real-time auditing to provide continuous assurance about the quality of the data that is called as continuous auditing. Continuous auditing enables auditors to significantly reduce and perhaps to eliminate the time gap between occurrence of the client's events and the auditor's assurance services thereon.

TYPES OF AUDIT TOOLS:

1) **SNAPSHOTS:**
   a) Tracing a transaction in a computerized system can be performed with the help of snapshots or extended records.
   b) 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.
   c) These images can be utilized to assess the authenticity, accuracy, and completeness of the processing carried out on the transaction.
2) **INTEGRATED TEST FACILITY (ITF):**
   1) 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.
   2) This test data would be included with the normal production data used as input to the application system.
3) **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.

4) **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.

5) **AUDIT HOOKS:**

   a) There are audit routines that flag suspicious transactions.

   b) *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.*

   c) 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.

   d) When audit hooks are employed, auditors can be informed of questionable transactions as soon as they occur. This approach of real time notifications displays a message on the auditor's terminal.

SIMILAR QUESTION:

1. Errors in a computerized system are generated at high speeds and the cost to correct and rerun programs are high. If these errors can be detected and corrected at the point or closest to the point of their occurrence the impact thereof would be the least and that requires several continuous auditing tools. As an IS auditor what tools do you use in general for continuous audit process. Make a brief note on them.

A. Refer above answer.

Q.No.4. Discuss the advantages of continuous Audit Techniques? (B) (RTP-M18)

Some of the advantages of continuous audit techniques are as under:

1) **TIMELY, COMPREHENSIVE AND DETAILED AUDITING:** Evidence would be available more timely and in a comprehensive manner. The entire processing can be evaluated and analysed rather than examining the inputs and the outputs only.

2) **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.

3) **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.

4) **TRAINING FOR NEW USERS:** Using the Integrated Test Facilities (ITF) s, new users can submit data to the application system, and obtain feedback on any mistakes they make via the system's error reports.

PART 2: AUDIT TRAIL

Q.No.5. What is Audit Trail? Explain types and objectives of Audit Trail? (A) (MTP2 N18)

1) **Audit Trails** are logs that can be designed to record activity at the system, application, and user level. When properly implemented, audit trails provide an important detective control to help accomplish security policy objectives.

   TYPES OF AUDIT TRAIL:

   a) **The Accounting Audit Trail** shows the source and nature of data and processes that update the database.

   b) **The Operations Audit Trail** maintains a record of attempted or actual resource consumption within a system.

2) **AUDIT TRAIL OBJECTIVES:** Audit trails can be used to support security objectives in three ways:

   a) **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.*

b) **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.

c) **Personal Accountability:** Audit trails can be used to monitor user activity at the lowest level of detail. This serves as a preventive control. Individuals are likely to violate an organization's security policy if they know that their actions are not recorded in an audit log.

SIMILAR QUESTIONS:

1. Electronic information storage has transformed many industries, including financial services, technology, and healthcare. The modern business and technological landscapes are infinitely more complex. There are innumerable challenges in limiting information access to only a few key members of the workforce, particularly in smaller organizations where team members perform multi-functional duties. In order to maintain control over private customer information, organizations must maintain robust, comprehensive audit trails to answer queries, fulfill statutory requirements, detect the consequences of error and allow system monitoring and tuning.. Then As an IS auditor with what objectives in mind do you setup Audit trails in the IS of an organization?

A. Refer above answer

Q.No.6. what is the role of auditor in Auditing Environmental Controls? What factors are to be considered by auditor in Auditing Environmental Controls? (B)

1) **ROLE OF AUDITOR IN AUDITING ENVIRONMENTAL CONTROLS:** The IS auditor should satisfy not only the effectiveness of various technical controls but also the overall controls safeguarding the business against environmental risks.

2) **AUDIT OF ENVIRONMENTAL CONTROLS:** Audit of environmental controls requires the IS auditor to conduct physical inspections and observe practices. Auditing environmental controls requires knowledge of building mechanical and electrical systems as well as fire codes. *The IS auditor needs to be able to determine if such controls are effective and if they are cost-effective.*

3) **AUDITING ENVIRONMENTAL CONTROLS REQUIRES ATTENTION TO THESE AND OTHER FACTORS AND ACTIVITIES, INCLUDING:**

a) **Power conditioning:** The IS auditor should determine how frequently power conditioning equipment, such as UPS, line conditioners, surge protectors, or motor generators, are used, inspected and maintained and if this is performed by qualified personnel.

b) **Backup power:** The IS auditor should determine if backup power is available via electric generators or UPS and how frequently they are tested. He or she should examine maintenance records to see how frequently these components are maintained and if this is done by qualified personnel.

c) **Heating, Ventilation, and Air Conditioning (HVAC):** The IS auditor should determine if HVAC systems are providing adequate temperature and humidity levels, and if they are monitored and maintained properly .

d) **Water detection:** The IS auditor should determine if any water detectors are used in rooms where computers are used. He or she should determine how frequently these are tested and if they are monitored.

e) **Fire detection and suppression:** The IS auditor should determine if fire detection equipment is adequate, if staff members understand their function, and if they are tested. He or she should determine how frequently fire suppression systems are inspected and tested, and if the organization has emergency evacuation plans and conducts fire drills.

f) **Cleanliness:** The IS auditor should examine data centers to see how clean they are. IT equipment air filters and the inside of some IT components should be examined to see if there is an accumulation of dust and dirt.

SIMILAR QUESTION:

1. The attack on the World Trade Centre in 2001 has created a worldwide alert bringing focus on business continuity planning and 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. In this context what are some of the critical environmental audit considerations that an IS auditor should consider while conducting his/her audit?

A. Refer above answer.

Q.No.7. what is the role of Auditor in Auditing Physical Access Controls? What are the Physical Access Controls that should be audited by Auditor? (B)

1) **ROLE OF IS AUDITOR IN AUDITING 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 the following:

   a) Risk Assessment

   b) Controls Assessment

   c) Review of Documents

2) **AUDIT OF PHYSICAL ACCESS CONTROLS:** Auditing physical security controls requires knowledge of natural and manmade hazards, physical security controls, and access control systems.

   a) **Siting and Marking:** Auditing building siting and marking requires attention to several key factors and features, including:

      Proximity to hazards:

      i) The IS auditor should estimate the building's distance to natural and man made hazards, such as Dams; Rivers; Natural gas and petroleum pipelines; Water mains and pipelines; Earthquake faults; Volcanoes;

      ii) The IS auditor should determine if any risk assessment regarding hazards has been performed and if any compensating controls that were recommended have been carried out.

      Marking: The IS auditor should inspect the building and surrounding area to see if building(s) containing information processing equipment identify the organization. Marking may be visible on the building itself, but also on signs or parking stickers on vehicles.

   b) **Physical barriers:** This includes fencing, walls, barbed/razor wire, bollards, and crash gates. The IS auditor needs to understand how these are used to control access to the facility and determine their effectiveness.

   c) **Surveillance:** The IS auditor needs to understand how video and human surveillance are used to control and monitor access. He or she needs to understand how (and if) video is recorded and reviewed, and if it is effective in preventing or detecting incidents.

   d) **Guards and dogs:** The IS auditor needs to understand the use and effectiveness of security guards and guard dogs. Processes, policies, procedures, and records should be examined to understand required activities and how they are carried out.

   e) **Key-Card systems:** The IS auditor needs to understand how key-card systems are used to control access to the facility. Whether the facility is divided into security zones and which persons are permitted to access which zones whether key-card systems record personnel movement;

SIMILAR QUESTION:

1. A comprehensive physical inspection and evaluation of every aspect of your security system, its controls, and their parameters throughout your space or facility is required. This is done on both an individual and a macro level, giving you the intelligence you need to make better decisions about how to run your facility. Then what are the key areas that an IS auditor should focus in physical security audit of an IS?

A. Refer above answer.

Q.No.8. what are the key areas in Auditing of Logical Access Controls? (B)

ROLE OF IS AUDITOR IN AUDITING LOGICAL ACCESS CONTROLS: Auditing Logical Access Controls requires attention to several key areas that include the following:

1) **Network Access Paths:** The IS auditor should conduct an independent review of the IT infrastructure to map out the organization's logical access paths. This will require considerable effort and may require the use of investigative and technical tools, as well as specialized experts on IT network architecture.

2) **Documentation:** The IS auditor should request network architecture and access documentation to compare what was discovered independently against existing documentation. The auditor will need to determine why any discrepancies exist.

SIMILAR QUESTION:

1. Logical access controls tools are used for credentials, validation, authorization, and accountability in an infrastructure and the systems within. These components enforce access control measures for systems, applications, processes, and information. This type of access control can also be embedded inside an application, operating system, database, or infrastructure administrative system. Then describe the role of auditor in auditing logical access controls.

A. Refer above answer.

Q.No.9. What factors are to be considered while auditing user Access Controls? (B)

USER ACCESS CONTROLS: User access controls are often the only barrier between unauthorized parties and sensitive or valuable information. Auditing user access controls requires keen attention to several key factors and activities in four areas:

1) **AUDITING USER ACCESS CONTROLS:** Auditing user access controls requires attention to several factors, including:

   1) **Authentication:** The auditor should examine network and system resources to determine if they require authentication, or whether any resources can be accessed without first authenticating.

   2) **Access violations:** The auditor should determine if systems, networks, and authentication mechanisms can log access violations.

   3) **User account lockout:** The auditor should determine if systems and networks can automatically lock user accounts that are the target of attacks.

   4) **Intrusion detection and prevention:** The auditor should determine if there are any IDSs or IPSs that would detect authentication-bypass attempts. The auditor should examine these systems to see whether they have up-to-date configurations and signatures.

   5) **Dormant accounts:** The IS auditor should determine if any automated or manual process exists to identify and close dormant accounts. Dormant accounts are user (or system) accounts that exist but are unused.

   6) **Shared accounts:** The IS auditor should determine if there are any shared user accounts; the principal risk with shared accounts is the inability to determine accountability for actions performed with the account.

   7) **System accounts:** The IS auditor should identify all system-level accounts on networks. The purpose of each system account should be identified. The IS auditor should determine who has the password for each system account, whether accesses by system accounts are logged, and who monitors those logs.

2) **AUDITING PASSWORD MANAGEMENT:** The IS auditor needs to examine password configuration settings on information systems to determine how passwords are controlled. Some of the areas requiring examination are how many characters must a password have and whether there is a maximum length; how frequently must passwords be changed.

SIMILAR QUESTION:

1. Identity and access management (IAM) is the process of managing who has access to what information over time. This cross-functional activity involves the creation of distinct identities for individuals and systems, as well as the association of system and application-level accounts to these identities. IAM processes are used to initiate, capture, record, and manage the user identities and related access permissions to the organization's proprietary information .Then in an IS audit what are the key controls related to user access are to be focused by the auditor?

A. Refer answer above.

Q.NO.10. Write about auditing the User Access Provisioning. (A) (M19 4M)

AUDITING USER ACCESS PROVISIONING: Auditing the user access provisioning process requires attention to several key activities, including:

ACCESS REQUEST PROCESSES: The IS auditor should identify all user access request processes and determine if these processes are used consistently throughout the organization.

1) **Access approvals:** The IS auditor needs to determine how requests are approved and by what authority they are approved.
2) **New employee provisioning:** The IS auditor should examine the new employee provisioning process to see how a new employee's user accounts are initially set up.
3) **Segregation of Duties (SOD):** The IS auditor should *whether there are any SOD matrices in existence and if they are actively used to make user access request decisions.*
4) **Access reviews:** The IS auditor should determine if there are any periodic access reviews and what aspects of user accounts are reviewed; this may include termination reviews, internal transfer reviews, SOD reviews, and dormant account reviews.

Q.NO.11. Write about Auditing of Employee Terminations (C)

AUDITING EMPLOYEE TERMINATIONS: Auditing employee terminations requires attention to several key factors, including:

a) **Termination process:** The IS auditor should examine the employee termination process and determine its effectiveness.
b) **Access reviews:** The IS auditor should determine if any internal reviews of terminated accounts are performed. *If such reviews are performed, the auditor should determine if any missed terminations are identified and if any process improvements are undertaken.*
c) **Contractor access and terminations:** The IS auditor needs to determine the effectiveness of contractor access and termination

Q.No.12. What factors are to be considered while Auditing user Access logs? (B) (MTP2 M18 MTP2 M19)

The IS auditor needs to determine what events are recorded in access logs. The IS auditor needs to understand the capabilities of the system being audited and determine if the right events are being logged.

1) **CENTRALIZED ACCESS LOGS:** The IS auditor should determine if the organization's access logs are aggregated or if they are stored on individual systems.
2) **ACCESS LOG PROTECTION:** The auditor needs to determine if access logs can be altered, destroyed, or attacked to cause the system to stop logging events. *For especially high-value and high-sensitivity environments, the IS auditor needs to determine if logs should be written to digital media that is unalterable.*
3) **ACCESS LOG REVIEW:** The IS auditor needs to determine if there are policies, processes, or procedures regarding access log review. *The auditor should determine if access log reviews take place, who performs them, how issues requiring attention are identified, and what actions are taken when necessary.*
4) **ACCESS LOG RETENTION:** The IS auditor should determine how long access logs are retained by the organization and if they are backed up.

SIMILAR QUESTION:

1. IT administrators often need to know who logged on to their computers and when for security and compliance reasons. Although you can use the native auditing methods supplied through OS to track user account logon and logoff events, you may end up having to sift through thousands of records to reach the required log. Once you've found the required log, getting the required information for compliance and security reports is not an easy process. Hence IS auditors design special user access logs and the IS auditor needs to determine what events are recorded in access logs. What areas are to be considered while auditing user access logs?

   A. Refer above answer

Q.No.13. What are the key activities to be performed while Auditing investigative procedures? (C)

AUDITING INVESTIGATIVE PROCEDURES REQUIRES ATTENTION TO SEVERAL KEY ACTIVITIES, INCLUDING:

1) **INVESTIGATION POLICIES AND PROCEDURES:** The IS auditor should determine if there are any policies or procedures regarding security investigations. This would include who is responsible for performing investigations, where information about investigations is stored, and to whom the results of investigations are reported.
2) **COMPUTER CRIME INVESTIGATIONS:** The IS auditor should determine if there are policies, processes, procedures, and records regarding computer crime investigations. The IS auditor should understand how internal investigations are transitioned to law enforcement.
3) **COMPUTER FORENSICS:** The IS auditor should determine if there are procedures for conducting computer forensics. The auditor should also identify tools and techniques that are available to the organization for the acquisition and custody of forensic data.

SIMILAR QUESTION:

1. Investigation involves inquiry into facts behind the books and accounts, into the technical, financial and the economic position of the business or organization. What activities should an IS auditor perform to understand the prevailing investigative procedures in an IS Setup?

A. Refer above answer.

Q.No.14. Explain Internet Points of Presence in Audit of Logical Access Controls? (A)

The IS auditor who is performing a comprehensive audit of an organization's system and network system needs to perform a "points of presence" audit to discover what technical information is available about the organization's Internet presence.

Some of the aspects of this intelligence gathering include:

1) **SEARCH ENGINES:** Google, Yahoo!, and other search engines should be consulted to see what information about the organization is available. Searches should include the names of company officers and management, key technologists, and any internal-only nomenclature such as the names of projects.
2) **SOCIAL NETWORKING SITES:** Social networking sites such as Facebook, LinkedIn, Myspace, and Twitter should be searched to see what employees, former employees, and others are saying about the organization. Any authorized or unauthorized “fan pages” should be searched as well.
3) **ONLINE SALES SITES:** Sites such as craigslist and eBay should be searched to see if anything related to the organization is sold online.
4) **DOMAIN NAMES:** The IS auditor should verify contact information for known domain names, as well as related domain names.
5) **JUSTIFICATION OF ONLINE PRESENCE:** The IS auditor should examine business records to determine on what basis the organization established online capabilities such as e-mail, Internet-facing web sites, Internet e-commerce, Internet access for employees, and so on.

Similar question:

1. Organizations internet presence may cause threat to the security of the information system in many ways in this respect what areas are to be focused by an IS auditor who is performing a comprehensive audit of an organization's system and network system to justify the organizations internet presence?

A. Refer above answer.

Q.No.15. What is the role of Auditor in Top Management and Information Systems Management Controls? (B)

The major activities that senior management must perform are – **Planning, Organizing, Leading** and **Controlling**. The Role of auditor at each activity is discussed below:

1) **PLANNING:** Auditors need to evaluate whether top management has formulated a high-quality information system's plan that is appropriate to the needs of an organization or not.

2) **ORGANIZING**: Auditors should be concerned about how well top management acquires and manages staff resources.

3) **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.

4) **CONTROLLING:** Auditors must evaluate whether top management's choice to the means of control over the users of IS services is likely to be effective or not.

SIMILAR QUESTION:

1. The auditors play a vital role in evaluating the performance of various controls under managerial controls. What are some of the key areas that auditors should pay attention to while evaluating Managerial controls?

A. Refer above answer.

Q.No.16. Explain the role of Auditor in System Development Management Controls? (B)

Three different types of audits may be conducted during system development process as discussed in the Table

Different types of Audit during System Development Process

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.

SIMILAR QUESTION:

1. 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 or systems effectiveness and efficiency. An external auditor is more likely to undertake general audits rather than concurrent or post-implementation audits of the systems development process. In this context what are the three different types of audits that may be conducted during system development process by the IS auditors. Elucidate

A. Refer above answer.

Q.No.17. Explain the role of Auditor in Programming Management Controls? (B)

Audit Trails under Programming Management Controls

Phase	Audit Trails
Planning	a) They should evaluate whether nature of and extent of planning are appropriate to different types of s/w that are developed or acquired. b) They must evaluate how well the planning work is being undertaken.
Control	a) 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. b) They must gather evidence on whether the control procedures are operating reliably.
Design	a) Auditors should find out whether programmers use some type of systematic approach to design. b) Auditors can obtain evidence of the design practices used by undertaking interviews, observations, and reviews of documentation.

Coding	Auditors should seek evidence – **a)** On the level of care exercised by programming management in choosing a module implementation and integration strategy. **b)** To determine whether programming management ensures that programmers follow structured programming conventions. **c)** To check whether programmers employ automated facilities to assist them with their coding work.
Testing	**a)** Auditors can use interviews, observations, and examination of documentation to evaluate how well unit testing is conducted. **b)** Auditors are most likely 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.

Similar question:

1. Programming management is an important phase in system development management.in this context what are the Some of the major concerns that an Auditor should address under different activities involved in Programming Management Control Phase of IS audit.

A. Refer above answer.

Q.No.18. Explain the role of Auditor in Data Resource Management Controls? (C)

1) Auditors should determine what controls are exercised to maintain data integrity.

2) They might also interview database users to determine their level of awareness of these controls.

3) Auditors might employ test data to evaluate whether access controls and update controls are working.

Q.No.19. Explain the role of Auditor in Quality Assurance Management Controls? (C)

1) Auditors might use interviews, observations and reviews of documentation to evaluate how well Quality Assurance (QA) personnel perform their monitoring role.

2) Auditors might evaluate how well QA personnel make recommendations for improved standards or processes through interviews, observations, and reviews of documentation.

3) Auditors can evaluate how well QA personnel undertake the reporting function and training through interviews, observations, and reviews of documentation.

Q.No.20. Explain the role of Auditor in Security Management Controls? (C)

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

2) Auditors check whether the organizations audited have appropriate, high-quality disaster recovery plan in place; and

3) Auditors check whether the organizations have opted for an appropriate insurance plan or not.

Q.No.21. Explain the role of Auditor in Operations Management Controls? (B)

1) Auditors should pay concern to see whether the documentation is maintained securely and that it is issued only to authorized personnel.

2) Auditors can use interviews, observations, and review of documentation to evaluate -

   a) the activities of documentation librarians;

   b) how well operations management undertakes the capacity planning and performance monitoring function;

   c) the reliability of outsourcing vendor controls;

d) whether operations management is monitoring compliance with the outsourcing contract; and

e) Whether operations management regularly assesses the financial viability of any outsourcing vendors that an organization uses.

Q.No.22. Audit Trails for Boundary Controls. (B)

This maintains the chronology of events that occur when a user attempts to gain access to and employ systems resources. This includes the following:

1) Identity of the would-be user of the system;
2) Authentication information supplied;
3) Resources requested;
4) Action privileges requested;
5) Terminal Identifier;
6) Start and Finish Time;
7) *Number of Sign-on attempts;*
8) *Resources provided/denied; and*

Accounting Audit Trail: Action privileges allowed/denied.

Operations Audit Trail

1) Resource usage from log-on to log-out time.
2) Log of Resource consumption.

Q.No.23. Audit Trails for Input Controls. (B)

This maintains the chronology of events from the time data and instructions are captured and entered into an application system until the time they are deemed valid and passed onto other subsystems within the application system.

1) **ACCOUNTING AUDIT TRAIL:**
   - **a)** The identity of the person(organization) who was the source of the data;
   - **b)** The identity of the person(organization) who entered the data into the system;
   - **c)** The time and date when the data was captured;
   - **d)** The identifier of the physical device used to enter the data into the system;
   - **e)** The account or record to be updated by the transaction;
   - *f) The standing data to be updated by the transaction;*
   - *g) The details of the transaction; and*
   - *h) The number of the physical or logical batch to which the transaction belongs.*

2) **OPERATIONS AUDIT TRAIL:**
   - **a)** Time to key in a source document or an instrument at a terminal;
   - **b)** Number of read errors made by an optical scanning device;
   - **c)** Number of keying errors identified during verification;
   - **d)** Frequency with which an instruction in a command language is used; and
   - **e)** Time taken to invoke an instruction using a light pen versus a mouse.

Q.No.24. Audit Trails for Communication Controls. (B)

This maintains a chronology of the events from the time a sender dispatches a message to the time a receiver obtains the message.

1) **ACCOUNTING AUDIT TRAIL:**

   a) Unique identifier of the source/sink node;

   b) Time and date at which the message was received by the sink node;

   c) Time and date at which node in the network was traversed by the message; and

   d) Message sequence number; and the image of the message received at each node traversed in the network.

2) **OPERATIONS AUDIT TRAIL:**

   a) Number of messages that have traversed each link and each node;

   b) Log of system restarts; and

   c) Message transit times between nodes and at nodes.

Q.No.25. Audit Trails for Processing Controls. (B)

The audit trail maintains the chronology of events from the time data is received from the input or communication subsystem to the time data is dispatched to the database, communication, or output subsystems.

1) **ACCOUNTING AUDIT TRAIL:**

   a) To trace and replicate the processing performed on a data item.

   b) To follow triggered transactions from end to end by monitoring input data entry, intermediate results and output data values.

   c) To check for existence of any data flow diagrams or flowcharts that describe data flow in the transaction, and whether such diagrams or flowcharts correctly identify the flow of data.

   d) To check whether audit log entries recorded the changes made in the data items at any time including who made them.

2) **OPERATIONS AUDIT TRAIL:**

   a) A comprehensive log on hardware consumption - CPU time used, secondary storage space used, and communication facilities used.

   b) A comprehensive log on software consumption - compilers used, subroutine libraries used, file management facilities used, and communication software used.

Q.No.26. Audit Trails for Database Controls. (B)

The audit trail maintains the chronology of events that occur either to the database definition or the database itself.

1) **ACCOUNTING AUDIT TRAIL:**

   a) To confirm whether an application properly accepts, processes, and stores information.

   b) To attach a unique time stamp to all transactions.

   c) To attach before-images and after-images of the data item on which a transaction is applied to the audit trail.

   d) Any modifications or corrections to audit trail transactions accommodating the changes that occur within an application system.

e) To not only test the stated input, calculation, and output rules for data integrity, but also should assess the efficacy of the rules themselves.

2) **OPERATIONS AUDIT TRAIL:** To maintain a chronology of resource consumption events that affects the database definition or the database.

Q.No.27. Audit Trails for output Controls? (C) (For Student's Self - Study)

The audit trail maintains the chronology of events that occur from the time the content of the output is determined until the time users complete their disposal of output because it no longer should be retained.

1) **ACCOUNTING AUDIT TRAIL:**

a) What output was presented to users;

b) Who received the output;

c) When the output was received;

d) What actions were taken with the output

2) **OPERATIONS AUDIT TRAIL:** To maintain the record of resources consumed - graphs, images, report pages, printing time and display rate to produce the various outputs.

PART 3: ORGANIZATION STRUCTURE AND RESPONSIBILITIES

Q.NO.28.What is ORGANIZATION STRUCTURE? Explain several conditions that changes organization structure? (C) (For student Self-study)

Organizations require structure to distribute responsibility to groups of people with specific skills and knowledge. The structure of an organization is called an organization chart (org chart). In most organizations, the organization chart is a living structure that changes frequently, based upon several conditions including the following:

1) **MARKET CONDITIONS:** Changes in market positions can cause an organization to realign its internal structure in order to strengthen itself. **Example**: if a competitor lowers its prices based on a new sourcing strategy, an organization may need to respond by changing its organizational structure to put experienced executives In charge of specific activities.

2) **REGULATION:** New regulations may induce an organization to change its organizational structure. For instance, an organization that becomes highly regulated may elect to move its security and compliance group away from IT and place it under the legal department, since compliance has much more to do with legal compliance than industry standards.

3) **AVAILABLE TALENT:** When someone leaves the organization (or moves to another position within the organization), particularly in positions of leadership, a space opens in the org chart that often cannot be filled right away. Instead, senior management will temporarily change the structure of the organization by moving the leaderless department under the control of someone else.

Q.NO.29. Write about Individual Roles and Responsibilities in an Organization? (C)

Several roles and responsibilities fall upon all individuals throughout the organization.

1) **EXECUTIVE MANAGEMENT:** The most senior managers and executives in an organization are responsible for developing the organization's mission, objectives, and goals, as well as policy. Executives are responsible for enacting security policy, which defines (among other things) the protection of assets.

2) **OWNER:** An owner is an individual (usually but not necessarily a manager) who is the designated owner-steward of an asset. If the asset is information, the owner may be responsible for determining who may access and make changes to the information.

3) **MANAGER:** A manager is, in the general sense, responsible for obtaining policies and procedures and making them available to their staff members. They should also, to some extent, be responsible for their staff members' behavior.

4) **USER:** Users are individuals (at any level of the organization) who use assets in the performance of their job duties. Each user is responsible for how he or she uses the asset, and does not permit others to access the asset in his or her name. Users are responsible for performing their duties lawfully and for conforming to organization policies.

These generic roles and responsibilities should apply across the organization chart to include every person in the organization.

Q.No.30. What is Job Title? How Job Title helps organizations in different ways? (A)

A Job Title is a label that is assigned to a job description. It denotes a position in the organization that has a given set of responsibilities, and which requires a certain level and focus of education and prior experience.

Job titles in IT have matured and are quite consistent across organizations. This consistency helps organizations in several ways:

a) **RECRUITING:** When the organization needs to find someone to fill an open position, the use of standard job titles will help prospective candidates more easily find positions that match their criteria.

b) **COMPENSATION BASELINING:** Because of the chronic shortage of talented IT workers, organizations are forced to be more competitive when trying to attract new workers. The use of standard job titles makes the task of comparing compensation far easier.

c) **CAREER ADVANCEMENT:** When an organization uses job titles that are consistent in the industry, IT workers have a better understanding of the functions of positions within their own organizations and can more easily plan how they can advance.

Q.No.31. Explain different job titles in Executive Management level? (A)

Executive managers are the chief leaders and policymakers in an organization. They set objectives and work directly with the organization's most senior management to help make decisions affecting the future strategy of the organization.

1) **CIO (Chief Information Officer):** This is the title of the top most leader in a larger IT organization.

2) **CTO (Chief Technical Officer):** This position is usually responsible for an organization's overall technology strategy. Depending upon the purpose of the organization, this position may be separate from IT.

3) **CSO (Chief Security Officer):** This position is responsible for all aspects of security, including information security, physical security, and possibly executive protection.

4) **CISO (Chief Information Security Officer):** This position is responsible for all aspects of data-related security.

5) **CPO (Chief Privacy Officer):** This position is responsible for the protection and use of personal information. This position is found in organizations that collect and store sensitive information for large numbers of persons.

Q.No.32. Explain different job titles in Software Development? (A)

Positions in software development are involved in the design, development, and testing of software applications.

a) **Systems Architect:** This position is usually responsible for the overall information systems architecture in the organization.

b) **Systems Analyst:** This position may develop technical requirements, program design, and software test plans.

c) **Software Developer, Programmer:** This position develops application software.

d) **Software Tester:** This position tests changes in programs made by software developers.

Q.No.33. Explain different job titles in Data Management? (A)

Positions in data management are responsible for developing and implementing database designs and for maintaining databases.

1) **DATABASE ARCHITECT:** This position develops logical and physical designs of data models for applications. With sufficient experience, this person may also design an organization's overall data architecture.

2) **DATABASE ADMINISTRATOR (DBA):** This position builds and maintains databases designed by the database architect and those databases that are included as a part of purchased applications. *The DBA monitors databases, tunes them for performance and efficiency, and troubleshoots problems.*

3) **DATABASE ANALYST:** This position performs tasks that are junior to the database administrator, carrying out routine data maintenance and monitoring tasks.

Q.No.34. Explain different job titles in Network Management? (A)

Positions in network management are responsible for designing, building, monitoring, and maintaining voice and data communications networks, including connections to outside business partners and the Internet.

1) **NETWORK ARCHITECT:** This position designs data and (increasingly) voice networks and designs changes and upgrades to the network as needed to meet new organization objectives.

2) **NETWORK ENGINEER:** This position builds and maintains network devices such as routers, switches, firewalls, and gateways.

3) **NETWORK ADMINISTRATOR:** This position performs routine tasks in the network such as making minor configuration changes and monitoring event logs.

4) **TELECOM ENGINEER:** Positions in this role work with telecommunications technologies such as data circuits, phone systems, and voice mail systems.

Q.No.35. Explain different job titles in Systems Management? (A)

Positions in systems management are responsible for architecture, design, building, and maintenance of servers and operating systems. This may include desktop operating systems as well.

1) **SYSTEMS ARCHITECT:** responsible for the overall architecture of systems.

2) **SYSTEMS ENGINEER:** responsible for designing, building, and maintaining servers and server operating systems.

3) **STORAGE ENGINEER:** responsible for designing, building, and maintaining storage subsystems.

4) **SYSTEMS ADMINISTRATOR:** responsible for performing maintenance and configuration operations on systems.

Q.No.36. Explain different job titles in General Operations (C)

Positions in operations are responsible for day-to-day operational tasks that may include networks, servers, databases, and applications.

1) **OPERATIONS MANAGER:** responsible for overall operations that are carried out by others. Responsibilities will include establishing operations shift schedules.

2) **OPERATIONS ANALYST:** responsible for the development of operational procedures; examining the health of networks, systems, and databases; setting and monitoring the operations schedule; and maintaining operations records.

3) **CONTROLS ANALYST:** responsible for monitoring batch jobs, data entry work, and other tasks to make sure that they are operating correctly.

4) **SYSTEMS OPERATOR:** responsible for monitoring systems and networks, performing backup tasks, running batch jobs, printing reports, and other operational tasks.

5) **DATA ENTRY:** responsible for keying batches of data from hard copy sources.

6) **MEDIA LIBRARIAN:** responsible for maintaining and tracking the use and whereabouts of backup tapes and other media.

Q.No.37. Explain different job titles in Security Operations? (B)

Positions in security operations are responsible for designing, building, and monitoring security systems and security controls, to ensure the confidentiality, integrity, and availability of information systems.

1) **SECURITY ARCHITECT:** This position is responsible for the design of security controls and systems such as authentication, audit logging, intrusion detection systems, intrusion prevention systems, and firewalls.

2) **SECURITY ENGINEER:** This position is responsible for designing, building, and maintaining security services and systems that are designed by the security architect.

3) **SECURITY ANALYST:** This position is responsible for examining logs from firewalls, intrusion detection systems, and audit logs from systems and applications. This position may also be responsible for issuing security advisories to others in IT.

4) **USER ACCOUNT MANAGEMENT:** This position is responsible for accepting approved requests for user access management changes and performing the necessary changes at the network, system, database, or application level.

5) **SECURITY AUDITOR:** This position is responsible for performing internal audits of IT controls to ensure that they are being operated properly.

Q.No.38. Explain different job titles in Service Desk? (C)

a) Positions at the service desk are responsible for providing front line support services to IT and its customers.

b) **HELP DESK ANALYST:** This position is responsible for providing front line user support services to personnel in the organization.

c) **TECHNICAL SUPPORT ANALYST:** This position is responsible for providing technical support services to other IT personnel, and perhaps also to IT customers.

PART 4: SEGREGATION OF DUTIES

Q.No.39. Define SEGREGATION OF DUTIES? Write Some Examples of Segregation of Duties Controls? (A) N19

SEGREGATION OF DUTIES (SOD): also known as separation of duties, ensures that single individuals do not possess excess privileges that could result in unauthorized activities such as fraud or the manipulation or exposure of sensitive data.

SOME EXAMPLES OF SEGREGATION OF DUTIES CONTROLS:

1) **TRANSACTION AUTHORIZATION:** Information systems can be programmed or configured to require two (or more) persons to approve certain transactions. In IT applications, transactions meeting certain criteria (for example, exceeding normally accepted limits or conditions) may require a manager's approval to be able to proceed.

2) **SPLIT CUSTODY OF HIGH-VALUE ASSETS:** Assets of high importance or value can be protected using various means of split custody. *For example, a password to an encryption key that protects a highly-valued asset can be split in two halves, one half assigned to two persons, and the other half assigned to two persons, so that no single individual knows the entire password.*

3) **WORKFLOW:** Applications that are workflow-enabled can use a second (or third) level of approval before certain high-value or high-sensitivity activities can take place. *For example, a workflow application that is used to provision user accounts can include extra management approval steps in requests for administrative privileges.*

4) **PERIODIC REVIEWS:** IT or internal audit personnel can periodically review user access rights to identify whether any segregation of duties issues exist. The access privileges for each worker can be compared against a segregation of duties control matrix.

   When SOD issues are encountered during a segregation of duties review, management will need to decide how to mitigate the matter. The choices for mitigating a SOD issue include -

5) **REDUCE ACCESS PRIVILEGES:** Management can reduce individual user privileges so that the conflict no longer exists.

6) **INTRODUCE A NEW MITIGATING CONTROL:** If management has determined that the person(s) need to retain privileges that are viewed as a conflict, then new preventive or detective controls need to be introduced that will prevent or detect unwanted activities.

THE END