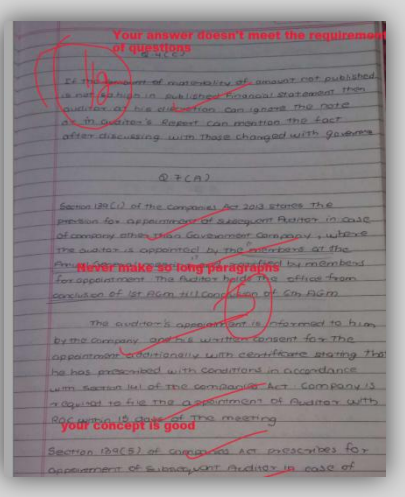
TEST SERIES AVAILABLE AT NOMINAL CHARGES STARTING 250/-

How It Works?	Why Choose Us?
 **HOW TO REGISTER?** - STUDENT CAN SIMPLY REGISTER BY VISITING WWW.CATESTSERIES.ORG AND SELECT PLAN AS THEIR PREFERANCE.  **HOW TO GIVE TEST?** - LOGIN AND DOWNLOAD PDF. WRITE TEST AND UPLOAD YOUR FILE.  **WHAT KINDS OF PLAN IT HAVE?** - CATESTSERIES.ORG COMES WITH 4 KINDS OF PLAN. VISIT - HTTPS://WWW.CATESTSERIES.ORG/SYLLABUS.PHP  **HOW CAN I WRITE AND UPLOAD TEST?** YOU CAN JUST WRITE TEST ON ANY OF YOUR NOTE BOOK AND CLICK PICS AND UPLOAD THEM.  **BENEFITS OF CA TEST SERIES?** - FREE NOTES, MORE THAN 2000 MCQ'S, DOUBT SOLVING SERVICES AND MUCH MORE.	- *Quality of papers, practice new questions also.* - *Practical suggestions + complete road map to improve* - *60% new questions different from ICAI mat* - *Topper sheets* - *Fast evaluations by former ICAI evaluator's* - *Doubt solving* - *Friendly calling service 24/7* - *Certified copies analysis* - *Concept notes, amendment notes, guidance notes* - *Practical questions* - *+2000 MCQ's available* - *Important questions of many more.*

"40% – 50% similar question came in ICAI exams from our test papers"

STUDENT RESPONSE AND TOPPER

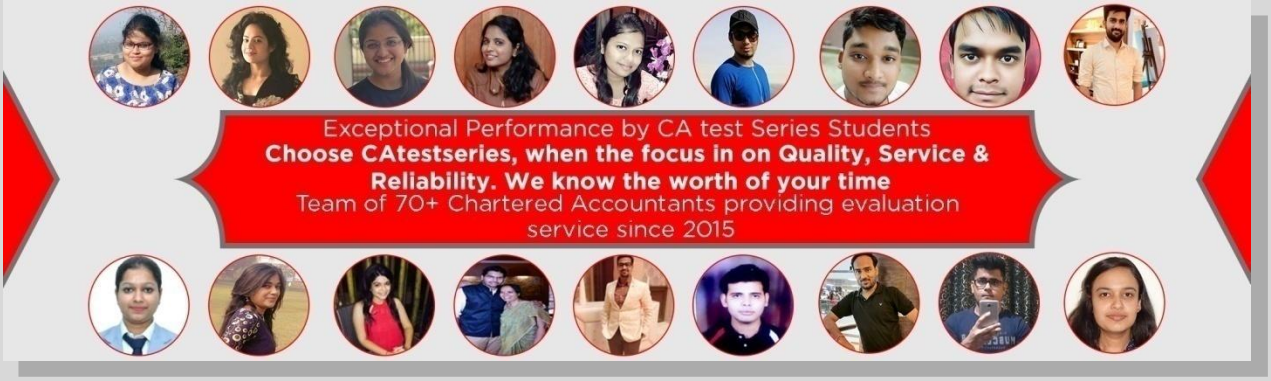


You will get to know where you have a lack of conceptual knowledge and needs to work. Comments on each answer will be given by the teacher so you can improve your performance.

Your doubts will be solving day by day. MTP's & RTP's will be given to do extra practice.

Certified copies will be checked here without any external charges.

TOPPER AND REVIEWS



Rahul Singla *"It was hard for me to think of what to do since it was my 3rd attempt of Inter but thanks to catestseries.org and their team who helped me through this test series. Now I am positive for my results"*

Sima Bansal *"I want to give a big thanks to catestseries.org. I had cleared my Ipcc 19 attempted. I have suggested all my friends about your test series and they are happy with their results."*

Vivek Pande *"My brother was old student of your website and he was the one who suggested me to join it. I had enough preparation But I was shocked when I saw where I had weak spots. Now I got passed with 37th rank is really makes me happy."*

3B INFORMATION SYSTEMS AUDITING

Q1. What is Information Systems auditing and explain its objectives?

Answer:

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:

a) **Asset Safeguarding Objectives:** The information system assets (hardware, software, data information etc.) must be protected by a system of internal controls from unauthorized access.

b) **Data Integrity Objectives:** The importance to maintain integrity of data of an organization requires all the time.

c) **System Effectiveness Objectives:** it is evaluated by auditing the characteristics and objective of the system to meet business and user requirements.

d) **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.

Q2. Explain the Need for Audit of Information Systems?

Answer:

a) **Organizational 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.

b) **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.

c) **Costs of Computer Abuse:** Unauthorized access to computer systems, malwares, unauthorized physical access to computer facilities and unauthorized copies of sensitive data can lead to destruction of assets (hardware, software, data, information etc.)

d) **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.

e) **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.

f) **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.

g) **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.

Q3. What is Audit Trail? Explain types and objectives of Audit Trail?

Answer:

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:

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

   ii. **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. Knowledge of the conditions that existed at the time of a system failure can be used to assign responsibility and to avoid similar situations in the future.

c) **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.

Q4. What is the role of auditor in Auditing Environmental Controls? What are the factors that should focused by Auditing Environmental Controls?

Answer:

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. Also, the auditor should determine if HVAC systems are properly maintained and if qualified persons do this.

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.

Q5. What is the role of Auditor in Auditing Physical Security Controls? What are the Physical Access Controls that should audit by Auditor?

Answer:

a) **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

b) **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:
   b) **Proximity to hazards**:
      i. The IS auditor should estimate the building's distance to natural and manmade 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.

c) **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.

d) **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.

e) **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.

f) **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.

g) **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;

Q6. Explain User Access Controls in Audit of Logical Access Controls?

Answer:

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:
    a) **Authentication:** The auditor should examine network and system resources to determine if they require authentication, or whether any resources can be accessed without authenticating.
    b) **Access violations:** The auditor should determine if systems, networks, and authentication mechanisms can log access violations. These usually exist in the form of system logs showing invalid login attempts
    c) **User account lockout:** The auditor should determine if systems and networks can automatically lock user accounts that are the target of attacks. A typical system configuration is one that will lock a user account after five unsuccessful logins attempts within a short period.
    d) **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.

e) **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.

f) **Shared accounts:** The IS auditor should determine if there are any shared user accounts; these are user accounts that are routinely (or even infrequently) used by more than one person. The principal risk with shared accounts is the inability to determine accountability for actions performed with the account.

g) **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:** Auditing password management requires attention to several key technologies and activities, including the following:

   Password standards: 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.

3. **Auditing User Access Provisioning:** Auditing the user access provisioning process requires attention to several key activities, including:

   a) **Access request processes:** The IS auditor should identify all user access request processes and determine if these processes are used consistently throughout the organization.

   b) **Access approvals:** The IS auditor needs to determine how requests are approved and by what authority they are approved.

   c) **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.

d) **Segregation of Duties (SOD):** The IS auditor should determine if the organization makes any effort to identify segregation of duties. This may include whether there are any SOD matrices in existence and if they are actively used to make user access request decisions.

e) **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.

4. **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. This examination should include understanding on how terminations are performed and how user account management personnel are notified of terminations.

   b) **Access reviews:** The IS auditor should determine if any internal reviews of terminated accounts are performed, which would indicate a pattern of concern for effectiveness in this important activity. 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 how contractor access and termination is managed and if such management is effective.

Q7. Explain User Access Logs in Audit of Logical Access Controls?

Answer:

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.

a) **Centralized access logs:** The IS auditor should determine if the organization's access logs are aggregated or if they are stored on individual systems.
b) **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.
c) **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, which performs them, how issues requiring attention are identified, and what actions are taken when necessary.
d) **Access log retention:** The IS auditor should determine how long access logs are retained by the organization and if they are back up.

Q8. What is Job Title? How Job Title helps organizations in different ways?

Answer:

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 Base lining:** 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.

Q9. Explain different job titles in General Operations

Answer:

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

a) **Operations Manager:** responsible for overall operations that are carried out by others. Responsibilities will include establishing operations shift schedules.

b) **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.

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

d) **Systems Operator:** responsible for monitoring systems and networks, performing backup tasks, running batch jobs, printing reports, and other operational tasks.

e) **Data Entry:** responsible for keying batches of data from hard copy sources.

f) **Media Librarian:** responsible for maintaining and tracking the use and whereabouts of backup tapes and other media.

Q10. Explain about SEGREGATION OF DUTIES? Explain Some Examples of Segregation of Duties Controls?

Answer:

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

a) **Transaction Authorization**: Information systems can be programmed or configured to require two (or more) persons to approve certain transactions. Many of us see this in retail establishments where a manager is required to approve a large transaction or a refund.

b) **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.

c) **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.

d) **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.

e) **Reduce access privileges:** Management can reduce individual user privileges so that the conflict no longer exists.

f) **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.

Q11. Explain the Application Areas of Computer Based Applications?

Answer:

Major areas of computer based applications are:

1. **Finance and Accounting:** The main goal of this subsystem (considering Business functions as whole system) is to ensure the financial viability of the organization, enforce financial discipline and plan and monitor the financial budget.
2. **Marketing and Sales:**
    a) The objective of this subsystem is to maximize the sales and ensure customer satisfaction.
    b) The marketing system facilitates the chances of order procurement by marketing the products of the company, creating new customers and advertising the products.
    c) The sales department may use an order processing system to keep the status and track of orders, generate bills for the orders executed and delivered to the customer.
3. **Production or Manufacturing:**
    a) The objective of this subsystem is to optimally deploy man, machine and material to maximize production or service.
    b) The system generates production schedules and schedules of material requirements, monitors the product quality, plans for replacement or overhauling the machinery and helps in overhead cost control and waste control.
4. **Inventory /Stores Management:**
    a) The inventory management system is designed with a view to keeping the track of materials in the stores.
    b) The system is used to regulate the maximum and minimum level of stocks, raise alarm at danger level stock of any material, give timely alert for re-ordering of materials, identification of important items in terms stock value (ABC analysis), identification most frequently moving items (XYZ analysis) etc.
5. **Human Resource Management:**
    a) Effective and efficient utilization of manpower in a dispute-free environment in this key functional area ensures to facilitate disruption free and timely services in business.

b) Human Resource Management System (HRMS) aims to achieve this goal. Skill database maintained in HRM system, with details of qualifications, training, experience, interests etc.

c) Helps management for allocating manpower to right activity at the time of need or starting a new project. This system also keeps track of employees' output or efficiency.