3. INFORMATION SYSTEMS RISKS & CONTROLS

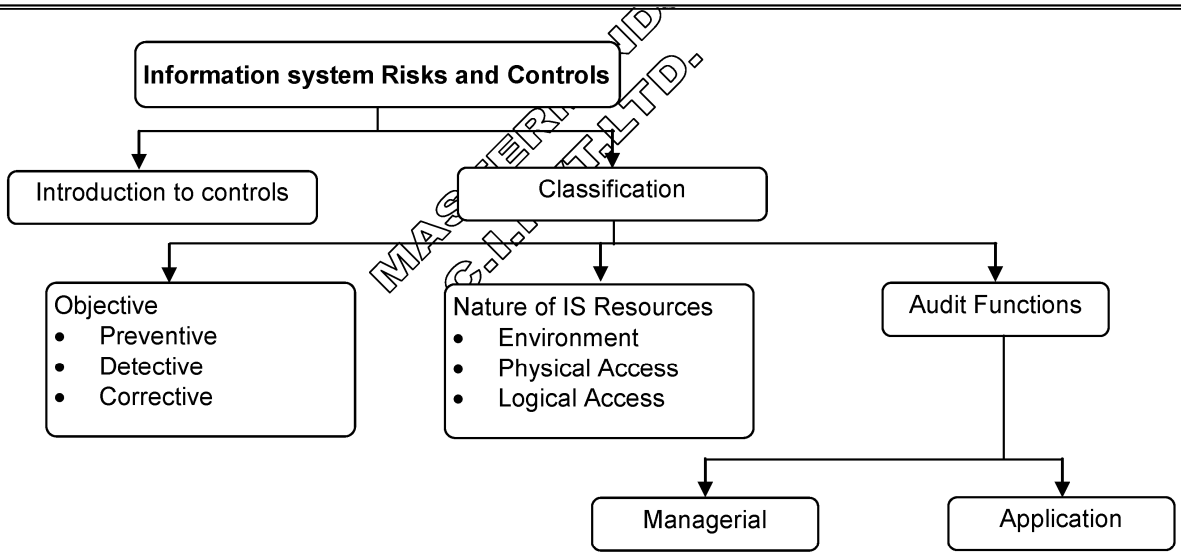
QUESTION WISE ANALYSIS OF PREVIOUS EXAMINATIONS

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																		
5.	-	-	-	-	-	-	-	-	-	-	4	-	-	-	-	-	-	-
13.	-	-	-	-	-	-	4	-	-	-	-	-	-	-	-	-	-	-

CHAPTER OVERVIEW

SECTION	TOPIC	STARTING PAGE NO.
1.	THEORY FOR CLASSROOM DISCUSSION	3.1

SECTION 1: THEORY FOR CLASSROOM DISCUSSION



PART 1: INTRODUCTION TO CONTROLS

Q.No.1. What is the basic purpose of Information system controls and how the purpose is achieved? **(B)**

1) The basic purpose of information system controls in an organization is to ensure that the business objectives are achieved and undesired risk events are prevented, detected and corrected.

2) This is achieved by designing and effective information control framework, which comprise policies, procedures, practices, and organization structure that gives reasonable assurances that the business objectives will be achieved.

SIMILAR QUESTION:

1. It is necessary for an organization to identify the nature of possible threats to its information systems and establish a set of measures to neutralize those threats how can an organization deal with the threats and achieve business objectives?

A The organization can neutralize threats using internal controls Refer above answer.

Q.No.2. What is Control? Explain the Need for Controls in Information Systems? (B) (For Academic interest)

CONTROL: Controls are defined as policies, procedures, practices, and organization structure ensure that the business objectives are achieved and undesired risk events are prevented, detected and corrected.

NEED FOR CONTROLS: Today's dynamic global enterprises need information integrity, reliability and validity for timely flow of accurate information throughout the organization.

a) Safeguarding assets to maintain data integrity to achieve system effectiveness and efficiency is a significant control process.

b) A well designed information system should have controls built-in for all its sensitive or critical sections.

Q.No.3. what are some of the critical controls lacking in a computerized environment? (C)

SOME OF THE CRITICAL CONTROLS LACKING IN A COMPUTERIZED ENVIRONMENT ARE AS FOLLOWS:

1) Lack of management understanding of IS risks and related controls;

2) Absence or inadequate IS control framework;

3) Absence of weak general controls and IS controls;

4) Lack of awareness and knowledge of IS risks and controls amongst the business users and even IT staff;

5) Complexity of implementation of controls in distributed computing environments and extended enterprises;

6) Lack of control features or their implementation in highly technology driven environments; and

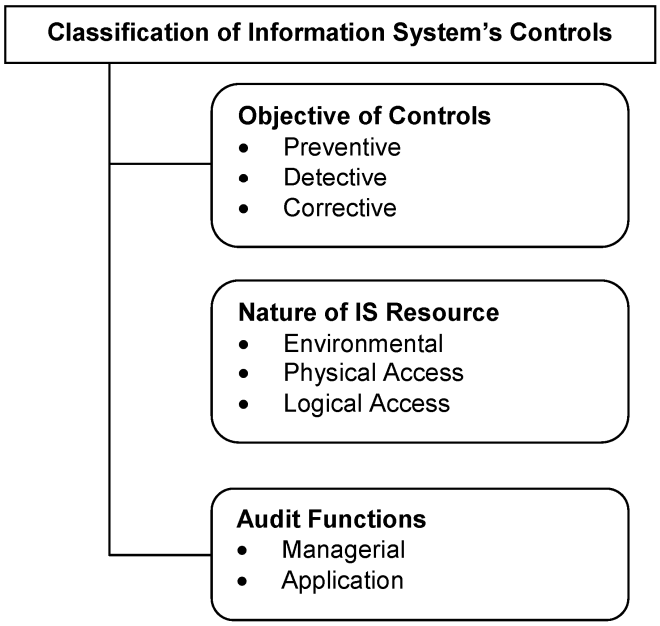
7) Inappropriate technology implementations or inadequate security functionality in technologies implemented.

SIMILAR QUESTION:

1. **Weaknesses in the IT environment at the entity level, or in the general or application controls at the process level, may result in a conclusion that there is a significant deficiency or material weakness which is a serious consideration for the management. As a IS specialist List out some instances exposing lack of critical controls in a computerized environment.**

A. Refer above answer

PART 2: CLASSIFICATION OF INFORMATION SYSTEMS CONTROLS



Q.No.4. Explain the Classification of controls based on "Objective of Controls"?
(A) (RTP N-18) (MTP N20) (MTP J20)

THE CLASSIFICATION BASED ON "OBJECTIVE OF CONTROLS" ARE:

1) **PREVENTIVE CONTROLS:** Preventive Controls are those inputs, which are designed to prevent an error, omission or malicious act occurring. Any control can be implemented in both manual and computerized environment.

Purpose	Manual Control	Computerized Control
Restrict unauthorized entry into the premises.	Build a gate and post a security guard.	Use access control software, smart card, biometrics, etc.
Restricted unauthorized entry into the software applications.	Keep the computer in a secured location and allow only authorized person to use the applications.	Use access control, viz. User ID, password, smart card, etc.

Some of the examples of Preventive Controls are:

a) Employ qualified personnel

b) Segregation of duties

c) Access control

d) User instruction manuals.

e) Firewalls, Passwords.

2) **DETECTIVE CONTROLS:** These controls are designed to detect errors, omissions or malicious acts that occur and report the occurrence. In other words, Detective Controls detect errors or incidents that escape from preventive controls. *For example, a detective control may identify account numbers of inactive accounts or accounts that have been monitoring for suspicious activities.*

Some of the examples of Detective Controls are as follows:

a) Review of payroll reports;

b) Compare transactions on reports to source documents;

c) Monitor actual expenditures against budget;

d) Hash totals;

e) Check points in production jobs

CHARACTERISTICS OF DETECTIVE CONTROLS:

1) Clear understanding of lawful activities so that anything which deviates from these is reported as unlawful, malicious, etc.

2) An established mechanism to report unlawful activities to the appropriate person or group.

3) Interaction with the preventive control to prevent unlawful and malicious acts from occurring.

4) Surprise checks by supervisor.

3) **CORRECTIVE CONTROLS:** These controls are used to correct errors, omissions, or incidents once they have been detected. They vary from simple correction of data-entry errors to recovery from incidents, disruptions, or disasters. **(MTP-M20)**

SOME OF THE EXAMPLES OF CORRECTIVE CONTROLS ARE:

a) Submitting corrective journal entries after discovering an error;

b) A Business Continuity Plan (BCP);

c) Contingency planning;

d) Investigate budget variance and report violations.

CHARACTERISTICS OF THE CORRECTIVE CONTROLS:

a) Minimizing the impact of the threat

b) Identifying the cause of the problem

c) Providing Remedy to the problems discovered by detective controls

d) Getting feedback from preventive and detective controls

e) Correcting error arising from a problem

f) Modifying the processing systems to minimize future occurrences of the incidents.

SIMILAR QUESTIONS:

1. **The primary purpose of internal controls is to help safeguard an organization and further its objectives. Internal controls function to minimize risks and protect assets, ensure accuracy of records, promote operational efficiency, and encourage adherence to policies, rules, regulations, and laws. As a control designer how do you classify the controls basing on their functions for better achievement of the organizational objectives?**

A. Refer above answer

PART 3: ENVIRONMENTAL CONTROLS

Q.No.5. What are environment controls? Explain about Fire Damage controls in Environmental Controls? (B) (RTP M18)

(OR)

Physical security mechanisms in an organization provides protection to people, data, equipment, systems, facilities and company assets. Determine some major ways of protecting the organization's computer installation in the event of any explosion or fire. (N18-4M)

ENVIRONMENTAL CONTROLS: These controls related to IT environment such as power, air-conditioning, Uninterrupted Power Supply (UPS), smoke detection, fire-extinguishers, dehumidifiers etc.

FIRE: It is a major threat to the physical security of a computer installation.

CONTROLS FOR FIRE DAMAGE:

1) Some of the major ways of protecting the installation against fire damage are as follows:
   - **a)** Both automatic and manual fire alarms may be placed at strategic locations.
   - **b)** Manual fire extinguishers can be placed at strategic locations.
   - **c)** Fireproof Walls, Floors and Ceilings surrounding the Computer Room and Fire Resistant Office Materials should be used.
   - **d)** Fire exits should be clearly marked.
2) **Documented and Tested Emergency Evacuation Plans:** Relocation plans should focus on human safety, but should not leave information processing facilities physically unsecured.
3) **Smoke Detectors:** Smoke detectors are positioned at places above and below the ceiling tiles. Smoke detectors should produce an audible alarm and must be linked to a monitored station (for example, a fire station).
4) **Wiring Placed in Electrical Panels and Conduit:** To reduce the risk of fire occurring and spreading, wiring should be placed in the fire-resistant panels and conduit.

SIMILAR QUESTION:

1. **Fire is a major threat to the physical security of a computer installation and also to human safety. As a IS security expert suggest some control mechanisms to physically protect the IS setup.**

A. Refer above answer

Q.No.6. Write about electrical Exposures? What controls are required for electrical exposures? (B)

ELECTRICAL EXPOSURES: These include risk of damages that may be caused due to electrical faults.

Ex., non-availability of electricity, spikes (temporary very high voltages), fluctuations of voltage and other such risks.

CONTROLS FOR ELECTRICAL EXPOSURE:

1) **Power Spikes:** The risk of damage due to power spikes can be reduced using Electrical Surge Protectors that are typically(=normally)built into the Un-interruptible Power System (UPS).

2) **Un-interruptible Power System (UPS)/ Generator:** In case of a power failure, the UPS provides backup electrical power from the battery to the computer for a certain span of time.

3) **Voltage regulators and circuit breakers** protect the computer systems from temporary increase or decrease of power.

4) **Emergency Power-Off Switch:** When the need arises for an immediate power shut down during situations like a computer room fire or an emergency evacuation, an emergency power-off switch at the appropriate locations would serve the purpose and should be easily accessible and yet secured from unauthorized people.

SIMILAR QUESTION:

1. **Electrical systems are the foundation of data-center operations. The very nature of these business-critical facilities makes them potential danger zones for those involved in building, maintaining, and modifying them. Working around data-center power systems can be dangerous due to their complexity, including redundant circuitry and uninterruptible power supplies (UPS) that can switch without warning in just a few milliseconds. The preceding discussion stresses the importance of controls over electrical exposures. In your observation what care should be taken to protect your IS facility from electrical exposures?**

A. **Refer above answer.**

Q.No.7. What causes water damage to a computer installation? What controls are required are required for water damage? (C)

1) **WATER DAMAGE:** Water damage to a computer installation can be the outcome of water pipes burst, Water damage may also result from other resources such as cyclones, tornadoes, floods etc.

2) **CONTROLS FOR WATER DAMAGE:**

   a) Wherever possible have waterproof ceilings, walls and floors.

   b) Ensure an adequate positive drainage system exists.

   c) Install alarms at strategic points within computer installation.

   d) In flood areas have the installation above the upper floors but not at the top floor.

SIMILAR QUESTIONS:

1. **Water leak detection is commonly installed in data centers, communications rooms and other information technology dependent structures. Leaking water from HVAC, AC units, water pipes, drainage or even ground water can cause significant disruption. What control measures do you suggest to prevent water damage?**

A. **Refer above answer**

Q.No.8. Explain the controls for Pollution Damage and other issues in Environmental Controls? (C)

1) **POLLUTION DAMAGE AND OTHERS:**

   a) The major pollutant in a computer installation is dust. Dust may cause either permanent damage or temporary failure.

   b) Dust caught between the surfaces of magnetic disk and the read write heads may cause permanent damage to data or read/ write errors.

2) **CONTROLS FOR POLLUTION DAMAGE EXPOSURE:**

   a) Power Leads from Two Substations:

      i) Electrical power lines may be exposed to many environmental dangers such as water, fire, lightning, cutting due to careless digging etc.

      ii) To avoid these types of events, additional power links should be maintained. Interruption of one power supply does not adversely affect electrical supply.

b) **Prohibition against Eating, Drinking and Smoking within the Information Processing Facility:** These activities should be prohibited from the information processing facility. This prohibition should be clear, e.g. a sign on the entry door and wall.

PART 4: PHYSICAL ACCESS CONTROLS

Q.No.9. What are physical Exposures? What are the different physical access controls helpful to restrict physical exposures? (B) (MTP1-N18)

PHYSICAL EXPOSURES: Includes abuse of data processing resources, Blackmail, Embezzlement(=Misappropriation), Damage, vandalism (=destruction) or theft to equipment or documents, Public disclosure of sensitive information and Unauthorized entry.

Physical Access Controls: These controls relate to physical security of the tangible IS resources (servers, computers, hard disks) and intangible resources like data stored on physical media like hard disk etc. Such controls include Access control doors, Security guards, door alarms, restricted entry to secure areas, visitor logged access, CCTV monitoring etc.

CONTROLS FOR PHYSICAL EXPOSURES:

1) **LOCKS ON DOORS:**

a) **Cipher locks (Combination Door Locks):** Cipher locks are used in low security situations. To enter, a person presses a four-digit number, and the door will unlock for a predetermined period, usually ten to thirty seconds.

b) **Bolting Door Locks:** A special metal key is used to unlock the door in bolting door lock system. To avoid illegal entry, the keys should not be duplicated.

c) **Electronic Door Locks:** A magnetic or embedded chip-based plastic card key or token may be entered in to a reader to gain access in these systems.

2) **PHYSICAL IDENTIFICATION MEDIUM:**

a) **Personal Identification Numbers (PIN):** A secret PIN number will be assigned to the visitor. The visitor has to log on by inserting a card in some device and then enter their PIN for authentication.

b) **Plastic Cards:** These cards are used for identification purposes. Customers should safeguard their card so that it does not fall into unauthorized hands. EX: ID cards.

c) **Identification Badges:** Special identification badges can be issued to personnel as well as visitors. Color codes can be used for easy identification.

3) **LOGGING ON FACILITIES:**

a) **Manual Logging:**

i) All visitors should sign in a visitor's log book indicating their name, their purpose of visit, and person to see.

ii) Logging may happen at both fronts - reception and entrance to the computer room.

iii) A valid identification such as a driver's license, business card may be asked before allowing entry inside the company.

b) **Electronic Logging:**

i) This feature is a combination of electronic and biometric security systems.

ii) The users logging can be monitored and the unsuccessful attempts being highlighted.

SIMILAR QUESTION:

1. **Work on physical security mainly focuses on the physical protection of information, buildings, personnel, installations, and other material resources. Additionally, physical security covers issues related to processes prior criminal activities, espionage, and terrorism. AS a security expert what are your insights towards Physical security mechanisms in an IS facility?**

A. **Refer above answer**

Q.No.10. Explain various other important means of controlling physical access? (B) (MTP 1-18)

OTHER MEANS OF CONTROLLING PHYSICAL ACCESS: Other important means of controlling physical access are given as follows:

1) **VIDEO CAMERAS:** Cameras should be placed at specific locations and monitored by security guards. Recordings should be retained for future use.
2) **SECURITY GUARDS:** Extra security can be provided by appointing guards for CCTV monitoring. Guards supplied by an external agency should be made to sign a bond to protect the organization from loss.
3) **CONTROLLED VISITOR ACCESS:** A responsible employee should escort all visitors. Visitors may be friends, maintenance personnel, computer vendors, consultants and external auditors.
4) **BONDED PERSONNEL:** All service contract personnel, such as cleaning people, offsite storage services should be asked to sign a bond.
5) **DEAD MAN DOORS:** This systems consist a pair of doors that are typically found at entry points of computer rooms and document stations. The first entry door must close and lock, for the second door to operate, with only one person permitted in the holding area.
6) **NON-EXPOSURE OF SENSITIVE FACILITIES**: here should not be any indications about presence of windows, directional signs, etc. Only the general location of the computer facility should be identifiable.
7) **COMPUTER TERMINAL LOCKS:** These locks ensure that no unauthorized user turn on the computer.
8) **CONTROLLED SINGLE ENTRY POINT:** A controlled entry point is monitored by a receptionist. Unnecessary or unused entry points should be eliminated or deadlocked.
9) ***ALARM SYSTEM:*** *Illegal entry can be avoided by linking alarm system to inactive entry point and the reverse flows of enter or exit only doors to avoid illegal entry.*
10) ***PERIMETER FENCING:*** *Fencing at boundary of the facility may also enhance the security mechanism.*
11) ***CONTROL OF OUT OF HOURS OF EMPLOYEE-EMPLOYEES:*** *Employees who are out of office for a longer duration during the office hours should be monitored carefully. Their movements must be noted and reported to the concerned officials frequently.*
12) ***SECURED REPORT / DOCUMENT DISTRIBUTION CART:*** *Secured carts, such as mail carts, must be covered and locked and should always be attended.*

SIMILAR QUESTIONS:

1. **The physical security of a Data Center is the set of protocols that prevent any kind of physical damage to the systems that store the organization's critical data. The selected security controls should be able to handle everything ranging from natural disasters to corporate espionage to terrorist attacks. In addition to locks, Physical identification medium and logging facilities what are the other additional techniques to restrict physical access?**

A. Refer above answer

PART 5: LOGICAL ACCESS CONTROLS

Q.No.11. Write about logical access controls (B) (MTP2-N18)

LOGICAL ACCESS CONTROLS:

1) These controls are related to logical access to information resources such as operating systems controls, application software boundary controls, networking controls, access to database objects, encryption controls etc.
2) Logical access controls are implemented to ensure that access to systems, data and programs is restricted to authorized users in order to safeguard information against unauthorized use, disclosure or modification, damage or loss.

3) The key factors considered in designing logical access controls include confidentiality and privacy requirements, authorization, authentication etc., for monitoring compliance, intrusion testing and reporting.

4) Logical access controls are the system-based mechanisms used to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted.

SIMILAR QUESTION:

1. **Businesses have often prioritized physical security. However, while this is an important part of protecting an enterprise's infrastructure, it's just one piece of what should be a comprehensive security apparatus—especially as businesses need next-generation cyber security strategies to protect proprietary information and secure their networks. This is where logical security controls come in. As an IS specialist can you make us understand the implication of logical access controls in information security.**

A. Refer above answer

Q.No.12. Explain the Technical Exposures in Logical Access Controls? (A)

TECHNICAL EXPOSURES: Technical exposures include unauthorized implementation or modification of data and software.

Technical exposures include the following.

1) **DATA DIDDLING (=to cheat):** This involves the change of data before or after it entered the system. A limited technical knowledge is required to data diddle and it occurs before computer security can protect the data.

2) **BOMB:** Bomb is a piece of bad code intentionally inserted by an insider or the supplier of a program. It is triggered by a logical event or it can be time based. It explodes when the required conditions are met. However, these programs cannot infect other programs.

3) **CHRISTMAS CARD:** It is a well-known example of Trojan (It is a type of malicious software developed by hackers to disguise as legitimate software to gain access to target users' systems) and was detected on internal E-mail of IBM system. On typing the word 'Christmas', it will draw the Christmas tree as expected, but in addition, it will send copies of similar Christmas tree to all other computers connected to the network. Because of this message on other computers, users cannot save their half-finished work.

4) **WORM:** A worm does not require a host program like a Trojan to relocate itself. Since, worms are stand-alone programs; they can be detected easily in comparison to computer viruses or trojans.

5) **ROUNDING DOWN:** This refers to rounding of small fractions of amount and transferring these small fractions into an authorized account. As the amount is small, it gets rarely noticed.

6) **SALAMI TECHNIQUES:** This involves slicing of small amounts of money from a computerized transaction or account. A Salami technique is slightly different from a rounding technique in the sense a fixed amount is deducted.

7) **TRAP DOORS:** Trap doors allow insertion of specific logic such as program interrupts that permit review of data. They also perform insertion of unauthorized logic.

8) **SPOOFING:** A spoofing attack involves forging (=falsifying/faking) one's source address. One machine is used to impersonate (=imitate/mimic) the other in spoofing technique. Spoofing occurs only after a particular machine has been identified as vulnerable (=susceptible/weak).

SIMILAR QUESTION:

1. **In order to protect your IS you need to know about the different ways in which your IS can be compromised and privacy infringed. Logical access threats happen when the perpetrators hack into the systems of the companies in question. Most businesses store their sensitive information on servers and the data may or may not be financial in nature. Hackers who can gain access into the systems of these companies get access to all the information available in these files. In this context write about the most common technical exposures due to lack of efficient logical access controls.**

A. Refer above answer

Q.No.13. What are Asynchronous attacks? Explain various forms of asynchronous attacks? (A)(OLD PM, RTP-N16, RTP-N14, MTP2-M16, MTP N-18) (M17-4M)

ASYNCHRONOUS ATTACKS:

1) They occur in many environments where data can be moved asynchronously(=irregular timings)across telecommunication lines.
2) Data that is waiting to be transmitted are liable to asynchronous attack. These attacks are hard to detect because they are usually very small pin like insertions.
3) There are many forms of **asynchronous attacks.**
   a) **Data Leakage:** Data leakage involves leaking information out of the computer by dumping files to paper or stealing computer reports and tape.
   b) **Subversive Attacks:** These can provide intruders with important information about messages being transmitted and the intruder may attempt to violate the integrity of some components in the sub-system.
   c) **Wire-tapping:** This involves spying on information being transmitted over telecommunication network.
   d) **Piggybacking:**
      i) This is the act of electronically attaching to an authorized telecommunication link that intercepts (=interrupt) and alters transmissions.
      ii) This involves intercepting communication between the operating system and the user and modifying them or substituting them with new messages.

SIMILAR QUESTION:

1. **These attacks typically targets timing. The objective is to exploit the delay between the time of check (TOC) and the time of use (TOU). These attacks are sometimes called *race conditions* because the attacker races to make a change to the object after it has been changed but before the system uses it. What type of attacks we are talking about and what are its different forms?**

A. **Refer above answer**

Q.No.14. Who are Logical Access Violators? What are their types? (B)

LOGICAL ACCESS VIOLATORS are often (=frequently): The same people who exploit physical exposures, although the skills needed to exploit logical exposures are more technical and complex.
They are mainly as follows:

1) **HACKERS:** Hackers try their best to overcome restrictions to prove their ability. Ethical hackers most likely never try to misuse the computer intentionally;
2) **EMPLOYEES** (authorised or unauthorized);
3) **IS PERSONNEL:** They have easiest access to computerized information since they come across information while discharging their duties. Segregation of duties and supervision help to reduce the logical access violations;
4) **FORMER EMPLOYEES:** should be cautious of former employees who have left the organisation on unfavorable terms.
5) **END USERS:** Generally end users consists of Interested or Educated Outsiders, Competitors, Foreigners, Organized Criminals, Crackers, Part - time and Temporary Personnel, Vendors and consultants and Accidental Ignorant Violation done unknowingly by the end users.

SIMILAR QUESTION:

1. **Auditing logical access area may seem intuitive for IT auditors but its importance can never be over emphasized, with latest security threats and Cyber Security attacks it is common that a successful cyber-attack may lead to a hacker gaining unauthorized access to critical system and data and allows them to alter or compromise the system/data. Apart from hackers there are other people who violate the logical access controls, make a list of people who can take the chance of access violation.**

A. **Refer answer above**

Q.No.15. Explain User Access Management and User Responsibilities in Logical Access Controls?
(B) MTP N-18

1) **USER ACCESS MANAGEMENT:** This is an important factor that involves following:
   a) **User Registration:** Information about every user is documented. The de-registration process is also equally important
   b) **Privilege management:** Access privileges are to be aligned with job requirements and responsibilities and are to be minimal w.r.t their job functions.
   c) **User password management:** Allocations, storage, cancellation, and reissue of password are password management functions. Educating users is a critical component about passwords, and making them responsible for their password
   d) **Review of user access rights:** Periodic review of access rights to check anomalies in the user's current job profile, and the privileges granted earlier.
2) **USER RESPONSIBILITIES:** User awareness and responsibility are also important factors and are as follows:
   a) **Password use:** Mandatory use of strong passwords to maintain confidentiality.
   b) **Unattended user equipment:** Users should ensure that none of the equipment under their responsibility is ever left unprotected.

SIMILAR QUESTION:

1. **Identity and access management (IAM) is the security discipline that enables the right individuals to access the right resources at the right times for the right reasons and then over time being able to prove it. The risk of not having a robust IAM system may lead to severe consequences, some of which include loss of data confidentiality, integrity, and even availability. This can inflict irreparable harm to organization's reputation, loss of investor confidence, financial penalties imposed by regulators, and in some cases, organization's inability to continue operating.AS an IS auditor what measures do you adopt for Identity and access management of users.**

A. **Refer answer above.**

Q.No.16. Explain Network Access Control in Logical Access Controls?
(Or) (A) (RTP-N19)N(19),MTP1M(18)
An Internet connection exposes an organization to the harmful elements of the outside world. As an EDP (Electronic Data Processing) operator of an organization ABC, prepare a checklist for Network Access Controls that are required to be implemented in the organization.
(MTP-N18)

NETWORK ACCESS CONTROL: An Internet connection exposes an organization to the harmful elements of the outside world. The protection can be achieved through the following means:

1) **POLICY ON USE OF NETWORK SERVICES:** The first step is to have an enterprise wide policy applicable to internet service requirements aligned with the business needs.
2) **ENFORCED PATH:** Based on risk assessment, it is necessary to specify the exact path or route connecting the networks. e.g. internet access by employees will be routed through a firewall and proxy.
3) **SEGREGATION OF NETWORKS:** Based on the sensitive information handling function, network is separated from the internet usage service; e.g. VPN connection between a branch office and the head-office, this VPN is to be isolated from the internet usage service
4) **NETWORK CONNECTION AND ROUTING CONTROL:** The traffic between networks should be restricted, based on identification of source and authentication access policies.
5) **SECURITY OF NETWORK SERVICES:** The techniques of authentication and authorization policy should be implemented across the organization's network.
6) **FIREWALL:** A Firewall is a system that enforces access control between two networks. All traffic between the external network and the organization's Intranet (=private network) must pass through the firewall.

7) **ENCRYPTION:** Encryption is the conversion of data into a secret code for storage in databases and transmission over networks.

8) **CALL BACK DEVICES:** The call- back device requires the user to enter a password and then the system breaks the connection. If the caller is authorized, the call back device dials the caller's number to establish a new connection.

SIMILAR QUESTION:

1. **Network Access Controls helps enterprises implement policies for controlling devices and user access to their networks it is the act of keeping unauthorized users and devices out of a private network. Organizations that give certain devices or users from outside of the organization occasional access to the network can use network access controls to ensure that these devices meet corporate security compliance regulations. In this context list out the elements of network access controls strategy of an IS.**

A. **Refer above answer.**

Q.No.17. Explain Operating System Access Control in Logical Access Controls?
(OR) (A) RTP M(20),N (18),MTP1 M(18)
Operating System security involves policy, procedure and controls that determine, 'who can access the operating system,' 'which resources they can access', and 'what action they can take'. As an Information Systems auditor, determine the key areas which shall be put in place by any organisation.

Protecting operating system access is extremely crucial and can be achieved using following steps.

1) **AUTOMATED TERMINAL IDENTIFICATION:** This will help to ensure that a specified session could only be initiated from a certain location or computer terminal.

2) **TERMINAL LOG-IN PROCEDURES:** A log-in procedure is the first line of defense against unauthorized access

   When the user initiates the log-on process by entering user-id and password, the system compares the ID and password to a database of valid users and accordingly authorizes the log-in.

3) **ACCESS TOKEN:** If the log on attempt is successful, the Operating System creates an access token that contains key information about the user including user-id, password, user group and privileges granted to the user. The information in the access token is used to approve all actions attempted by the user during the session

4) **ACCESS CONTROL LIST:** This list contains information that defines the access privileges for all valid users of the resource. When a user attempts to access a resource, the system compares his or her user-id and privileges with that of the access token. If there is a match, the user is granted access.

5) **DISCRETIONARY ACCESS CONTROL:** The system administrator usually determines who is granted access to specific resources and maintains the access control list.

6) **USER IDENTIFICATION AND AUTHENTICATION:** The users must be identified and authenticated in a fool proof manner. Depending on risk assessment, more strict method like Biometric Authentication or Cryptographic means like Digital Certificates should be employed.

7) **PASSWORD MANAGEMENT SYSTEM:** An operating system could enforce selection of good passwords. Internal storage of password should use one way hashing algorithms and the password file should not be accessible to users.

8) ***USE OF SYSTEM UTILITIES:*** *System utilities are the programs that help to manage critical functions of the operating system e.g. addition or deletion of users.*

9) ***DURESS(=PRESSURE/THREAT) ALARM TO SAFEGUARD USERS:*** *If users are forced to execute some instruction under threat, the system should provide a means to alert the authorities.*

10) ***TERMINAL TIME OUT:*** *Log out the user if the terminal is inactive for a defined period. This will prevent misuse in absence of the legitimate user.*

11) ***LIMITATION OF CONNECTION TIME:*** *Define the available time slot. Do not allow any transaction beyond this time.*

SIMILAR QUESTION:

1. **Securing operating systems is the first step towards safeguarding the IS Applications deployment from intrusion. Workstations and servers are typically installed with a multitude of development tools and utilities which needs lots of attention and care. This process also requires that all appropriate security features are activated and configured correctly to restrict unauthorized access in to the system. As an IS auditor explore the mechanism followed to achieve OS Access security in IS.**

A. Refer above answer.

Q.No.18. Explain Application and Monitoring System Access Control in logical controls? (C)

1) **INFORMATION ACCESS RESTRICTION:** A user can access only to those items, s/he is authorized to access. Controls are implemented on the access rights of users.
2) **SENSITIVE SYSTEM ISOLATION:** Based on the importance of a system in an enterprise, it may even be necessary to run the system in an isolated environment. This control will detect and report any unauthorized activities.
3) **EVENT LOGGING:** All incoming and outgoing requests along with attempted access should be recorded in a transaction log.
4) **MONITOR SYSTEM USE:** Based on the risk assessment, a constant monitoring of some critical systems is essential. *Define the details of types of accesses, operations, events and alerts that will be monitored.*
5) **CLOCK SYNCHRONIZATION:** Event logs maintained across an enterprise network plays a significant role in correlating an error and generating report on it. Hence, the need for maintaining the same clock time across the network as per a standard time is mandatory.

SIMILAR QUESTION:

1. **Any security policy must maintain a record of system activity to ensure that users are held accountable for their actions. Auditing helps deter unauthorized user behavior that may not otherwise be prevented. It is particularly useful to ensure that authorized system users do not abuse their privileges. Then what control mechanisms are required to restrict people from accessing application and monitoring systems in an information system?**

A. Refer above answer.

Q.No.19. What kind of logical controls are to be put in place when mobile computing is adopted by the organizations? (C)

CONTROLS WHEN MOBILE COMPUTING IS ADOPTED BY THE ORGANIZATION:

1) In today's organizations, computing facility is not restricted to a certain data center alone.
2) Ease of access on the move provides efficiency and results in additional responsibility on the management to maintain information security.
3) Theft of data carried on the disk drives of portable computers is a high-risk factor. Both physical and logical access to these systems is critical.
4) Information is to be encrypted and access identifications like fingerprint, eye-iris, and smart cards are necessary security features

Similar question:

1. **Mobile technologies are increasingly finding a place in a multitude of organizational settings .when mobile computing is adopted by the organization the lack of encrypted communication can allow malware to access the network and propagate Trojans and viruses throughout the organization. As an IS expert what control measures do you suggest to organizations adopting mobile computing technologies?**

A. Refer above answer.

PART 6: MANAGERIAL CONTROLS.

Q.No.20. What are Managerial Controls? Explain Top Management and Information Systems Management Controls in Managerial Controls? (B)(RTP-N19)

MANAGERIAL CONTROLS: The managerial controls should ensure the development, implementation,

operation and maintenance of information systems in a planned and controlled manner in an organization. The controls at this level provide a stable infrastructure in which IS can be built, operated, and maintained on a day-to-day basis.

TOP MANAGEMENT AND INFORMATION SYSTEMS MANAGEMENT CONTROLS: Top management is responsible for preparing a master plan for the information systems function. The senior managers who take responsibility for IS function in an organization face many challenges.

1) **THE MAJOR FUNCTIONS THAT A SENIOR MANAGER MUST PERFORM ARE AS FOLLOWS:**
   a) **PLANNING:** Involves determining the goals of the information systems and means to achieve these goals. The steering committee should assume overall responsibility for the activities of the information systems function.
   b) **ORGANIZING:** There should be a prescribed IT organizational structure with documented roles and responsibilities and agreed job descriptions. This includes gathering, allocating, and coordinating the resources needed to accomplish the goals that are established during planning function.
   c) **LEADING:** Motivating, guiding, and communicating with personnel.
   d) **CONTROLLING:** This includes comparing actual performance with planned performance as a basis for taking any corrective actions that are needed. This involves determining when the actual activities of the information system's functions deviate from the planned activities.

SIMILAR QUESTIONS:

1. **Top Management Controls determine how effectively the senior management manages the IS functions in an organization. The senior managers who take responsibility for IS function in an organization face many challenges. In this context what functions are to be carried out by the top level management in the development, implementation, operation and maintenance of information systems?**

A. **Refer above answer**

2. **Mr. X is an auditor of the company and plays a vital role in evaluating the performance of various controls under managerial controls. The top management is the one who takes responsibility for Information Systems function. Explain the functions that a senior manager must perform in organizing and controlling functions.**

A. **Write Organizing And Controlling Points In The Above Answer.**

Q.No.21. Explain Systems Development Management Controls in Managerial Controls? (B) (MTPJ20) (MTPN20) (RTPN18)

Systems Development Management has responsibility for the functions concerned with analyzing, designing, building, implementing, and maintaining information systems. System development controls are targeted to ensure that proper documentations and authorizations are available for each phase of the system development process.

The six activities discussed below deal with system development controls in IT setup.

1) **SYSTEM AUTHORIZATION ACTIVITIES:** All systems must be properly and formally authorized to ensure their economic justification and feasibility.
2) **USER SPECIFICATION ACTIVITIES:** Users must be actively involved in the systems development process wherein a detailed written descriptive document of the logical needs of the users is created.
3) **TECHNICAL DESIGN ACTIVITIES:** The technical design activities translate the user specifications into a set of detailed technical specifications of a system that meets the user's needs.
4) **INTERNAL AUDITOR'S PARTICIPATION:** Internal auditor should be involved from the starting point of the system development process to ending point to give suggestions about system requirements and controls.
5) **PROGRAM TESTING:** All program modules must be thoroughly tested before they are implemented. The results of the tests are then compared against predetermined results to identify programming and logic errors.
6) **USER TEST AND ACCEPTANCE PROCEDURES:** Just before implementation, the individual modules of e system must be tested as a unified whole A test team comprising user personnel, systems professionals, and internal audit personnel subjects(=put through/expose) the system to rigorous testing. Once the test team is satisfied that the system meets its stated requirements, the system is formally accepted by the user department(s).

SIMILAR QUESTION

1. **A controlled systems development process is required to mitigate the risks of incomplete, inaccurate, unauthorized, untimely or inefficient systems development. This process should be documented in a standard corporate systems development methodology that emphasizes documentation, justification, approval, review, monitoring, user involvement and testing. In this context what are the control activities that deal with information system development management in an organization.**

A. Refer above answer

Q.No.22. Explain Programming Management Controls in Managerial Controls? (A) (M-19)

PROGRAMMING MANAGEMENT CONTROLS:

1) Program development and implementation is a major phase within the systems development life cycle.

2) The primary objective of this phase are to produce or acquire and to implement high-quality programs.

Phases of Program Development Life Cycle

PHASE	CONTROLS
Planning	Techniques like PERT Charts, Work Breakdown Structures can be used to monitor progress against plan.
Control	The Control phase has two major purposes: a) Task progress in various software life-cycle phases should be monitored against plan and corrective action should be taken in case of any deviations b) Control over software development, acquisition, and implantation tasks should be exercised to ensure software released for production use is authentic, accurate, and complete.
Design	A systematic approach to program design, such as any of the structured design or object-oriented design ~~can be used~~ is adopted
Coding	Programmers must choose a module implementation and integration strategy, a coding strategy and a documentation strategy
Testing	Three types of testing can be: **a) Unit Testing -** which focuses on individual program modules; **b) Integration Testing -** Which focuses in groups of program modules **c) Whole-of-Program Testing** - which focuses on whole program. These tests are to ensure that a developed or acquired program achieves its specified requirements.
Operation and Maintenance	Three types of maintenance can be used as: **a) Repair Maintenance -** in which program errors are corrected. **b) Adaptive Maintenance -** in which the program is modified to meet changing user requirements. **c) Perfective Maintenance -** in which the program can be reset to decrease the resource consumption.

SIMILAR QUESTION:

1. **Program Development Life Cycle (PDLC) is a systematic way of developing quality software. It provides an organized plan for breaking down the task of program development into manageable chunks, each of which must be successfully completed before moving on to the next phase. Being a SDLC expert list out the important phases of PDLC elucidating each phase briefly.**

A. Refer above answer

Q.No.23. Explain Data Resource Management Controls in Managerial Controls? (B)(RTP-N19)

DATA RESOURCE MANAGEMENT CONTROLS

1) Many organizations now recognize that data is a critical resource that must be managed properly and therefore, accordingly, centralized planning and control are implemented.

2) For data to be managed better; users must be able to share data; data must be available to users when it is needed, in the location where it is needed, and in the form in which it is needed.

3) It must be possible to modify data easily and the integrity of the data must be preserved.

4) Data repository system must be controlled carefully, because the consequences are serious if the data definition is compromised or destroyed.

5) Careful control should be exercised over the roles by appointing senior, trustworthy persons by, separating duties to the extent possible.

6) Logs related to Data administrator's and database administrator's activities are to be maintained and monitored.

SIMILAR QUESTION:

1. **Propelled by the Internet, intranets, a flood of multimedia information, and applications such as data warehousing and data mining, data storage at most companies is growing faster than ever. That is why organizations and their managers need to practice data resource management, a managerial activity that applies information systems technologies like database management, data warehousing, and other data management tools to the task of managing an organization's data resources to meet the information needs of their business stakeholders. In this context, write about the managerial controls towards data resource management.**

A. Refer above answer.

Q.No.24. Explain Quality Assurance Management Controls in Managerial Controls? (C)

QUALITY ASSURANCE MANAGEMENT IS CONCERNED WITH ENSURING THAT:

1) Information systems produced by the information systems function achieve certain quality goals;

2) Development, implementation, operation and maintenance of Information systems comply with a set of quality standards.

3) Quality Assurance (QA) personnel should work to improve the quality of information systems produced, implemented, operated, and maintained in an organization.

4) They perform a monitoring role for management to ensure that -

   a) Quality goals are established and understood clearly by all stakeholders; and

   b) Compliance occurs with the standards that are in place to attain quality information systems.

SIMILAR QUESTION:

1. **Poor quality control over the production, implementation, operation, and maintenance of software can be costly in terms of missed deadlines, dissatisfied users and customers, lower morale among information system staff, higher maintenance, and strategic projects that must be abandoned. In this context what is the criticality of quality assurance management in the development of IS?**

A. Refer above answer

Q.No.25. Explain Security Management Controls in Managerial Controls? (B)

1) Information security administrators are responsible for ensuring that information systems assets categorized under Personnel, Hardware, Facilities, Documentation, Supplies Data, Application Software and System Software are secure.

2) Assets are secure when the expected losses that will occur over some time, are at an acceptable level.

3) The control's classification based on "Nature of Information System Resources" like Environmental Controls, Physical Controls and Logical Access Controls are all security measures against the possible threats. However, despite the controls on place, there could be a possibility that a control might fail.

4) Disasters are events / incidents that are so critical that has capability to hit business continuity of an entity in an irreversible manner.

5) When disaster strikes, it still must be possible to recover operations and mitigate losses using the last resort controls like a Disaster Recovery Plan (DRP) and Insurance.

6) A comprehensive DRP comprise four parts – **an Emergency Plan, a Backup Plan,** a **Recovery Plan** and a **Test Plan.** The plan lays down the policies, guidelines, and procedures for all Information System personnel.

7) Adequate insurance must be able to replace Information Systems assets and to cover the extra costs associated with restoring normal operations.

8) **BCP (Business Continuity Planning) Controls:** These controls are related to having an operational and tested IT continuity plan, which is in line with the overall business continuity plan, to ensure a minimum impact on business in the event of a major disruption

SIMILAR QUESTION:

1. **Auditing information security is a vital part of any IT audit and is often understood to be the primary purpose of an IT Audit. The broad scope of auditing information security includes such topics as data centers networks and application security. Then what areas are to be considered by the auditors with regard to the security management controls?**

A. Refer above answer.

Q.No.26. What are Operation Management Controls and explain its functions?
(B) (RTP-M18) (RTP-M19)

Operations management is responsible for the daily running of hardware and software facilities. Operations management typically performs controls over the functions as below:

1) **COMPUTER OPERATIONS:** The controls over computer operations govern the activities that directly support the day-to-day execution of either test or production systems on the hardware/software platform available.

2) **NETWORK OPERATIONS:** This includes the proper functioning of network operations and monitoring the performance of network communication channels, network devices, and network programs and files.

3) **DATA PREPARATION AND ENTRY:** Irrespective of whether the data is obtained indirectly from source documents or directly from customers, the data should be entered with speed and accuracy by keyboard operators.

4) **PRODUCTION CONTROL:** This includes the major functions like- receipt and dispatch of input and output, job scheduling, management of service-level agreements with users, transfer pricing/charge-out control, and acquisition of computer consumables.

5) **FILE LIBRARY:** This includes the management of an organization's machine- readable storage media like magnetic tapes, cartridges, and optical disks.

6) **DOCUMENTATION AND PROGRAM LIBRARY:** This involves that documentation librarians ensure that documentation is stored securely, that only authorized personnel gain access to documentation, that documentation is kept up-to- date and that adequate backup exists for documentation.

7) **HELP DESK/TECHNICAL SUPPORT:** This assists end-users in problem resolution with respect to production systems.

8) **CAPACITY PLANNING AND PERFORMANCE MONITORING:** Regular performance monitoring facilitates the capacity planning wherein the resource deficiencies must be identified well in time so that they can be made available when they are needed.

9) **MANAGEMENT OF OUTSOURCED OPERATIONS:** This has the responsibility for carrying out day-to-day monitoring of the outsourcing contract.

SIMILAR QUESTION:

1. **Operational control can be a very big job, requiring substantial overhead for management, data collection, and operational improvement. The idea behind operational control is streamlining the process to minimize costs and work as quickly and efficiently as possible. Operational control systems are designed to ensure that day-to-day actions are consistent with established plans and objectives. In this context what are the key areas an IS auditor should pay attention with regard to operational controls in IS?**

A. Refer above answer.

PART 7: APPLICATION CONTROLS

Q.No.27. What are Application Controls? Explain Boundary Controls in Application Controls? (B) (N-18)

1) Any function or activity that works to ensure the processing accuracy of the application can be considered an application control.
2) The objective of application controls is to ensure that data remains complete, accurate and valid during its input, update and storage.
3) **BOUNDARY CONTROLS:** The major controls of the boundary system are the access control mechanisms that links the authentic users to the authorized resources, they are permitted to access.
4) **MAJOR BOUNDARY CONTROL ARE AS FOLLOWS:**
   a) **Cryptography:** It deals with programs for transforming data into cipher text (secret code) that are meaningless to anyone, who does not have permission to access the respective system resource or file.

      Three techniques of cryptography are transposition (rearrange the order of characters within a set of data), substitution (replace text with a key text) and product cipher (combination of transposition and substitution).

   b) **Passwords:** For user identification, password mechanism can be used. The passwords may be personal characteristics like name, birth date, employee code, function, designation etc.

PERSONAL IDENTIFICATION NUMBERS (PIN):

1) PIN is similar to a password assigned to a user by an institution.
2) It is a random number stored in its database independent to a user identification details, or it may be customer selected number.
3) Hence, a PIN may be exposed to vulnerabilities while issuance or delivery, validation, transmission and storage.
   a) **Identification Cards:** Identification cards are used to store information required in an authentication process of an employee or user.
   b) **Biometric Devices:** Biometric identification e.g. thumbs and/or finger impression, eye retina etc. are also used as boundary control techniques.

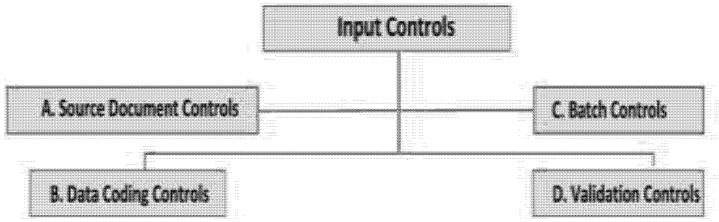
SIMILAR QUESTION:

1. **The objective of application controls is to ensure that application systems safeguard assets and maintain data integrity. Application controls are exercised by hardware and software and not by people. The boundary subsystem in application controls establishes the interface between the would-be user of a computer system and the computer system itself. In this context make a brief note on the boundary controls subsystem in application controls.**

A. Refer above answer

Q.No.28. Briefly explain Input Controls in Application Controls? (B)

1) Input Controls are responsible for ensuring the accuracy and completeness of data and instruction input into an application system.
2) Input controls are important and critical because large time is spent on input of data, which involves human intervention and are, therefore prone to errors and frauds.
3) Input control techniques are:
   a) Source Document Control
   b) Data Coding Controls
   c) Batch Controls
   d) Validation Controls



SIMILAR QUESTION:

1. **A typical way auditors evaluate controls in an application system is to trace instances of material transaction types through the system. If they are to undertake this task, they must first understand how the application system obtains its data input. In this context make a brief note on the criticality of input controls along with a list of input control techniques.**

A. **Refer above answer.**

Q.No.29. Explain Source Document Controls in Input controls? (B)

SOURCE DOCUMENT CONTROLS:

1) In systems that use physical source documents to initiate transactions, careful control must be exercised over these instruments.
2) Source document fraud can be used to remove assets from the organization.
3) For example, an individual with access to purchase orders and receiving reports could make a purchase transaction to a non-existent supplier.
4) In the absence of other compensating controls to detect this type of fraud, the system would create an account payable and subsequently write a cheque for payment.
5) To control against this type of exposure, the organization must implement control procedures over source documents to account for each document.

SIMILAR QUESTIONS:

Auditors must understand the fundamentals of good source document design. Source document design begins after carrying out source document analysis. Source document analysis determines what data will be captured, how data will be captured etc., in this context what should be the insights of auditor with regard to source document controls?

Ans: Refer above answer.

Q.No.30. Explain Data Coding Controls in Input controls? (A) M (18)

Two types of errors i.e **Transcription** and **Transposition** errors can corrupt the data and cause processing errors. Any of these errors can cause serious problems in data processing if they go undetected.

1) **TRANSCRIPTION ERRORS:** It is a special type of data entry error that is commonly made by human operators or by Optical Character Recognition (OCR) programs. These fall into three classes:
   a) **Addition errors** (when an extra digit is added to the code);
   b) **Truncation Errors** (when a digit is removed from the code) and
   c) **Substitution Errors** (replacement of a digit in a code with another)
2) **TRANSPOSITION ERRORS:** It is a simple error of data entry that occurs when two numbers are reversed (Transpose) when posting a transaction.

   For example, a sales order for customer 987654 that is transposed into 897654 will be posted to the wrong customer's account.

SIMILAR QUESTIONS:

1. **Data codes have two purposes. First, they uniquely identify an entity second they are compact poorly designed codes affect the input process in two ways. They are error prone and they cause recording and keying processes to be inefficient. In this context what areas are to be considered by the IS auditor with respect to data coding controls?**

A. **Refer above answer**

Q.No.31. Explain Batch Controls in Input controls? (B)

Batching is the process of grouping together transactions that carry some type of relationship to each other.

To identify errors or irregularities in either a physical or logical batch, three types of control totals are as follows:

1) **FINANCIAL TOTALS:** Grand totals calculated for each field containing money amounts.
2) **HASH TOTALS:** Grand totals calculated for any code on a document in the batch, EX: the source document serial numbers can be totalled.
3) **DOCUMENT/RECORD COUNTS:** Grand totals for number of documents in record in batch.

SIMILAR QUESTION:

1. **Some of the simplest and most effective controls over data capture and entry activities are batch controls. Various controls then can be exercised over the batch to prevent or detect errors or irregularities in batches. Then what insights an IS auditor should have to identify errors or irregularities in either a physical or logical batch of transactions?**

A. **Refer above answer**

Q.No.32. Define validation controls. Explain Field Interrogation level in input validation controls? (B) (MTP2-M19)

VALIDATION CONTROLS: Input validation controls are intended to detect errors in the transaction data before the data are processed.

Field interrogation: It involves programmed procedures that examine the characters of the data in the field.

This includes the checks like

1) Limit Check (against predefined limits),
2) Picture Checks (against entry into processing of incorrect/invalid characters),
3) Valid check codes (against predetermined transactions codes, tables) etc.

SIMILAR QUESTIONS:

1. **Data submitted, as input to an application system should be validated as soon as possible after it has been captured and as close as possible to its source. Errors then can be corrected by persons who are likely to have most knowledge about them and while the circumstances surrounding the data are still fresh in their minds. In this context write about validation controls and also about field interrogation checks.**

A. **Refer above answer**

Q.No.33. Explain Record Interrogation level in input validation controls? (B) (MTP2-M19)

RECORD INTERROGATION: These are discussed as follows:

1) **Reasonableness Check:** Whether the value specified in a field is reasonable for that particular field?
2) **Valid Sign:** The contents of one field may determine which sign is valid for a numeric field.
3) **Sequence Check:** If physical records follow a required order matching with logical records.

SIMILAR QUESTION:

With a record check, the validation tests applied to a field depend on the field's logical interrelationships with other fields in a record. Then what types of record checks can be applied during Record interrogation process?

Ans: Refer above answer.

Q.No.34. Explain file Interrogation level in input validation controls? (B) MTP2M19

FILE INTERROGATION CONTROLS INCLUDES:

1) Version usage
2) Internal and external labeling

3) Data file security

4) File updating and maintenance authorization etc.

SIMILAR QUESTION:

1. **With a file check, the validation tests examine whether the characteristics of a file used during data entry are congruent with the sated characteristics of the file. Then list out some file interrogation controls.**

A. Refer above answer

Q.No.35. Explain about Communication Controls in brief? (B) (M18)

COMMUNICATION CONTROLS: Components in the communication system are responsible for transporting data from one system to another system.

SOME COMMUNICATION CONTROLS ARE AS FOLLOWS:

1) **Physical Component Controls:** These controls include features that mitigate (=lessen) the possible effects of exposures.

2) **Line Error Control:** Whenever data is transmitted over a communication line, remember that it can be received in error because of noise that occurs on the line. These errors must be detected and corrected. **(M-18)**

3) **Flow Controls:** Flow controls are needed because two nodes in a network can differ in terms of the rate at which they can send, receive, and process data. For example, a main frame can transmit data to a microcomputer terminal.

4) **Link Controls:** In Wide Area Network (WAN), line error control and flow control are important functions in the component that manages the link between two nodes in a network.

5) **Channel Access Controls:** Two different nodes in a network can compete to use a communication channel. Whenever the possibility of contention (=conflict) for the channel exists, some type of channel access control technique must be used.

SIMILAR QUESTION:

1. **IS Auditors are likely to spend increasing amounts of time evaluating controls relating to the communication subsystem because the communication subsystem is responsible for transporting data among all the other subsystems within a system and for transporting data to or receiving data from another system. Then what are the critical areas of communication for which controls are to be designed by the IS auditor?**

A. Refer above answer.

Q.No.36. Define processing controls and write about Processor controls in processing controls**? (B)**

PROCESSING CONTROLS :

1) The processing subsystem is responsible for computing, sorting, classifying, and summarizing data.

2) Its major components are the Central Processor, the real or virtual memory, the operating system that manages system resources, and the application programs.

PROCESSOR CONTROLS: The following Table enlists the Controls to reduce expected losses from errors and irregularities associated with Central processors.

CONTROL	EXPLANATION
Error Detection and Correction	1. Occasionally, processors might malfunction because of design errors, manufacturing defects etc., 2. The failure might be transient(=temporary), intermittent(=Irregular) or permanent.
Multiple Execution States	This helps auditors to determine which user processes will be able to carry out unauthorized activities
Timing controls	An operating system might get stuck in an infinite loop. In the absence of any control, the program will retain use of processor and prevent other programs from undertaking their work.

Component replication	In some cases, processor failure can result in significant losses. Redundant processors allow errors to be detected and corrected

SIMILAR QUESTION:

1. **The central processing unit is the most important resource to allocate in a computer system. It executes program instructions that are fetched from primary memory. The processor is connected to main memory and input/output devices via a high-speed bus. An IS auditor should enforce four types of controls that can be used to reduce expected losses from errors and irregularities associated with central processors what are they?**

A. **Refer above answer**

Q.No.37. write about a)Real Memory Controls b)Virtual Memory Controls c) Data Processing Controls? (B)

1) **REAL MEMORY CONTROLS:** Real memory controls seek to detect and correct errors that occur in memory cells and to protect areas of memory assigned to a program from illegal access by another program.

2) **VIRTUAL MEMORY CONTROLS:**

   a) Virtual Memory exists when the addressable storage space is larger than the available real memory space.

   b) To achieve this outcome, a control mechanism must be in place that maps virtual memory addresses into real memory addresses.

3) **DATA PROCESSING CONTROLS:**

   a) Data Processing Controls perform validation checks to identify errors during processing of data. They are required to ensure both the completeness and the accuracy of data being processed.

   b) Normally, the processing controls are enforced through database management system that stores the data.

   c) However, adequate controls should be enforced through the front-end application system also to have consistency in the control process.

Q.No.38.-Define Update and Report controls .Explain Update controls in Database Controls. (B)

CONTROLS: Protecting the integrity of a database when application software acts as an interface to interact between the user and the database, are called **Update Controls** and **Report Controls**.

1) **MAJOR UPDATE CONTROLS ARE:**

   Sequence Check between Transaction and Master Files: Synchronization and the correct sequence of processing between the master file and transaction file is critical to maintain the integrity of data in the master file with respect to the transaction records.

   If errors, in this stage are overlooked, it leads to corruption of the critical data.

2) **ENSURE ALL RECORDS ON FILES ARE PROCESSED:** While processing, the transaction file records mapped to the respective master file, and the end-of-file of the transaction file with respect to the end-of-file of the master file is to be ensured.

3) **PROCESS MULTIPLE TRANSACTIONS FOR A SINGLE RECORD IN THE CORRECT ORDER:** Multiple transactions can occur based on a single master record. All transactions should be processed in correct order.

4) **MAINTAIN A SUSPENSE ACCOUNT:** When mapping between the masters records to transaction record results in a mismatch due to failure in the corresponding record entry in the master record; then these transactions are maintained in a suspense account.

SIMILAR QUESTION:

1. **Update protocols in application software seek to ensure that changes to the database reflect changes to the real-world entities and associations between entities that data in the database is supposed to represent. In this context what are the significant areas should an IS auditor consider with respect to update controls?**

A. **Refer above answer**

Q.No.39. Explain Report Controls in Database Controls in detail? (B)

MAJOR REPORT CONTROLS ARE:

1) **STANDING DATA:** Application programs use many internal tables to perform various functions like gross pay calculation, billing calculation based on a price table, bank interest calculation etc. Maintaining integrity of the pay rate table, price table and interest table is critical within an organization.
2) **PRINT-RUN-TO RUN CONTROL TOTALS:** Run-to-Run control totals help in identifying errors or irregularities like record dropped erroneously from a transaction file ,wrong sequence of updating or the application software processing errors.
3) **PRINT SUSPENSE ACCOUNT ENTRIES:** Similar to the update controls, the suspense account entries are to be periodically monitored with the respective error file and action taken on time.
4) **EXISTENCE/RECOVERY CONTROLS:** The back-up and recovery strategies together encompass the controls required to restore failure in a database. Recovery strategies involve roll-forward (current state database from a previous version) or the roll-back (previous state database from the current version) methods.

SIMILAR QUESTION:

1. **Report protocols in application software have been designed to provide information to users of the database that will enable them to identify errors or irregularities that have occurred when the database has been updated. In this context what are the significant areas should an IS auditor consider with respect to report controls?**

A. **Refer above answer**

Q.No.40. Explain different Output Controls in Detail? (B)

1) **OUTPUT CONTROLS:** ensure that the data delivered to users will be presented, formatted and delivered in a secured manner.
2) **VARIOUS OUTPUT CONTROLS ARE AS FOLLOWS:**
   a) **Storage and Logging of sensitive, critical forms:** Pre-printed stationery should be stored securely to prevent unauthorized destruction or removal and usage.
   b) **Logging of output program executions:** When programs used for output of data are executed, these should be logged and monitored, otherwise confidentiality/integrity of the data may be compromised.
   c) **Spooling/Queuing:** "SPOOL" is an acronym for "**Simultaneous Peripherals Operations Online**". This is a process used to ensure that the user can continue working, while the print operation is getting completed.

      A queue is the list of documents waiting to be printed on a particular printer; this should not be subject to unauthorized modifications
   d) **Controls over printing:** Outputs should be made on the correct printer and it should be ensured that unauthorized disclosure of information printed does not take place.
   e) **Report Distribution and Collection Controls:** Distribution of reports should be made in a secure way to prevent unauthorized disclosure of data. It should be made immediately after printing to ensure that the time gap between generation and distribution is reduced.
      i) A log should be maintained for reports that were generated and to whom these were distributed.
   f) **Retention Controls:** Retention controls consider the duration for which outputs should be retained before being destroyed. Retention control requires that a date should be determined for each output item produced.

SIMILAR QUESTION:

1. **The output subsystem provides functions that determine the content of data that will be provided to users, the ways data will be formatted and presented to users and the ways data will be prepared for and routed to users. As an IS auditor what is your criteria in designing the output controls?**

A. **Refer above answer.**

THE END