TA2-CSAC

Q1. What is IT Security Assessment and IT Security Audit?

Ans:- **IT Security Assessment**:- Security assessments are carried out by individuals who are unclear as to the quality of the security measures put in place on their IT systems and networks. The benefits to a secure network are many and include the security measure's ability to protect user confidentiality, sensitive data, system resources, and much more.

Types of IT security Assessment-

- Who can access and with what permission based
- Existing protective systems
- Compliance with security regulations
- Vulnerability to security incidents
- Resilience against potential harm

IT Security Audit:- An IT security audit is an independent assessment of an organization's internal policies, controls, and activities. You use an audit to assess the presence and effectiveness of IT controls and to ensure that those controls are compliant with stated policies. In addition, audits provide reasonable assurance that organizations are compliant with applicable regulations and other industry requirements.

There are many types of audits, such as the following:

- **Financial audits—**These determine whether an organization's financial statements accurately and fairly represent the financial position of the organization.
- **Compliance audits**—These determine if an organization is adhering to applicable laws, regulations, and industry requirements.
- **Operational audits**—These provide a review of policies, procedures, and operational controls across different departments to ensure processes are adequate.
- **Investigative audits**—These investigate company records and processes based on suspicious activity or alleged violations.
- **Information technology audits—**These address the risk exposures within IT systems and assess the controls and integrity of information systems

Q2. What is Governance & explain various types of Governance.

Ans:- Governance is all the processes of interactions be they through the laws, norms, power or language of an organized society over a social system.

It is done by the government of a state, by a market, or by a network.

Types of Governance:-

1. Participatory or Democratic Governance
2. Global Governance
3. Good Governance

4. Corporate Governance
5. Environmental Governance
6. E-Governance

Q3. What is Compliances and how to maintaining IT Compliances.

Ans:- Compliances:- Compliance is the act of complying with a command, desire, wish, order, or rule. It can also mean adhering to requirements, standards, or regulations. Both of these compliance definitions are important for your organization.

Maintaining IT Compliances :-To maintain compliance, however, organizations should create a framework for IT security. A policy framework provides for a structured approach for outlining requirements that must be met

- Policy—Users are required to use strong authentication when accessing company systems.
- Standard—Users are required to use two-factor authentication when accessing the remote network, combining a physical one-time token code with a personal identification number.
- Guideline—Always keep your token within your possession and be aware of your surroundings when entering your personal identification number

Q4. What is the scope of an IT compliance audit?

Ans:- Compliance Audit is detailed review of organization's loyalty towards uphold of the rules and regulations which includes statutory and internal rules, regulations, policies and procedures framed by Government, local authorities and organization's management by evaluating compliance procedure, security policies, user access control, risk management procedure and entity's policy, procedure, and processes.

examples:

- The audit will cover the manufacture of product A and B, but not the manufacture of product C. The audit will cover head office plus the branches in New York, London, and Tokyo.
- The audit will cover the work period from January through to June inclusively. Without effective scope, both the auditor and the auditee are unsure of the boundaries of the audit and time is often wasted through checking and verifying information that is not required (out of scope).

Q5. What does your organization do to be in compliance?

Ans:-

- Remove barriers to compliance.
- Stay on track with changing laws and regulations
- Involve specialists
- Ensure employees follow procedures

- Schedule regular internal audits
- Use the right software
- Avoiding criminal proceedings
- Assumption of social responsibility
- Assemble a compliance team
- Compliance analysis
- Formulate and communicate compliance policies
- Implementation in regular operation and adjustment
- Coordinate internal teams
- Don't forget about international locations

Q6. What are you auditing within the IT infrastructure?
Ans:-

- Having outdated policies or no policies in place.
- Lack of vulnerability scanning or penetration (PEN) testing.
- Lack of an Intrusion Prevention System (IPS). Alternatively, if your IPS is not properly managed.
    - Lack of two-factor authentication for any form of remote access.
    - You allow your IT staff to enact as security staff and do not have a dedicated security staff.
- There is no up-to-date disaster recovery plan or tested business continuity plan.
- No data loss prevention plan in place.
- Lack of keeping up to date with OS, network or applications updates.
- Lack of a network and system drawings showing the architecture of the network as well as data flow.

Q7. Explain Planning and implementation of an IT Infrastructure Audit for compliance.
Ans:-

The audit planning process directly affects the quality of the outcome. A proper plan ensures that resources are focused on the right areas and that potential problems are identified early. A successful audit first outlines the objectives of the audit, the procedures that will be followed, and the required resources.

items for an organization you are familiar with:

1. Scope
2. Goals and objectives
3. Frequency of the audit
4. Duration of the audit
5. Identify the critical requirements of the audit for your chosen organization and explain why you consider them to be critical requirements.

6. Choose privacy laws that apply to the organization, and suggest who is responsible for privacy within the organization.
7. Develop a plan for assessing IT security for your chosen organization by conducting the following:
8. Risk management
9. Threat analysis
10. Vulnerability analysis
11. Risk assessment analysis
12. Explain how to obtain information, documentation, and resources for the audit.
13. Analyze how each of the seven (7) domains aligns within your chosen organization.
14. Align the appropriate goals and objectives from the audit plan to each domain and provide a rationale for your alignment.
15. Develop a plan that:
16. Examines the existence of relevant and appropriate security policies and procedures.
17. Verifies the existence of controls supporting the policies.
18. Verifies the effective implementation and ongoing monitoring of the controls.
19. Identify the critical security control points that must be verified throughout the IT infrastructure, and develop a plan that includes adequate controls to meet high-level defined control objectives within this organization.
20. Use at least three (3) quality resources in this assignment. Note: Wikipedia and similar Websites do not qualify as quality resources.

Q8.What Are Controls and Why Are They Important?

Ans:- Controls are a security mechanism, policy, or procedure that can successfully counter attacks, reduce risk, resolve vulnerabilities, and otherwise improve security within an organization. The main focus of control formulation and development should be on the security of hardware, telecommunications, and software. Moreover, the level of control implementation chosen should protect sensitive information in one of the following three states: data at rest, data in transit, and data in process. Security controls can be grouped in one of two categories: goal based and implementation.

Q9. Explain The IT Audit Process and types of Audits.

Ans:- The process of performing an IT audit is summarised in the five steps below:

1. Determine the objective and scope of the IT audit
2. Develop an audit plan to achieve the audit objectives
3. Gather information on relevant IT systems, operations and related controls

4. Perform audit tests on key IT controls, using Computer-Assisted Audit Techniques (CAATs), where appropriate
5. Report on the audit findings

Types of Audits:

- Financial audits
- Compliance audits
- Operational audits
- Investigative audits
- Information technology audits

Q10.What is Computer-Assisted Audit Techniques and application control for CAAT.

Ans:- Computer Assisted Audit Techniques (CAATs) is the tool which is used by the auditors. This tool facilitates them to make search from the irregularities from the given data. With the help of this tool, the internal accounting department of any firm will be able to provide more analytical results. These tools are used throughout every business environment and also in the industry sectors too. With the help of Computer Assisted Audit Techniques, more forensic accounting with more analysis can be done. It's really a helpful tool that helps the firm auditor to work in an efficient and productive manner.

The CAAT tool supports the forensic accounting in which larger amount can be diverted to the analytical form and it also prompts where the tool detects the fraud. This tool simplifies the data and in the automated form. The name of CAATs tool is placed in almost every firm where the auditing or advance level accounting takes place. The firm is well aware of the benefits of these tools and also making some advancement in this tool in accordance with their need, in return all the large raw data becomes in statistical and analytical form. It's a time saving tool.

Q11.Explain Seven Domains of a Typical IT Infrastructure in details.

Ans:-

1. **User Domain**
   The User Domain covers the end users of information systems. An audit of the User Domain should be considered for anyone accessing the organization's information systems. This includes not just employees but nonemployees as well, such as contractors and consultants. This domain considers the roles and responsibilities of the users. It should examine all policies that relate to them—specifically, access policies
   The policies that apply might include the following:
   • Acceptable use policy (AUP)

- System access policy
- Internet access policy
- E-mail policy

2. **Workstation Domain**

   The Workstation Domain comprises the desktop environment of an end user's computing environment and includes the following:

   - Desktop computers
   - Laptop computers
   - Printers
   - Scanners
   - Handheld computers and mobile devices
   - Modems
   - Wireless access points

   Each of these devices should be authorized to access and connect to the organizational network and information resources. Thereafter, an audit of this domain would also ensure proper procedures and controls around maintaining the system hardware and software. Any desktop operating system, for example, should comply with the standards defined by the organization. The audit would take into consideration those security controls already applied. Standard operating systems and patch levels are typically mandated as well as specific configuration controls and the presence of anti-malware, desktop firewalls, and other security controls.

3. **LAN Domain**

   A LAN is typically made up of computing and networking equipment in close proximity, such as a single room or building. LANs provide each computer on the network access to centralized resources, such as file servers and printers. In addition, they provide an easy method by which all the computers can be administered. Various other elements comprise the LAN Domain, including the physical connections required, such as the wiring, and networking equipment, such as hubs and switches. An audit of the LAN Domain can examine various elements, such as the following:

   - Logon mechanisms and controls for access to the LAN
   - Hardening and configuration of LAN systems
   - Backup procedures for servers
   - The power supply for the network

4. **LAN-to-WAN Domain**

While a LAN typically covers a smaller defined geographical area, a WAN provides for long distance communication to extend a network across a wider geographic area. Thus, a WAN can connect multiple LANs together. The transition from a LAN to a WAN typically involves equipment such as a router or a firewall. A router is used to forward data between different networks. A firewall is another common component. A firewall is placed between networks and is designed to permit authorized access while blocking everything else. The WAN Domain is considered an untrusted zone. It might be made up of components outside the direct control of the organization, and is often more accessible by attackers. The area between the trusted and untrusted zone, the LAN-toWAN Domain, is protected with one or more firewalls. This is also called the boundary, or edge. The public side of the boundary is often connected to the Internet and has public Internet Protocol (IP) addresses. These IP addresses are accessible from anywhere in the world. Attackers constantly probe public IP addresses looking for open ports and vulnerabilities. A high level of security is required to keep the LAN-to-WAN Domain secure. An audit is critical to ensure that the environment is controlled correctly to prevent unauthorized access. There are many components and controls that work together to provide security. Organizations should carefully manage the configurations of all devices in this domain, such as firewalls, routers, and intrusion detection systems.

5. **WAN Domain**

The Remote Access Domain is made up of the authorized users who access organization resources remotely. Access most often occurs over unsecured transports such as the Internet. Other unsecured transports include dial-up via a modem. Mobile workers often need access to the private LAN while traveling or working from home, for example. Mobile workers are granted this access using remote access solutions. Remote access solutions, such as a virtual private network (VPN), can create an encrypted communications tunnel over a public network such at the Internet. Because the Internet is largely untrusted, remote access might represent a significant risk. Attackers can access unprotected connections. They might try to break into the remote access servers as well. Using a VPN is an example of a control to reduce the risk. VPNs, however, have their own vulnerabilities. For example, how does a user authenticate with the VPN? An attacker can gain access via the secured encrypted tunnel back to the corporate data just by knowing or guessing the credentials of the authorized user. An audit should carefully consider the governing policies and procedures as well as the type of access provided.

6. **Remote Access Domain**

The Remote Access Domain is made up of the authorized users who access organization resources remotely. Access most often occurs over unsecured transports such as the Internet. Other unsecured transports include dial-up via a modem. Mobile workers often need access to the private LAN while traveling or working from home, for example. Mobile workers are granted this access using remote access solutions. Remote access solutions, such as a virtual private network (VPN), can create an encrypted communications tunnel over a public network such at the Internet. Because the Internet is largely untrusted, remote access might represent a significant risk. Attackers can access unprotected connections. They might try to break into the remote access servers as well. Using a VPN is an example of a control to reduce the risk. VPNs, however, have their own vulnerabilities. For example, how does a user authenticate with the VPN? An attacker can gain access via the secured encrypted tunnel back to the corporate data just by knowing or guessing the credentials of the authorized user. An audit should carefully consider the governing policies and procedures as well as the type of access provided.

7. **System/Application Domain**
   The System/Application Domain is made up of the many systems and software applications that users access. This, for example, includes mainframes, application servers, Web servers, proprietary software, and applications. Mail servers send and receive e-mail. Database servers host data that is accessed by users, applications, or other servers. Domain Name System (DNS) servers provide name-to-IP address resolution for clients. Knowledge within this domain can be very specialized. Operators may focus on one specific aspect, such as mail servers, and be quite familiar with associated security ramifications. On the other hand, that same person might know very little about databases. Like the desktop operating system, server operating systems should be hardened to authorized baselines and configured according to policies and standards with the appropriate controls

Q12. How to Identifying the Minimum Acceptable Level of Risk and Appropriate Security in IT Infrastructure.

Ans:- For an organization to develop security baselines, it must select proper controls. However, the decision to apply or not apply controls is based on risk. Specifically, the controls put in place manage the identified risks. As a result, a risk assessment needs to be completed first. It might seem easiest to apply a wide range of controls based on different recommendations. Remember, however, that there are costs associated with these controls. For example, you can take many different steps to secure your home and minimize risks. Most people consider door locks as necessary. Beyond that, there is no universal rule of home security to which everyone adheres. Even door locks are available in varying strengths. Consider other measures a homeowner might take. Examples include bars on the windows, storm shutters, insurance, burglar alarms, smoke detectors, carbon monoxide detectors, cameras, safes, watchdogs, outdoor lighting, fences, and even weapons. These examples of home controls are similar to IT controls in that there is a cost associated with each of them. Depending on the type or mission of the business, the cost justifications vary. The controls are based on the level of risk the organization faces.

Q13.Define the following term.

- **Risk Analysis :-** A risk analysis involves identifying the most probable threats to an organization and analyzing the related vulnerabilities of the organization to these threats.
- **Risk identification :-**Risk identification is the process of documenting any risks that could keep an organization or program from reaching its objective. It's the first step in the risk management process, which is designed to help companies understand and plan for potential risks. Examples of risks include theft, business downturns, accidents, lawsuits or data breaches. When you identify risks, look for events that may prevent a project from achieving its goal. The risk's origin can be the project itself or external sources. There are several situations for which you might need to identify risks, including:
    - To support an investment decision
    - To assess cost uncertainty or operational costs
    - To analyze multiple alternatives
    - To test a program before its acquisition
- **Risk Assessment:-** A risk assessment involves evaluating existing security and controls and assessing their adequacy relative to the potential threats of the organization.
- **Risk response & Mitigation :-**
    - Identify and document asset vulnerabilities
    - Identify and document internal and external threats
    - Assess your vulnerabilities
    - Identify potential business impacts and likelihoods
    - Identify and prioritize your risk responses
- **Risk reporting :-** Risk reporting is a method of identifying risks tied to or potentially impacting an organization's business processes. The identified risks are usually compiled into a formal risk report, which is then delivered to an organization's senior management or to various management teams throughout the organization.

Q14. Explain Business Continuity Planning and life Cycle of BCP.

Ans:- There isn't a day which goes by, when we aren't concerned about things such as market share, branding, competitive intelligence, revenue streams, supply chain efficiencies and human capital. But what tops all these issues is a question that underlies all our concerns at a fundamental level: How do we keep our business running in the face of things like:

- Strict legislative mandates and/or regulatory requirements?
- A deadly computer virus that can bring the network down?
- Two cyclones in one year?
- All commercial air traffic being grounded for 72 hours?
- The actions of a disgruntled employee?
- Absenteeism due to an epidemic?

A well-thought-out business continuity management (BCM) plan is the answer which will help to keep a company moving in such unforeseen circumstances. Basically, the business continuity management lifecycle has six phases to it: program management, understanding the organization, determining the BCM strategy, developing and implementing a BCM response, exercising the response, as well as maintaining, reviewing and embedding BCM in the organization's culture. Here are the six steps of a business continuity management lifecycle. Awareness and training should happen at each and every stage.

Step 1: Since BCM is crucial, it should have the top management's nod. Therefore, the first step in any business continuity management lifecycle is to get the top management's commitment. A policy has to be created since the entire project will be executed by them.

Step 2: The next step in the business continuity management lifecycle is to communicate this policy to all key stakeholders including vendors and outsourced parties.

Step 3: Identify a BCM sponsor who has the authority to implement business continuity management as per the policy. He can have a team and formulate a framework which covers activities identified under the BCM software's scope. Under the scope of BCM service, key products and services have to be identified. Additionally, the BCM objective should be aligned with the organizational objective. This should include the acceptable level of risk, as well as legal, regulatory and contractual obligations in order to meet the interests of the stakeholders.

Step 4:The next step to follow in the business continuity management lifecycle is to analyze the basic impact to identify critical functions under the scope of BCM and carry out a risk assessment of those critical functions. After this, depending on the results, you have to look at alternative responses and recovery strategies. This should be followed by putting in place an incident management plan with an incident response structure. This should be followed by a business recovery plan and a disaster recovery plan. Implementing these plans is the next phase.

Step 5: After implementing all the above plans, create an exercise program to cover different plans in line with the plans' objectives, review the plans, and ascertain their limitations or gaps. Update these plans based on any gaps.

Step 6: The next step in the business continuity management lifecycle is to carry out the plan-do-check-act cycle. This includes managing the program through periodic management review, internal audits and self-assessments; embedding the BCM culture; carrying out exercises; and carrying out preventive and corrective actions to show continual improvement.

Q15. Why Business Continuity Planning required

Ans:-

- Provide an immediate response to emergency situations
- Protect lives and ensure safety
- Reduce business impact
- Resume critical business functions
- Reduce confusion during a crisis
- Ensure survivability of the business
- Get up and running ASAP after a disaster

Q16. Define the following terms.

- **Disaster Recovery:-** Disaster recovery involves a set of policies, tools, and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster

- **Compliances:-** Compliance is the act of complying with a command, desire, wish, order, or rule. It can also mean adhering to requirements, standards, or regulations. Both of these compliance definitions are important for your organization.

- **Audit:-** Audit is a process to assess and review of an organization's internal policies, controls, and activities in accordance with guideline, framework or compliances. Audit can be used to assess the presence and effectiveness of IT controls and to ensure that those controls are compliant with stated policies

- **IT Security:-** -IT security is a set of cybersecurity strategies that prevents unauthorized access to organizational assets such as computers, networks, and data. It maintains the integrity and confidentiality of sensitive information, blocking the access of sophisticated hackers.

- **System Monitoring:-** System monitoring software is an umbrella category of software that enables organizations to manage, operate, and monitor IT systems in a centralized manner. System monitoring is often found as a core offering for many managed service providers that also delve into other aspects of application, infrastructure, and service monitoring. System monitoring is used by IT teams for things like configuration and security management, backup and restore capabilities, patch management, and more.

- **Log Analysis :--** Log analysis is the process of reviewing computer-generated event logs to proactively identify bugs, security threats or other risks. Log analysis can also be used more broadly to ensure compliance with regulations or review user behavior. A log is a comprehensive file that captures activity within the operating system, software applications or devices. The log file automatically documents any information designated by the system administrators, including: messages, error reports, file requests, file transfers and sign-in/out requests. The activity is also timestamped, which helps IT professionals and developers establish an audit trail in the event of a system failure, breach or other outlying event

Q17. Explain Disaster Recovery & planning of DR.

Ans:- Disaster Recovery:- Disaster recovery involves a set of policies, tools, and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster

The availability of a business process or service depends on technical services, such as a server or database. Therefore, the direct goal of a DRP is to realize the objectives of Therefore, DRP deals with strategies and procedures for recovering one or more IT solutions a BCP. While DR focuses on recovering an IT solution from a technical point of view, a BCP takes a more complete system and outlines strategies and procedures for all components, such as incident and crisis management

Disaster Recovery Plans (DRP) contains procedures for emergency response, extended backup operations and post-disaster recovery, should a computer installation experience a partial or total loss of computer resources and physical facilities. The primary objective of the disaster recovery plan is to provide the capability to process mission-essential applications, in a degraded mode, and return to normal mode of operation within a reasonable amount of time.

Q18. How to identify of potential disaster status of any organization.

Ans:- According to the International Federation of Red Cross and Red Crescent Societies: "More people are becoming vulnerable to disasters or are forced to cope with acts of violence, financial crises and growing uncertainty, often without adequate support from their governments." Disasters can be either natural or human-made events and can include pandemics, technological disasters or environmental cataclysms.

Disaster types include the following:

- Earthquakes
- Tornadoes
- Hurricanes
- Pandemics
- Volcano eruptions
- Wildfires
- Floods
- Mass shootings
- Acts of terror
- Nuclear explosions
- Chemical emergencies

Q19.Explain DR Strategies in detail.

Ans:- Disaster Recovery Strategy:- Recovery strategy is a set of predefined & management approved actions implemented in response to a business interruption from a disaster.

– Natural / Environmental

• Earthquakes, floods, storms, hurricanes, fires, snow/ice, etc.

– Man made / political events

• Explosives, disgruntled employees, unauthorized access, employee errors, espionage, sabotage, arson/fires, hazardous/toxic spills, chemical contamination, malicious code, vandalism and theft, etc.

• Recovery strategy focuses on:

– Meeting the predetermined recovery time frames (i.e. MTD).

– Maintaining the operation of the critical business functions.

– Compiling the resource requirements.

– Identifying alternatives that are available for recovery.

Procedure for developing a recovery strategy:

- Step 1: Document all costs associated with each contingencies.
- Step 2: Obtain cost estimates for any outside services (using RFI, RFQ, or RFP).
- Step 3: Develop written agreements for outside services (i.e. Service Level Agreement (SLA)).
- Step 4: Evaluate resumption strategies based on a full loss of the facility.
- Step 5: Identify risk reduction measures and update Business Resumption Plan (BRP).
- Step 6: Document recovery strategies and present to management for comments and approval.

Q20. Explain IT security policy framework to the seven domains of typical IT infrastructure.
Ans:- The IT security policy framework includes policies, standards, and guidelines. Each of these includes technology, processes, and personnel. The seven domains of a typical IT infrastructure need to be mapped into the framework. The seven domains of a typical IT infrastructure are as follows:

- User Domain
- Workstation Domain
- LAN Domain
- LAN-to-WAN Domain
- WAN Domain
- Remote Access Domain
- System/Application Domain

In some cases, policies might be very specific to only a single domain. For example, the User Domain maps specifically to human resources security. This encompasses controls relating to items such as pre-employment background checks and information security awareness and training. The seven domains also map across various high-level areas. Examples include access control and operations management.