Puneet Mishra
MSC DFIS

Q1) What is IT security Assessment and IT security Audit?

→
- IT security assessment is a study to locate IT security vulnerabilities and risks.
- The benifits to a secure network are many and they have ability to protect user confidentiality, sensitive data, system resources and much more.
- These types of security audits are :-

a) Who can access and with what permission level.
b) Compliance with security regulations
c) Vulnerability to security incidents

- A security audit is the high level description of the many ways organizations can test and assess their overall security, including cybersecurity.
- Types of audit :-

a) Internal audit
b) External audit
c) Manual audit
d) Automated audit

2) What is governance & explain various types of governance?

→

- Governance is all the process of interaction through the laws, power of an organised society over a system. It is done by government of a state, by a market, or by a network.
- Types of governance :-

a) Corporate governance :- It consists of the processes, customs, policies, laws and institutions affecting the way people direct, administer or control an organisation.

b) Non profit governance :- It has dual focus, achieving the organisation's social mission and ensuring the organisation is viable.

c) Governance as process :- In most abstract sense, governance is a theoretical concept referring to the actions and processes by which stable practices and organisations arise and persist.

3) What is compliances and how to maintains IT compliances?

→
- Compliance is a set of digital security requirements and practices. It refers to certain guidelines and organisation must follow to ensure its process and secure.
- Maintaining IT compliance :-

a) Start with cybersecurity
b) Take time for training
c) Encrypt network data
d) Implement user access control

4) What is the scope of an IT compliance audit?

→
- It is a detailed review of organisation's loyalty towards holding the rules & regulation's which includes internal rules, regulations, policies and procedure given by government, security policies, users access control.
- The purpose behind conducting a compliance audit is to access the organisation's compliance program is effective or not and bringing out the non-compliance in front of management and government authorities.
- IT compliance is taking control and protecting information, including how it is obtained and stored, how its secured its availability and how data is protected.

5) What does your organization do to be in compliance?

→
- Involve specialists
- Use the right software
- Assemble a compliance team
- Avoiding criminal proceedings
- Stay on track with changing laws and regulations
- Schedule Regular internal audits

6) What are you auditing within the IT infrastructure?

→
- Having outdated policies or no policies in place
- Lack of vulnerability scanning and penetration testing
- Lack of two factor authentication from any form of access
- No data loss prevention plan in place
- Lack of keeping up to date OS, application updates or network

7) Explain Planning and implementation of an IT infrastructure Audit for compliance?

→
- Audit planning should not be overlooked. What goes into the 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 what's supposed to be achieved as well as what procedures will be followed and the required resources to carry out the procedures.
- Although each audit will vary, the plan and approach to each audit follow similar characteristics. Despite the best plans, however, circumstances do change, and plans need to be adjusted. As a result flexibility must be considered. Significant errors, suspected fraud, and misrepresentation can all have a considerable effect upon the initial plan. Regardless proper planning helps ensure an effective and timely audit.

8) What are controls and why are they important?

→ • The environments of controls are made up largely of a basic set of principles that apply across the various domains. These basic principles embedded throughout security operations and administration management.
• These includes the following :-
a) Defined roles and responsibilities.
b) Configuration and change management.
c) Environments for development test and production.
d) Segregation of duties.
e) Identify and authentication.
f) Principle of least privilege.
g) Monitoring, measuring and reporting.
h) Appropriate documentation.

9) Explain IT Audit process and types of audits.

→ • An IT audit is the process of investigation and assessment of IT systems, policies, operations, and infrastructure.
• Types of audit :-
• Internal audit
• External audit
• Manual audit
• Automated audit.

10) What is Computer Assisted Audit Techniques and application control for CAAT.

→ • Computer Assisted Audit techniques or CAATs can be defined as an auditing method that uses computer software tools to query business data to produce reports that will enhance an audit. CAATs can sometimes be known as CAATs (Computer Assisted Tools and Techniques) or BEAST (Beneficial Electronic audit Support Tools)

• CAATs have been used for many years to confirm more traditional audit methods. CAAT, tools include ACL (Audit Command Language), IDEA, Excel, Access and SQL Server.

11) Explain Seven Domains of a Typical IT infrastructure in details.

→ • Lan Domain :- The Lan Domain includes all the things that make up the Lan, wifi and routers. These devices connect all the workstation to one another. The following risks in this domain are :-

a) IT employes may lack the experience in designing or maintaining a secure network.

b) Lack of security policy governing network.

• Lan - to - Wan Domain :- The Lan-to-Wan Domain is where the corporate LAN connects to Wan. The following risks can be exist in this domain :-

a) No firewall present.

b) Lack of any defensive parameter control.

Wan Domain :- The Wan Domain is represented by the Internet and stands for Wide area network. The following risk exist in this domain are :-

a) Lack of the firewall and possibly unconfigured modem at the parameter could introduce many attack.

Remote access domain :- The ROD is represented by any employe or any person works in the field or from home, instead of office and access to corporate LAN. The following risk in this domain :-

a) Weak passwords can lead to unauthorized entry in the network.

System / Application Domain :- The system or Application Domain includes all system & application related issues. The risks are :-

a) An email not scanned for viruses.
b) Lack of antivirus software to protect company assets.

User Domain :- Almost 90% attacks caused by human error.
Risks identified are :-

a) Employes fail to lock their computers.
b) Employes leave sensitive information on their desks.

Workstation Domain :- The workstation domain includes any computing devices used by end users and represents how the users connect to the IT infrastructure. Risks are :-

a) Old OS present with huge vulnerability.
b) Old hard drives can lead to failure and the data loss of information.

Q12) How to identifying the Minimum Acceptable Level of Risk and Appropriate Security in IT infrastructure.

⇒
- For an organization to develop security baseline, it must select proper controls. 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 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 lock as necessary. Even door lock are available in varying strengths.
- Payment card industry Data Security Standard (PCI DSS) provides an example of a concise set of baseline controls required for those organizations that process or transmit payment card information.
- The requirement of PCI considers the general risks to payment card data and provide a baseline approach of safeguarding the sensitive data.
- When a basic control environment is in place, organization can begin implementing additional controls to continue reducing risk to acceptable levels.

13) Define the following term.

- Risk Analysis :- Risk analysis is one step in the overall cyber security risk management and risk assessment process.
- The analysis includes examining each risk to the security of your organization's information system devices and data & priorities.

- Risk Identification :- Identifying what kind of harm to the assets like information, data that you need to protect there are many threats in the world what threats are related to cyber security is done in Risk identification.

- Risk Assessment :- Cyber Security risk assessment is the process of identifying analyzing and evaluating risk it helps to ensure that the cyber security controls you choose are appropriate to the risk your organization faces.

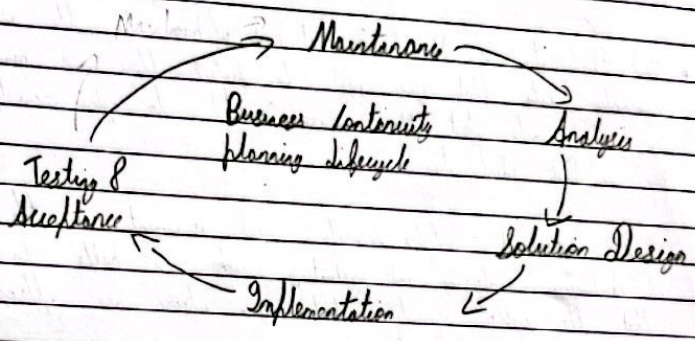
- Risk response and mitigation :- A cybersecurity Response is a document that gives IT and IT cyber security professionals instruction on how to respond to a serious security incident such as data breach on how to respond to a serious incidents or recover from them.

- Risk reporting :- A cyber risk report details information about potential risk within an organization's digital footprint and vendor ecosystem also to identify gaps in security controls and the performance of security programs.

Q14) Explain Business Continuity Planning and life cycle of BCP.

→

- A business continuity plan (BCP) is a document that consists of the critical information an organization needs to continue operating during an unplanned event.



- Analysis :- It consists of impact analysis threat risk and impact scenarios (BIA) Business impact analysis and Risk analysis.
- Solution Design :- Define the team structure and assign individual roles and responsibilities. Design data protection strategies and develop infrastructure
- Implementing :- Implement risk management and mitigation procedures that include backup replication and management of resource.
- Testing :- Training the employee who are responsible backup and replication of business critical data on a regular basis or whenever there is a modification in the plan.
- Maintenance :- To maintain the plan the solution and protection strategies and contigency scenarios.

Q15) Why Business Continuity planning Required.

→
- Business Continuity is a proactive plan to avoid and mitigate risks associated with a disruption of operation it details steps to be taken before during and after an event to maintain its financial viability of an organization also Disaster recovery is a reactive plan for responding an event.
- Benefits of having a Business continuity plan :-
  1) Your Business will be more prepared to handle the unexpected
  2) Your Business will have safeguard in place.
  3) Your Business will invest in itself and its ability to bounce back.
  4) Your Business will have a plan to continue providing acceptable service after disaster.
  5) Your business will better preserve its corporate reputation

Q16) Define the following terms.

- Disaster Recovery :- It is a reactive plan for responding after an event. It deals with the safety and restoration of critical location and operational procedure after disaster and is part of business ~~continuity~~ continuity plan.
- IT compliance :- IT compliance includes legal internal or contractually prescribed requirement for the IT of an organization. these requirement are made up of various requirements for IT security data protection, availability and integrity that apply to system.
- Audit :- It is an examination of the management controls within an information technology infrastructure and business application.

- System Monitoring :- It involves the certain constant continuous monitoring of a infrastructure. It includes monitoring of CPU server memory routers switches bandwidth and application as well as the performance and availability of important network devices.

Q17) Explain Disaster Recovery & planning of DR.

→ Disaster Recovery is a reactive plan for responding after an event. It deals with the safety and restruction of critical personal location and operational procedure after a disaster is a part of business continuity planning. DR plan is more focused than BRP and does not necessarily cover all contingencies for business process assets human resources and business partners.

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

Identify the Sources of Risk :- By addressing the major fields of threats exposure, this phase details the framework for risk assessment to provide a suitable response.

Identify crisis type :- Threats, either man made or natural, are situation or condition that can cause disruption or crisis to an organization operation or services

From the sources of risk, there are some basic types of crisis:

Natural
Technological
Confrontation
Organizational Misdeeds
Malevolence

Q 19) Explain DR strategies in detail.

→ • Disaster recovery is a process by the organization anticipate and addresses technology-related disasters. IT systems in any company can go down unexpectedly due to power outages, natural events or security issues.

• Prevention :- To reduce the likelihood of a technology-related disaster, business need a plan to ensure that all key systems are as reliable and secures as possible.

• Anticipation :- Anticipation include predicting possible future disaster, knowing the consequences, and planning appropriate disaster recovery procedures.

• Mitigation :- Mitigation is how a business responds after disaster scenario
  • Updating documentation
  • Conducting regular disaster recovery tests

Q20) Explain IT security policy framework to the seven domains of typical IT infrastructure.

• Users Domain :- User domain covers all the users.
Risks :- User can destroy data in application and delete all.

• Workstation Domain :- A computer of an Individual users where the production takes place.
Risks :- A workstation hard drive can fail causing data loss

- LAN Domain :- Contains all of the workstations, hubs, switches and routers.
  Risk :- An unauthorized user can access the organization's workstations in a LAN.
- LAN/WAN Domain :- The boundary between the trusted and untrusted zones.
  Risk :- A hacker can penetrate your IT infrastructure and gain access to your internal network.
- WAN Domain :- Stands for Wide area Network and consists of the Internet and semi private lines.
  Risk :- Service provider can have a major network outage.
- Application Domain :- This domain is made up of user accessed servers such as email and database.
  Risk :- A DOS attack can cripple the organization email.
- Remote access Domain :- The domain in which a mobile user can access the local network remotely, usually through a VPN.
  Risk :- Remote communication from office can be unsecured.