1 What is IT Security Assessment and IT Security Audit?

IT security Assessment

- The evaluation of an organization's IT infrastructure and practices to assess their current state and identify areas of improvements.
- It provides measurements and feedbacks.
- It is non attributive.
- It is focused on identifying vulnerabilities and risks in an organization's IT environment.

IT Security Audit

- The examination of an organization's IT systems and controls to assess their effectiveness, security and compliance with regulations and best practices.
- It provides insights, recommendations and identify non-compliance.
- It is focused on verifying compliance with established security standards and policies.
- Findings might place blame on specific individual or group.

2. What is governance and explain various types of governance.

Governance is a set of policies, procedures and practices that guide and manage an organization's overall strategy and operations and behaviour. It is comprehensive and covers all aspects of the organizations. It seeks to better run an organization using complete and accurate information and management processes or controls.

The different types of governance are as follows:

- Corporate governance: It is concerned with how companies are directed and controlled. It encompasses the relationship among stakeholders.
- IT governance: It focuses on aligning IT strategies with business objectives ensuring that IT resources and systems effectively support organization's goal.

- Data governance : It manages data as strategic asset. It includes establishing policies, procedures, roles and responsibilities for data quality, integrity, security and compliances.
- Regulatory governance : Refers to compliance with laws, regulations and industry standards. It involves establishing policies and procedures to ensure that an organization operates within legal boundaries and adheres to applicable regulations.
- Public governance : Organizations are required to be compliant with government regulations, laws and policies. They also engage with public institutions for permits, licenses, taxation and adherence to standards set by governmental bodies.
- Private governance : It includes internal rules, code of conduct, policies and decision-making framework set by private entities. These governs behaviour of stakeholders within organization.
- Global Governance : Global governance framework impacts organization by setting international standards, trade rules, environmental regulations, norms that affects cross country operations intellectual property rights and coporate responsibilities on global scale.

3 What is compliances and how to maintain IT Compliances?

Compliance is the act of conforming to rules, regulations, laws or standards established by a governing body, organization or authority. It is required to be compliant to meet legal or regulatory requirement and avoid potential legal consequences or penalities. Few of the widely known compliances are. GDPR, PCIDSS, HIPAA etc...

To maintain IT compliance:

- Stay Informed about regulations and standards
- Risk Assessment and Management regularly
- Implement security policies and procedures
- Enforce strict access control and user management

ANKIT

- Data Protection and Encryption for sensitive data.
- Regular Audit and Assessment
- Develop and regular update of Incident Response Plan
- Retain logs and proper event monitoring.
- Penalty and Fine Awareness
- Documentation and Data Recovery Record keeping
- Data backup and Recovery.

4. What is the scope of an IT compliance Audit?

The scope of an IT compliance audit is comprehensive and involves assessing an organization's adherence to various regulations, standards, policies and procedures related to information technology. A typical IT compliance audit may include:

- Regulatory Compliance
  Ensuring compliance within industry-specific regulations.
- Data Privacy and Protection.
  Assessing the handling, storage and protection of sensitive and personal data to ensure compliance with data privacy laws and regulations.
- Cyber Security Controls.
  Evaluating the effectiveness of cyber security controls to protect against data breaches and cyber threats
- Access and Authentication Management
  Review of access management practices to ensure only authorized person have access to IT systems and data.
- Change Management
  To ensure that changes to IT systems, applications and configurations are properly tested, documented and approved.
- Incident Response and Disaster Recovery
  Examining Incident response plan and disaster recovery procedures to ensure that the organization is prepared to respond to security incidents, data breaches and system failures
- Vulnerability Management
  To identify, prioritize and remediate security vulnerability in a timely manner.

- Network Security
  Evaluate network security measures to protect against data exfiltration and unauthorized access.
- Third-Party Risk Management
  To ensure third party vendors meet security and compliance requirement.
- Physical Security
  Assessing physical security measures such as access controls to data centers and server rooms to prevent unauthorized physical access to IT infrastructure.

5 What does your organization do to be in compliance?

To be in compliance, organizations typically take following steps:

- Assessment: Identify the relevant regulations that apply to the organization based on industry, location and type of data it handles.
- Policies and Procedures: Develop and document policies that align with compliance requirements.
- Data Protection: Implementation of data protection measures for safeguarding data.
- Access Control: Enforce strict access control and user authentication.
- Regular Audits: Conduct regular internal audit and assessment to identify areas of non-compliance and security vulnerabilities.
- Employee Training: Provide training to employees to educate about compliance policies
- Incident Response: Develop an indent response plan to address security incidents effectively.
- Legal and Regulatory Expertise: Seek legal and compliance expertise when interpreting complex regulatory requirements.
- Continous Improvement: Continously evaluate and improve security and compliance measures based on lessons learnt from audits, incidents and industry development.

6 What are you auditing within the IT infrastructure?

The specific elements audited within IT infrastructure may include:

- Network Security
  Firewalls, routers, switches to ensure protection against unauthorized access.
- Access Control
  Evaluation of user access management, authorization & authentication.
- Data Protection
  Access data encryption practices, data classification and measures to safeguard sensitive information.

- Vulnerability Management
  Review vulnerability management and patch management processes.
- End point security.
  Assessment of antivirus software and end point security controls
- Application Security
  Analysis including secure coding practices, web application firewalls etc..
- Third-Party Vendor Assessment
  Examine security practices of third party vendors & service providers.
- Audit Trails and Records
  Confirmations that comprehensive audit trail and records are generated.
- Regulatory Reporting.
  Documentation of compliance efforts and audit results to demonstrate adherence to regulatory requirements.

Explain planning and implementation of an IT infrastructure Audit for compliance

- Define Scope for Audit
  - Objective definition
  - Scope limitations
  - Stakeholder Engagement
  - Scope Documents
- Identifying Critical Requirement for Audit
  - Regulatory Requirement
    Determine which standards are relevant to audit
  - Organizational Goals
    Ensure audit aligns with organization's objectives
  - Risk Assessment
    Conduct risk assessment and prioritize audit areas based on their risk levels
  - Industry Best Practices
    Refer industry best practices and framework like NIST or ISO27001
- Assessing IT Security
  - Risk Analysis
    Perform comprehensive risk analysis to identify vulnerabilities and potential impacts on IT security.

- Security Controls
  Evaluate the effectiveness of existing security controls in place.
- Security Testing
  Conduct vulnerability assessment and penetration testing to identify weakness
- Incident History
  Review the organization's incident history to identify recurring security incidents

- Obtaining Informations, documentation and Resources.
  - Data Collection
    Gather relevant informations, documents and datasources related to audit scope.
  - Access Permission
    Ensure audit team has relevant access permissions and credentials to review system & data.
  - Resource Allocation.
    Allocate relevant resources including personnel, tools and equipments to conduct audit effectively.
  - Communication
    Maintain open communication through out the process.

What are controls and Why are they important?

Security controls are actions taken or automated software or hardware applications or process that reduce security risks.

Control activities are policies and procedures that helps to ensure management directives are carried out.

Controls are essential for several reasons:

- Risk Mitigation : control helps to mitigate security risk by reducing the likelihood and impact of security incidents
- Data Protection: Safeguard sensitive and critical data ensuring data confidentiality and integrity.

- Business Continuity
  They support disaster recovery and incident response effort.
- Compliance
  Many regulations require organizations to implement specific controls to meet compliance requirements.
- Security Policy Enforcement
  Controls enforces security policies and procedures established by the organization
- Detection and Response
  Some controls like IDS and security monitoring enable the early detection of security incidents allowing timely response and mitigation.
- Auditing and Accountability
  Enable auditing and logging of activities providing a record of system events.

Explain the IT audit process and types of audits.

IT audit process involves systematic evaluation of an organization's information technology systems, processes, policies and controls to ensure that they align with established standards and business objectives. The IT audit process follows the given steps :

- Planning
  Define scope and objectives
  Identify key IT systems assets and risks to be assessed.
  Determine audit methodology
  Gather necessary resources
- Execution
  Data Collection
  Analysis and assessment
  Testing depending on scope
  Documentation to keep detailed records

- Reporting
  - Prepare audit report
  - Recommendation for improvements
  - Executive summary
  - Action Plan with timelines and responsibilities.

Types of IT Audit

- Compliance Audit
  - Assess whether organization complies internal policies or regulations
  - less expensive and less time consuming
  - Cannot always identify security weakness that attackers exploit.
- Penetration Audit
  - Designed to simulate real world attacks and identify vulnerabilities that could be exploited.
  - Expensive and time consuming
  - Offer more comprehensive assessment of an organization's security state
- Risk Assessment Audit
  - Identifying potential threats and assessing the likelihood that the threat will materialize
  - Useful in identifying potential security problem.
  - Cannot always provide complete picture of organization's security.

What is Computer Assisted Audit Techniques and application for CAAT?

CAAT or Computer Assisted Audit Techniques is a set of tools and techniq used by auditors to perform audit and examinations of financial statement and other accounting records with assistance of computer software.

It helps auditors gather, analyze and interpret data more effectively and accurately than traditional manual methods.

Application controls for CAATs involve specific controls embedded within system that auditors utilize to ensure accuracy, completeness, security of data processing.
Some application controls used with CAATs include:

- Input controls: Verify the accuracy and completeness of data entered to system
- Processing Controls: Ensure accuracy and integrity of data processing within applications.
- Output Controls: Validate accuracy and completeness of data generated by application.

1. Explain Seven Domains of a Typical IT infrastructure in details.

- User Domain
  - Includes all individuals who has access to an organization's information system
  - It is important to have security policies that define user responsibilities, account management, password policies and acceptable use of resources
  - Policies in this domain should address employee training regarding security practices
  - Risks

    User can destroy data in app [intentionally or not] and delete all
- Workstation domain
  - Workstations including desktops, laptops and mobile devices falls under this.
  - Security policies should cover end point security, encryption, patch management, secure remote access.
  - Policies should also address the use of personal device for work related activities
  - Risk

    The workstation's OS can have a known software vulnerability which allows a hacker to connect remotely and steal data.

- Local Area Network Domain
  - Encompasses the network infrastructure within an organization.
  - Security policies should define network segmentation, access control, wireless network security and monitoring of network traffic for intrusions/anomalies
  - Risk
    A worm can spread through LAN and infect all computers in it.
- Wide Area Network Domain
  - Consist of internet and semiprivate lines.
  - Appropriate policies and procedures should be there to support compliance like for network access, data handling, incident response.
  - Risk
    Service provider can have major network outage.
- LAN to WAN Domain
  - The boundary between trusted and untrusted zone.
  - The zones are filtered with a firewall
  - Risk
    Weak ingress/egress traffic filtering can degrade performance.
- Remote Access Domain
  - A mobile user can access the local network remotely usually through VPN.
  - Security policies should address secure communication protocols, authentication of remote users, protection of data in transit
  - Risk
    Communication circuit outage can deny connection
- Application Domain
  - Relates to the servers and applications hosted by an organization.
  - Policies should include server hardening guidelines, access control, authentication mechanism and application security
  - Risk
    A DoS attack can cripple the organization's email
    A fire can destroy primary data.

12. How to identify the Minimum Acceptable Level of Risk and Appropriate Security in IT infrastructure?

- Prioritizes risk reduction.
- Raises awareness of potential hazards and risks on site.
- Identifies who/what may be at risk.
- Quantifies potential cost any risk entail.
- Highlights any short comings in existing risk reduction strategies
- Addresses the increase in risk over time.
- Provide clear risk information for both site personnel and the public.
- The level of residual risk that has been determined to be a reasonable level of potential loss/disruption for a specific IT system.

13 Define the following terms : a) Risk Analysis b) Risk Identification c) Risk Assessment d) Risk Response and Mitigation & e) Risk reporting

- Risk Analysis

It involves the systematic process of identifying, evaluating and analyzing potential risk and impact on an organization.

- Risk Identification

It is the initial step in risk management. This process involve gathering information, reviewing historical data, conducting interviews and utilizing various techniques to identify potential risks.

- Risk Assessment

Risk Assessment is the process of evaluating and prioritizing identified risk based on the likelihood of occurance and their potential impact.

- Risk Response and Mitigation

Refers to actions taken to address identified risks. It involves developing and implementing strategies to manage, reduce or eliminate risks

- Risk Reporting

  Involves communicating information about identified risks, their analysis, assessments and management strategies to relevant stakeholders.

14 Explain Business Continuity Planning and lifecycle of BCP

Business Continuity Planning is to help organization identify the impacts of potential data processing and operation disruptions and data loss, formulate recovery plans to ensure the availability of data processing and operational resources. It deals with the natural and man-made events and the consequences if not dealt with promptly and effectively. It helps to identify organization's exposure to internal and external threats.

The BCP addresses issues in terms of project scope and planning, business impact analysis, recovery strategies, recovery plan development and implementation

Lifecycle of BCP:

- Project Initiation

  Establish a project team and obtain management support

- Business Impact Analysis [BIA]

  Identify time-critical business processes and determine maximum outages

- Recovery Strategy

  Identify and select the recovery alternatives to meet the recovery time requirements.

- Plan, Design and Development

  Document the entire BCP outlining the strategies, procedures and protocols to be followed during and after a disruptive event.

- Implementation

  Implementing the BCP across the organization and establishing communication channels and protocols for activating the plan when needed.

- Testing

  Conducting simulation drills or tests to validate the effectiveness of BCP.

- Maintenance, Awareness and Training

  Monitor configuration management and update BCP accordingly

  BCP awareness on policy and procedure should be conducted annually for employees and contractors

15 Why Business Continuity Planning required.

- The Business Continuity Planning addresses the prexcuation of business in the face of major disruptions to normal business operations.
- It helps to identify the organization's exposure to internal and external threats
- It synthesize hard and soft assests to provide effective prevention and recovery for the organizaton and maintains competative advantage and value syster integrity.
- It counteracts interuptions to business activites and should be available to protect critical business processes from the effects of major failure.
- It deals with the natural and man-made events and consequences, if not dealt with promptly and effectively.

16 Define following terms: • Disaster Recovery • Compliances • Audit • IT security • System Monitoring • Log Analysis.

• Disaster Recovery

Refers to the proces and set of procedures an organizations implement to resume its critical business functions and IT systems after a disruptive event occurs. The goal is to minimize downtime.

• Compliance

The act of conforming to rules, regulations, laws or standards established by a governing body, organization or authority. Some examples are HIPAA, GDPR

• Audit

Examination of an organization's IT systems and controls to assess their effectiveness, security and compliance with regulations and best practices.

• IT security

Involves the protection of an organization's information technology systems, network, data and resources from unauthorized access, breaches, cyber threats and other potential risks

• System Monitoring

Proces of continuously observing and tracking the performance, health and behaviour of an organization's IT system, networks, application and infrastructure.

• Log analysis

Examination and interpretation of log data generated by IT systems, applications, servers, networks and devices.

17 Explain Disaster Recovery and planning of DR

A plan that provides detailed procedures to facilitate recovery of capabilities at an alternate site is called disaster recovery

The process of developing and maintaing a disaster recovery plan is called disaster recovery planning.

Recovery strategy focuses on:

- Meeting predetermined recovery time frames
- Maintaining the operation of the critical business functions
- Compiling the resource requirements
- Identifying alternatives that are available for recovery

8 How to identify potential disaster states of an organization?

- Risk Assessment

  Conduct a comprehensive risk assessment to identify potential threats that could disrupt business operation.

- Business Impact Analysis [BIA]

  Determine the impact of downtime, data loss, system unavailability and financial losses that could arise from different identified threats.

- Asset Identification

  Identify and prioritize critical assets.

- External Risk Factors

  Consider external risk factors such as regulatory changes, environmental factors, geopolitical risks. Assess how these could lead to potential disaster.

- Gap Analysis and Mitigation Strategies

  Conduct gap analysis to identify weakness or deficiencies in current disaster preparedness measures.

19 Explain DR strategies in detail.

The different disaster strategies are:

- Business recovery strategy

  It focuses on recovery of business operations
  Includes identifying critical business functions, establishing priorities and protocols to restore operations quickly.

- Facility and Supply Recovery strategy.

  Focuses on facility restoration and enables alternate recovery site.
  Ensure the availability of essential supplies or resources to resume.

- User Recovery Strategy.

  Focuses on people and accomodations
  Ensures employees have necessary accomodation, resources and support to continue working or returns to work efficiently.

- Technical Recovery Strategy.

  Focuses on recovery of IT services and infrastructure.
  Includes the plans for restoring hardwares, softwares, networks and ensuring their functionality to support business processes.

- Data Recovery Strategy.

  Focuses on recovery of information assets.
  Ensures availability and integrity of critical data.

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

- User Domain

  Security policy in this domain should cover user access controls, authentication password policies, user training on security practices, acceptable use of asset and incident reporting procedure.

- Workstation Domain.

  Security policies should focus on configuring and maintaining security softwares [antivirus, firewalls], enforcing access controls, implementing security patches and updates and securing physical access to devices. Policy should also addres the use of personal device for work related activities.

- Local Area Network Domain

  Security policy should define network segmentation, access control, wireless network security and monitoring of network traffic for anomalies / intrusions.

- Wide Area Network Domain

  Security policies should address VPN usage; to support compliance for network access, data handling, incident response.

The four risk management strategies are:

- Risk Control

focuses on reducing the likelihood or impact of the risk through proactive measures, safeguards or controls. If probability medium-high and impact low to medium level

eg:- Implementing security controls like firewall, antivirus software, IDS and encryption to reduce risk of cyber attacks and data breaches.

- Risk Avoid

This involves avoiding or eliminating the risk altogether by taking actions to prevent the risk from occuring or removing root cause of the risk. If probability as well as impact is medium to high level.

eg:- A company may decide not to enter a market known for political instability to avoid potential business disruption

- Risk Accept

When an organization acknowledges a risk but decides not to take action to mitigate it actively. Mostly chosen when cost of mitigation outweighs potential impact of risk. If probability and impact is low to medium level.

eg:- Accepting the risk of market fluctuation in stock market when investing in high risk, high return stocks without implementing any specific hedging strategies

- Risk Share

Transferring or sharing risk with other parties such as insurance companies to reduce the impact. If probability low to medium and impact is medium to high level

eg:- Purchasing insurance policies to cover potential losses from events like natural disaster, property damage or liability claims.

ANKIT