**Security Posture & Risk Assessment Interview Questions**

**1. General IT & Security Questions**

* What security frameworks does your organization follow (e.g., NIST, ISO 27001, CIS Controls)?
* How does your organization monitor and respond to security threats?
* What security tools are in place (SIEM, EDR, Firewalls, MFA)?
* What is the organization's approach to security awareness training?
* Are there documented security policies for employees? How often are they updated?

**2. Shadow IT & Unauthorized Applications**

* How does the organization identify and track unauthorized IT resources (Shadow IT)?
* Do employees use personal devices for work? If so, how is security enforced on them?
* What policies are in place to regulate the use of third-party cloud applications?
* Has the organization experienced security incidents related to Shadow IT? If so, how were they handled?

**3. Network & Data Security**

* How is network traffic monitored for potential threats and anomalies?
* What security measures are in place to protect critical data (encryption, backups, access control)?
* How often are security audits and vulnerability assessments conducted?
* Are there any known vulnerabilities or security gaps in the organization's IT infrastructure?
* How is data classified based on sensitivity and protected accordingly?

**4. Identity & Access Management (IAM)**

* What authentication methods are enforced (MFA, SSO, biometric authentication)?
* How is user access reviewed and managed, particularly for privileged accounts?
* Are inactive accounts regularly identified and removed?
* What processes are in place to ensure proper role-based access control (RBAC)?
* How does the organization handle employee offboarding to prevent unauthorized access?

**5. Incident Response & Compliance**

* What is the organization's protocol for handling security incidents?
* How quickly can the organization detect and respond to a security breach?
* What regulatory and compliance requirements apply to the organization (GDPR, HIPAA, PCI DSS)?
* How is compliance with security standards ensured and documented?
* Are penetration tests conducted regularly? If so, what were the most recent findings?

**6. Recommendations & Security Improvements**

* What are the biggest security challenges the organization currently faces?
* Are there any security enhancements planned for the near future?
* What additional security tools or practices would improve the organization's security posture?

*Prepared by:* [Mian Fazal ur Rehman]  
*Date:* [19th March 2025]