SAMA CONTROL DOMAIN 3.0 INTERVIEW QUESTIONS

1.What is Control Domain 3.0 in the SAMA Framework?

Answer: Control Domain 3.0 in the SAMA Framework focuses on the implementation and management of cybersecurity controls to protect information systems and data within financial institutions.

2.What are the primary objectives of Control Domain 3.0?

Answer: The primary objectives are to establish, implement, and maintain appropriate security measures to safeguard information assets, ensure data integrity, confidentiality, and availability, and comply with regulatory requirements.

3.What types of controls are included in Control Domain 3.0?

Answer: Control Domain 3.0 includes technical, administrative, and physical controls to protect against cybersecurity threats.

4.How does Control Domain 3.0 address access control?

Answer: It mandates the implementation of policies and mechanisms to manage user access rights, ensuring that only authorized individuals can access sensitive information and systems.

5.What is the role of encryption in Control Domain 3.0?

Answer: Encryption is used to protect data at rest and in transit, ensuring that sensitive information is unreadable to unauthorized users.

6.How does Control Domain 3.0 approach network security?

Answer: It includes measures such as firewalls, intrusion detection/prevention systems (IDS/IPS), and secure network design to protect against network-based threats.

7.What requirements does Control Domain 3.0 set for incident response?

Answer: It requires the establishment of an incident response plan, regular incident response drills, and mechanisms for detecting, reporting, and recovering from cybersecurity incidents.

8.How does Control Domain 3.0 ensure the security of third-party vendors?

Answer: It mandates the assessment and management of third-party risks, including due diligence, contractual security requirements, and ongoing monitoring of third-party compliance.

9.What is the importance of monitoring and logging under Control Domain 3.0?

Answer: Continuous monitoring and logging are critical for detecting suspicious activities, investigating incidents, and ensuring compliance with security policies.

10.How does Control Domain 3.0 handle data protection and privacy?

Answer: It requires implementing measures like data encryption, access controls, and data masking to protect sensitive information and comply with data privacy laws.

11.What are the audit requirements in Control Domain 3.0?

Answer: Regular internal and external audits are required to assess the effectiveness of cybersecurity controls, identify weaknesses, and ensure compliance with the framework.

12.How does Control Domain 3.0 address patch management?

Answer: It mandates timely application of security patches and updates to systems and applications to mitigate vulnerabilities.

13.What is the role of identity and access management (IAM) in Control Domain 3.0?

Answer: IAM ensures that only authenticated and authorized users can access specific resources, reducing the risk of unauthorized access.

14.How does Control Domain 3.0 support business continuity and disaster recovery?

Answer: It requires institutions to have business continuity and disaster recovery plans that include cybersecurity considerations to ensure resilience against disruptions.

15.What does Control Domain 3.0 say about physical security?

Answer: It includes measures to protect physical access to critical systems and data centers, such as security guards, access control systems, and surveillance.

16.How does Control Domain 3.0 approach the secure configuration of systems?

Answer: It requires that systems be securely configured according to industry best practices and regularly reviewed to ensure compliance.

17.What is the significance of user training and awareness in Control Domain 3.0?

Answer: Regular training and awareness programs are essential to ensure that employees understand security policies, recognize threats, and follow best practices.

18.How does Control Domain 3.0 address malware protection?

Answer: It requires the implementation of anti-malware solutions, regular updates, and monitoring to detect and prevent malware infections.

19.What are the requirements for secure software development in Control Domain 3.0?

Answer: It mandates secure coding practices, regular code reviews, and security testing to identify and mitigate vulnerabilities during the development process.

20.How does Control Domain 3.0 ensure email security?

Answer: It includes measures like spam filters, email encryption, and security awareness to protect against phishing and other email-based threats.