FRAMEWORK ORIENTATION INTERVIEW QUESTIONS

1.What is the SAMA Framework 1.1 in the context of cybersecurity?

Answer: The SAMA (Saudi Arabian Monetary Authority) Framework 1.1 is a set of guidelines and standards aimed at strengthening cybersecurity within financial institutions in Saudi Arabia.

2.How does SAMA define cybersecurity?

Answer: SAMA defines cybersecurity as the practice of protecting systems, networks, and programs from digital attacks aimed at accessing, changing, or destroying sensitive information, extorting money, or interrupting normal business processes.

3.What is the primary goal of the SAMA Framework in cybersecurity?

Answer: The primary goal of the SAMA Framework is to enhance the cybersecurity posture of financial institutions, ensuring the protection of information assets and maintaining the stability of the financial sector in Saudi Arabia.

4.What entities are covered under the scope of the SAMA Framework?

Answer: The scope of the SAMA Framework includes all financial institutions regulated by SAMA, such as banks, insurance companies, finance companies, and credit bureaus operating within Saudi Arabia.

5.Why is the SAMA Framework important for financial institutions?

Answer: The SAMA Framework is important because it provides a comprehensive approach to managing cybersecurity risks, ensuring that financial institutions implement robust security measures to protect against cyber threats.

6.What are the key components of the SAMA Framework?

Answer: Key components of the SAMA Framework include governance, risk management, cybersecurity controls, monitoring and response, awareness and training, and third-party management.

7.Who is responsible for implementing the SAMA Framework within an organization?

Answer: The implementation of the SAMA Framework is the responsibility of the organization’s executive management and cybersecurity professionals, with oversight from the board of directors.

8.How does the SAMA Framework define the roles and responsibilities of cybersecurity professionals?

Answer: The SAMA Framework outlines specific responsibilities for cybersecurity professionals, including developing and implementing cybersecurity policies, managing security risks, monitoring threats, and ensuring compliance with the framework’s requirements.

9.What is the SAMA Framework’s approach to risk management?

Answer: The SAMA Framework’s approach to risk management involves identifying, assessing, and mitigating cybersecurity risks through a structured process that includes regular risk assessments, implementing controls, and continuous monitoring.

10.What are the applicability criteria for the SAMA Framework?

Answer: The applicability criteria include all financial institutions regulated by SAMA, and the framework applies to all aspects of their operations, including IT systems, data, processes, and personnel.

11.What are the responsibilities of the board of directors under the SAMA Framework?

Answer: The board of directors is responsible for providing oversight, ensuring that adequate resources are allocated for cybersecurity, approving cybersecurity policies, and reviewing cybersecurity reports and risk assessments.

12.How does the SAMA Framework address third-party cybersecurity risks?

Answer: The SAMA Framework requires financial institutions to assess and manage cybersecurity risks associated with third-party service providers, including conducting due diligence, setting security requirements, and monitoring compliance.

13.What is the role of the Chief Information Security Officer (CISO) according to the SAMA Framework?

Answer: The CISO is responsible for overseeing the cybersecurity program, ensuring compliance with the SAMA Framework, leading incident response efforts, and reporting on cybersecurity to executive management and the board.

14.How does SAMA interpret compliance with its cybersecurity framework?

Answer: SAMA interprets compliance as the adherence to the guidelines, standards, and best practices outlined in the framework, requiring institutions to implement necessary controls and regularly demonstrate their effectiveness through audits and assessments.

15.Who is the target audience for the SAMA Framework?

Answer: The target audience includes executive management, board members, cybersecurity professionals, IT staff, and compliance officers within financial institutions regulated by SAMA.

16.What kind of training and awareness programs does the SAMA Framework recommend?

Answer: The SAMA Framework recommends comprehensive training and awareness programs for all employees, covering cybersecurity policies, threat awareness, best practices, and incident response procedures.

17.How does the SAMA Framework ensure continuous improvement in cybersecurity?

Answer: The framework promotes continuous improvement through regular risk assessments, audits, incident reviews, and updates to cybersecurity policies and controls based on emerging threats and technological advancements.

18.What are the reporting requirements under the SAMA Framework?

Answer: Financial institutions must regularly report on their cybersecurity posture, incidents, risk assessments, and compliance status to SAMA, ensuring transparency and accountability.

19.How does the SAMA Framework align with international cybersecurity standards?

Answer: The SAMA Framework aligns with international standards such as ISO/IEC 27001, NIST Cybersecurity Framework, and other globally recognized best practices, ensuring a comprehensive and effective approach to cybersecurity.

20.What measures does the SAMA Framework suggest for incident response?

Answer: The framework suggests measures including establishing an incident response plan, conducting regular drills, having clear communication protocols, and ensuring rapid detection, containment, and recovery from cybersecurity incidents.

21.How does the SAMA Framework address data protection and privacy?

Answer: The framework mandates the implementation of strong data protection measures, including encryption, access controls, data loss prevention, and compliance with relevant data privacy regulations.

22.What is the significance of governance in the SAMA Framework?

Answer: Governance is crucial as it ensures that cybersecurity is integrated into the organizational culture, with clear roles, responsibilities, policies, and oversight mechanisms to manage cybersecurity risks effectively.

23.How are financial institutions expected to handle cybersecurity audits under the SAMA Framework?

Answer: Financial institutions are expected to conduct regular internal and external cybersecurity audits to assess compliance with the framework, identify gaps, and implement corrective actions.

24.What are the consequences of non-compliance with the SAMA Framework?

Answer: Non-compliance can lead to regulatory penalties, increased vulnerability to cyber threats, reputational damage, and potential financial losses for the institution.

25.How does the SAMA Framework facilitate collaboration among financial institutions?

Answer: The framework encourages information sharing and collaboration among financial institutions, including sharing threat intelligence, best practices, and participating in industry-wide cybersecurity initiatives.