Cybersecurity Intern (GRC Team) - Viva Preparation

1. What is GRC in cybersecurity?

Answer: GRC stands for Governance, Risk, and Compliance. It's a strategy for managing governance (policies and decision-making), risk (identifying and mitigating threats), and compliance (adhering to laws and regulations).

2. Why is GRC important?

Answer: It aligns cybersecurity with business goals, ensures regulatory compliance, reduces risk, and protects the organization's reputation.

3. What's the difference between governance and compliance?

Answer: Governance defines the policies and strategy, while compliance is the act of following internal and external rules and regulations.

4. What are internal controls in GRC?

Answer: Policies, procedures, and tools used to ensure risks are managed and regulatory requirements are met.

5. What is a risk assessment?

Answer: The process of identifying, analyzing, and evaluating risks to the organization's information assets.

6. What is a risk register?

Answer: A document that lists identified risks, their severity, mitigation measures, and responsible owners.

7. Define inherent risk and residual risk.

Answer: Inherent risk is the natural risk without controls; residual risk is what remains after controls are applied.

8. What is a security policy?

Answer: A formal document outlining rules and practices for securing an organization's assets.

9. What is a control in cybersecurity?

Answer: A safeguard or countermeasure to mitigate risks, such as access controls or encryption.

10. What is a compliance audit?

Answer: A check to ensure the organization is adhering to applicable policies, standards, and regulations.

11. What is ISO/IEC 27001?

Answer: An international standard for managing information security through an Information Security Management System (ISMS).

12. What are the key domains in ISO 27001 Annex A?

Answer: Organizational, People, Physical, and Technological domains, containing 93 controls.

13. What is the difference between ISO 27001 and ISO 27002?

Answer: 27001 defines requirements for an ISMS; 27002 provides implementation guidance for security controls.

14. What is SOC 2?

Answer: A framework for managing customer data based on five Trust Service Criteria: Security, Availability, Processing Integrity, Confidentiality, and Privacy.

15. Difference between SOC 1, SOC 2, and SOC 3?

Answer: SOC 1 focuses on financial reporting; SOC 2 on data security; SOC 3 is a simplified, public version of SOC 2.

16. What is PCI DSS?

Answer: A standard for securing credit card information. Organizations handling cardholder data must comply.

17. What is GDPR?

Answer: A European regulation governing data protection and privacy for individuals in the EU.

18. What is CMMI?

Answer: Capability Maturity Model Integration, a framework for improving business processes.

19. What is COBIT?

Answer: A framework for developing, implementing, monitoring, and improving IT governance and management practices.

20. What is the Essential 8?

Answer: An Australian framework of eight mitigation strategies to improve cybersecurity posture.

21. What is a Statement of Applicability (SoA)?

Answer: A document listing all ISO 27001 controls, showing which are implemented and justification for exclusions.

22. What is an ISMS?

Answer: Information Security Management System, a framework of policies and procedures for systematically managing information risks.

23. What is data classification?

Answer: The process of labeling data based on sensitivity, such as Public, Internal, Confidential, and Restricted.

24. What are administrative, technical, and physical controls?

Answer: Administrative: policies; Technical: encryption; Physical: locked rooms, CCTV.

25. What is a vulnerability vs. threat vs. risk?

Answer: Vulnerability: weakness; Threat: potential cause of harm; Risk: likelihood and impact of a threat exploiting a vulnerability.

26. What is a business continuity plan (BCP)?

Answer: A plan to ensure essential functions can continue during and after a disaster.

27. What is incident response?

Answer: The process of identifying, managing, and recovering from security incidents.

28. What is the CIA Triad?

Answer: Confidentiality, Integrity, and Availability - the core principles of cybersecurity.

29. What is a data subject and data controller under GDPR?

Answer: Data subject: individual whose data is collected. Data controller: entity that determines why and how data is processed.

30. What are privacy by design and default?

Answer: Principles of embedding privacy into systems from the start and limiting data collection by default.

31. What is an IS Audit?

Answer: A systematic evaluation of IT systems to ensure compliance, security, and effectiveness.

32. What are the steps of a risk management process?

Answer: Identify, Analyze, Evaluate, Treat, Monitor risks.

33. What is a vulnerability assessment vs. penetration test?

Answer: VA identifies known issues; Pen test simulates attacks to find real-world exploitable flaws.

34. What are risk treatment options?

Answer: Accept, Avoid, Transfer, or Mitigate the risk.

35. What is segregation of duties (SoD)?

Answer: A principle ensuring no single individual controls all aspects of a critical process, reducing fraud risk.

36. What is a policy, standard, procedure, and guideline?

Answer: Policy: high-level rule; Standard: specific rule; Procedure: how to follow rules; Guideline: recommendation.

37. What is access control?

Answer: Ensuring only authorized users can access certain data or systems.

38. What is the purpose of encryption in compliance?

Answer: To protect data confidentiality and integrity during storage and transmission.

39. What is audit logging?

Answer: Recording system activities to track and review actions and detect issues.

40. What is multi-factor authentication (MFA)?

Answer: Using two or more verification methods (e.g., password + OTP) for secure access.

41. If you find a control not working during an audit, what do you do?

Answer: Document it, assess impact, report to responsible team, and suggest corrective actions.

42. How would you help an organization achieve ISO 27001 certification?

Answer: Assist with ISMS implementation, risk assessments, documentation, internal audits, and training.

43. What is phishing and how does GRC address it?

Answer: Phishing is a social engineering attack. GRC combats it via policies, training, and incident response.

44. Why is documentation important in GRC?

Answer: It provides proof of compliance, ensures consistency, and helps during audits.

45. What is a corrective action plan?

Answer: A documented plan to fix non-compliance issues or failures found during audits.

46. How do you stay updated on compliance standards?

Answer: By reading official documentation, attending webinars, and following industry blogs.

47. What is asset inventory in GRC?

Answer: A list of all IT assets that helps in identifying, assessing, and managing security risks.

48. What is change management in cybersecurity?

Answer: A process to ensure changes are tested, documented, and do not compromise security.

49. What is the role of training in compliance?

Answer: It ensures staff understand policies, reduces risk of human error, and maintains awareness.

50. What qualities make a good GRC professional?

Answer: Detail-oriented, strong communicator, analytical, knowledgeable of standards, and eager to learn.