IT Audit & Security Question Bank

1. **What are the key steps involved in defining the scope for an IT audit, and why is scope definition critical to audit success?**
2. **Explain how to identify critical requirements for an IT audit. What factors should be considered when prioritizing audit areas?**
3. **Describe the process of assessing IT security during the audit planning phase. What preliminary assessments should be conducted?**
4. **What are the primary sources for obtaining information during an IT audit? Discuss both internal and external information sources.**
5. **How does the audit scope impact resource allocation and timeline planning? Provide examples.**
6. **Explain the relationship between business objectives and audit scope definition. How should auditors align their scope with organizational priorities?**
7. **What are the seven domains of a typical IT infrastructure? Briefly describe each domain.**
8. **How do you map an IT security policy framework to the seven domains of IT infrastructure? Provide examples for at least three domains.**
9. **What types of documentation are essential for conducting an effective IT audit? Categorize them by purpose.**
10. **Explain the importance of resource planning in IT audits. What types of resources (human, technical, financial) are typically required?**
11. **Describe how security policies should be tailored differently for each of the seven IT infrastructure domains.**
12. **What challenges might auditors face when mapping security policies to infrastructure domains, and how can these be overcome?**
13. **How does documentation support the audit trail and evidence collection process? Provide specific examples.**
14. **What is the process for identifying monitoring requirements in an IT environment? What factors influence these requirements?**
15. **Describe various testing methodologies used to validate monitoring controls. Compare at least three different approaches.**
16. **How do you determine the adequacy of existing monitoring controls? What metrics or criteria should be used?**

17. **Explain the difference between continuous monitoring and periodic testing. When is each approach appropriate?**
18. **What are common gaps in monitoring implementations, and how can auditors identify them during testing?**
19. **Describe the relationship between monitoring requirements and incident response capabilities.**
20. **Define goal-based security controls and provide three examples. What are their advantages and limitations?**
21. **Define implementation-based security controls and provide three examples. How do they differ from goal-based controls?**
22. **Compare and contrast goal-based versus implementation-based security controls. In what scenarios is each approach more effective?**
23. **How do goal-based controls support compliance with multiple regulatory frameworks simultaneously?**
24. **Explain how implementation-based controls can be more precise but potentially less flexible than goal-based controls.**
25. **Discuss the concept of compensating controls. How do they relate to goal-based and implementation-based approaches?**
26. **What role does risk assessment play in choosing between goal-based and implementation-based security controls?**
27. **Describe the security control formulation and development process from initial concept to implementation.**
28. **What are the key phases in the security control development lifecycle? Explain each phase.**
29. **How does security architecture design set the stage for control implementation? Provide specific examples.**
30. **Explain the importance of threat modeling in the control development process.**
31. **What principles of secure design should be incorporated during security architecture development?**
32. **How do you ensure that security controls are aligned with business processes and not just technical requirements?**
33. **What is a multitiered governance and control framework? Describe its typical layers or tiers.**

34. **How do you implement a multitiered governance framework in a business environment? What are the critical success factors?**
35. **Explain the relationship between corporate governance, IT governance, and security governance in a multitiered framework.**
36. **What are the benefits and challenges of implementing a multitiered control framework?**
37. **Describe how different organizational levels (board, executive, operational) interact within a governance framework.**
38. **Outline the components of a comprehensive IT audit plan. What elements must be included?**
39. **Describe the typical IT audit process from planning through reporting. What are the key milestones?**
40. **Compare and contrast three different types of IT audits (e.g., compliance audit, operational audit, integrated audit).**
41. **What is the difference between internal and external IT audits? How do their objectives and approaches differ?**
42. **Explain the role of risk assessment in audit planning. How does it influence audit prioritization?**
43. **Describe the audit closing process, including findings validation, management response, and follow-up activities.**
44. **What are Computer-Assisted Audit Techniques (CAATs)? Explain their purpose and benefits in IT auditing.**
45. **Describe how CAATs are used for sampling. What are the advantages of computerized sampling over manual methods?**
46. **Explain how CAATs can be applied to application reviews. Provide examples of specific techniques.**
47. **How are CAATs used for auditing application controls? Describe at least three specific applications.**
48. **Compare different types of CAATs such as test data methods, embedded audit modules, and generalized audit software.**
49. **What are the limitations and risks associated with using CAATs? How can auditors mitigate these risks?**

50. **Discuss the skills and training required for auditors to effectively utilize CAATs in their audit engagements.**
51. **How do you identify the minimum acceptable level of risk for an organization? What frameworks or methodologies can be used?**
52. **What is a security baseline definition? How does it relate to the minimum acceptable level of risk?**
53. **Describe the process of establishing appropriate security baseline definitions for each of the seven domains of IT infrastructure.**
54. **Explain the concept of risk appetite and risk tolerance. How do these influence security baseline decisions?**
55. **How should security baselines be customized based on industry, regulatory requirements, and organizational context?**
56. **Describe the process for reviewing and updating security baselines over time. How often should this occur and what triggers updates?**