◇ EASY (Q1–Q10)

Q1. Cyber Security Auditing is primarily concerned with evaluating:
A. Network performance
B. Effectiveness of security controls
C. Software development speed
D. User productivity

Q2. Which principle ensures that audit findings are unbiased and reliable?
A. Confidentiality
B. Integrity
C. Objectivity
D. Independence

Q3. Which of the following best defines compliance?
A. Risk elimination
B. Adherence to laws and standards
C. Security automation
D. Incident prevention

Q4. Internal security audits are mainly conducted to:
A. Satisfy regulators
B. Improve internal controls
C. Replace external audits
D. Certify the organization

Q5. Which audit type is performed by an independent third party?
A. Internal audit
B. Self-assessment
C. External audit
D. Operational audit

Q6. The CIA triad in information security stands for:
A. Control, Integrity, Audit
B. Confidentiality, Integrity, Availability
C. Compliance, Investigation, Assurance
D. Cybersecurity, Infrastructure, Access

Q7. Audit evidence should be:
A. Verbal only
B. Assumption-based
C. Objective and verifiable
D. Informal

Q8. Which role has the ultimate responsibility for cybersecurity governance?
A. IT administrators
B. External auditors
C. Board of Directors
D. Security analysts

Q9. Which phase of an audit focuses on defining scope and objectives?
A. Execution
B. Reporting
C. Planning
D. Follow-up

Q10. Auditor independence primarily helps in ensuring:
A. Faster audits
B. Cost reduction
C. Credibility of findings
D. Technical accuracy

◇ MEDIUM (Q11–Q25)

Q11. Which factor MOST influences the frequency of a security audit?
A. Organization size
B. Risk exposure
C. Number of employees
D. IT budget

Q12. Compliance audits mainly focus on:
A. Risk prioritization
B. Regulatory adherence
C. Threat modeling
D. Penetration testing

Q13. A risk-based audit approach primarily emphasizes:
A. Equal review of all controls
B. High-impact risk areas
C. Random control selection
D. Past audit reports only

Q14. Which audit phase involves collecting and analyzing evidence?
A. Planning
B. Initiation
C. Execution
D. Closure

Q15. Lack of documentation during an audit most directly affects:
A. Availability
B. Audit reliability
C. System uptime
D. Compliance cost

Q16. Which is a key challenge faced by modern cybersecurity audits?
A. Static threats
B. Skilled workforce surplus
C. Rapidly evolving threat landscape
D. Excessive regulations

Q17. Which of the following BEST differentiates security audit from security assessment?
A. Audit is informal
B. Assessment focuses on compliance only
C. Audit provides formal assurance
D. Assessment is mandatory

Q18. Auditor professional skepticism refers to:
A. Distrust of management
B. Questioning audit evidence critically
C. Avoiding assumptions
D. Following audit checklists strictly

Q19. Which principle ensures audit findings are supported by facts?
A. Confidentiality
B. Evidence-based approach
C. Due care
D. Integrity

Q20. Which stakeholder benefits MOST directly from audit assurance?
A. Attackers
B. Regulators and management
C. End users only
D. Developers

Q21. Operational audits mainly assess:
A. Financial statements
B. Process efficiency and effectiveness
C. Network vulnerabilities
D. Regulatory compliance

Q22. Which factor determines audit scope the MOST?
A. Auditor preference
B. Legal mandates and risk
C. Employee feedback
D. Available tools

Q23. An internal audit team should primarily report to:
A. IT department
B. Security operations
C. Audit committee / Board
D. System administrators

Q24. Which is NOT a core audit principle under ISO guidelines?
A. Integrity
B. Confidentiality
C. Scalability
D. Fair presentation

Q25. Ethical responsibility of auditors includes:
A. Ignoring minor issues
B. Reporting material risks objectively
C. Supporting management decisions
D. Limiting audit scope unnecessarily

△ HARD (Q26–Q40)

Q26. Which scenario BEST illustrates audit decision factors influencing scope?
A. Auditing all systems equally
B. Focusing on critical systems after a breach
C. Reviewing only documented controls
D. Ignoring third-party risks

Q27. A compliance-driven organization with weak risk management is MOST likely to:
A. Be secure
B. Meet all security objectives
C. Experience control failures
D. Eliminate cyber threats

Q28. Which limitation is inherent to cybersecurity audits?
A. Lack of standards
B. Snapshot-in-time assessment
C. No management involvement
D. Unlimited scope

Q29. Auditor independence is compromised when:
A. Auditor has technical expertise
B. Auditor reports to the board
C. Auditor participates in system design
D. Audit follows standards

Q30. Which audit phase ensures accountability for remediation?
A. Planning
B. Execution
C. Reporting
D. Follow-up

Q31. An organization meeting compliance but suffering frequent breaches indicates:
A. Effective governance
B. Over-compliance
C. Compliance ≠ security
D. Excessive audits

Q32. Which challenge MOST affects audits in cloud-based organizations?
A. Static infrastructure
B. Clear asset ownership
C. Shared responsibility ambiguity
D. Reduced attack surface

Q33. Which auditor ability is MOST critical when evaluating management assertions?
A. Technical scripting
B. Professional skepticism
C. Speed of execution
D. Report formatting

Q34. A risk-based audit would prioritize which asset?
A. Public website
B. Archived systems
C. Core banking database
D. Training portal

Q35. Which failure most commonly leads to audit findings being rejected?
A. Complex language
B. Lack of sufficient evidence
C. Use of standards
D. Stakeholder involvement

Q36. Which audit type BEST supports continuous improvement?
A. Regulatory audit
B. External audit
C. Internal audit
D. Certification audit

Q37. Auditor objectivity is BEST maintained by:
A. Familiarity with systems
B. Management guidance
C. Independence and ethics
D. Tool-based audits

Q38. Which governance failure MOST increases cyber audit findings?
A. Strong board oversight
B. Poor risk appetite definition
C. Clear policies
D. Regular audits

Q39. Which audit outcome MOST supports executive decision-making?
A. Raw logs
B. Vulnerability scans
C. Risk-ranked findings
D. System diagrams

Q40. The PRIMARY value of cybersecurity auditing is:
A. Eliminating all threats
B. Ensuring reasonable assurance
C. Replacing security controls
D. Automating compliance