? EASY (Q1–Q10)

Q1. Cyber security auditing primarily evaluates:
A. Network speed
B. Effectiveness of security controls
C. Software performance
D. User productivity

Q2. Which framework is BEST known for IT governance?
A. NIST CSF
B. COBIT
C. CIS Controls
D. PCI DSS

Q3. GDPR mainly protects:
A. Organizations
B. Networks
C. Personal data of individuals
D. Software licenses

Q4. ISO/IEC 27001 focuses on establishing a:
A. Firewall architecture
B. Risk-based ISMS
C. Compliance checklist
D. Network security tool

Q5. PCI DSS applies to organizations that:
A. Store HR data
B. Process cardholder data
C. Use cloud services
D. Are publicly listed

Q6. HIPAA protects which type of information?
A. Intellectual property
B. Financial statements
C. Protected Health Information
D. Software code

Q7. NIST CSF is BEST described as:
A. A regulation
B. A certification
C. A risk-based framework
D. A legal mandate

Q8. COBIT distinguishes clearly between:
A. Security and privacy
B. Governance and management
C. Risk and audit
D. Policy and controls

Q9. CIS Controls are developed by:
A. ISO
B. ISACA
C. Center for Internet Security
D. AICPA

Q10. DPDP Act 2023 is a:
A. Security standard
B. Technical framework
C. Privacy legislation
D. Compliance checklist

□ MEDIUM (Q11–Q25)

Q11. The primary goal of cyber security auditing is to:
A. Detect hackers
B. Provide assurance on control effectiveness
C. Replace penetration testing
D. Eliminate all risks

Q12. Which audit type is performed by an independent external body?
A. Internal audit
B. Operational audit
C. External audit
D. Management review

Q13. Risk-based auditing prioritizes controls based on:
A. Cost
B. Likelihood and impact
C. Auditor preference
D. Vendor recommendations

Q14. ISO/IEC 27001 uses which improvement model?
A. Agile
B. Waterfall
C. PDCA
D. DevOps

Q15. NIST CSF “Identify” function primarily focuses on:
A. Incident response
B. Asset and risk understanding
C. Recovery planning
D. Monitoring threats

Q16. GDPR “right to be forgotten” refers to:
A. Data anonymization
B. Data erasure
C. Data encryption
D. Data portability

Q17. SOX Section 404 focuses on:
A. Cybercrime
B. Internal control effectiveness
C. Data privacy
D. Vendor risk

Q18. SOC 2 reports are based on:
A. ISO clauses
B. Trust Services Criteria
C. COBIT objectives
D. PCI controls

Q19. COBIT goals cascade helps organizations:
A. Improve network security
B. Translate business goals into IT goals
C. Perform audits
D. Automate compliance

Q20. HIPAA Security Rule safeguards are categorized into:
A. Legal and technical
B. Administrative, physical, technical
C. Preventive and detective
D. Network and system

Q21. PCI DSS compliance levels depend on:
A. Organization size
B. Transaction volume
C. Number of systems
D. Revenue

Q22. CIS Benchmarks mainly provide:
A. Risk models
B. Secure configuration standards
C. Legal guidance
D. Audit templates

Q23. SSE-CMM evaluates security at the level of:
A. Tools
B. Controls
C. Organizational processes
D. Individual users

Q24. IT Act Section 43A mandates:
A. Encryption usage
B. Reasonable security practices
C. Mandatory audits
D. Certification

Q25. Internal audit independence ensures:
A. Faster audits
B. Objective assessment
C. Reduced scope
D. No findings

🔴 HARD (Q26–Q40)

Q26. A compliant organization with poor security maturity MOST likely follows:
A. Risk-based governance
B. Checklist-driven compliance
C. Optimized controls
D. Predictive assurance

Q27. Which framework is CERTIFIABLE?
A. NIST CSF
B. COBIT
C. ISO/IEC 27001
D. CIS Controls

Q28. Which GDPR principle MOST supports ethical data processing?
A. Availability
B. Consent and transparency
C. Encryption
D. Portability

Q29. Treating PCI DSS purely as a checklist MOST often leads to:
A. Optimized payment security
B. Superficial compliance
C. Reduced fraud
D. Certification exemption

Q30. NIST CSF Implementation Tiers represent:
A. Network layers
B. Control categories
C. Risk management maturity
D. Compliance levels

Q31. COBIT vs ITIL comparison shows that ITIL focuses MORE on:
A. Governance
B. Risk optimization
C. Service management
D. Enterprise oversight

Q32. HIPAA penalties are tiered based on:
A. Revenue
B. Level of negligence
C. Number of patients
D. Type of system

Q33. SSE-CMM MOST strongly reinforces which principle?
A. Zero Trust
B. Security by design
C. Encryption everywhere
D. Incident-driven security

Q34. A global bank audit is MOST complex due to:
A. Network size
B. Multi-jurisdiction regulations
C. Hardware diversity
D. Tool limitations

Q35. DPDP Act places primary accountability on:
A. Data Principals
B. Data Fiduciaries
C. Regulators
D. Vendors

Q36. CIS Controls differ from ISO 27001 mainly because they are:
A. Governance-focused
B. Prescriptive and prioritized
C. Certifiable
D. Legal mandates

Q37. SOX compliance MOST directly supports which governance goal?
A. Availability
B. Transparency and accountability
C. Performance optimization
D. Encryption

Q38. Security evaluation differs from audit by emphasizing:
A. Compliance verification
B. Control effectiveness and maturity
C. Legal enforcement
D. Certification

Q39. Anti-corruption compliance audits primarily assess:
A. Firewall rules
B. Ethical conduct and bribery risks
C. Data encryption
D. Backup procedures

Q40. The PRIMARY objective common to all governance frameworks is to:
A. Eliminate cyber threats
B. Provide reasonable assurance
C. Replace regulations
D. Automate security