

❖ EASY (Q1–Q10)

Q1. The Sarbanes–Oxley Act (SOX) was enacted primarily to:

- A. Improve network security
- B. Protect investors and ensure financial integrity
- C. Regulate cloud computing
- D. Certify IT systems

Q2. SOX applies mainly to:

- A. All private companies
- B. Publicly traded companies
- C. Government organizations
- D. Educational institutions

Q3. Which SOX section focuses on management responsibility for internal controls?

- A. Section 201
- B. Section 302
- C. Section 802
- D. Section 906

Q4. SOC reports are issued under standards defined by:

- A. ISO
- B. NIST
- C. AICPA
- D. PCI SSC

Q5. Which SOC report focuses on controls over financial reporting?

- A. SOC 1
- B. SOC 2
- C. SOC 3
- D. SOC 4

Q6. SOX compliance primarily emphasizes:

- A. Operational efficiency
- B. Financial reporting integrity
- C. Network performance
- D. Software quality

Q7. SOC reports are primarily intended for:

- A. General public
- B. Internal IT teams only
- C. Customers and regulators
- D. Hackers

Q8. Which framework is commonly used to assess internal controls under SOX?

- A. ITIL
- B. COBIT
- C. COSO
- D. NIST CSF

Q9. SOX requires retention of audit records for a minimum of:

- A. 2 years
- B. 3 years
- C. 5 years
- D. 7 years

Q10. Which entity enforces SOX compliance?

- A. ISO
 - B. SEC
 - C. PCI SSC
 - D. HHS
-

◊ MEDIUM (Q11–Q25)

Q11. Section 404 of SOX requires management to:

- A. Eliminate all risks
- B. Assess and report on internal control effectiveness
- C. Perform penetration testing
- D. Certify network security

Q12. Which SOC report is based on Trust Services Criteria?

- A. SOC 1
- B. SOC 2
- C. SOC 3
- D. SOC for Cybersecurity

Q13. SOC 2 Trust Services Criteria include all EXCEPT:

- A. Security
- B. Availability
- C. Confidentiality
- D. Financial accuracy

Q14. Which SOC report is suitable for public distribution?

- A. SOC 1 Type II
- B. SOC 2 Type II
- C. SOC 3
- D. SOC 1 Type I

Q15. Which internal control component relates to ethical values and integrity?

- A. Risk Assessment
- B. Monitoring
- C. Control Environment
- D. Information & Communication

Q16. Which SOX requirement MOST directly impacts IT controls?

- A. Section 302
- B. Section 404
- C. Section 409
- D. Section 802

Q17. SOC Type II reports differ from Type I reports because they:

- A. Focus only on design
- B. Cover operating effectiveness over time
- C. Are uncertified
- D. Are informal

Q18. Which role signs off on SOX Section 302 certifications?

- A. IT Manager
- B. External Auditor
- C. CEO and CFO
- D. Compliance Officer

Q19. Which SOX section addresses criminal penalties for document tampering?

- A. Section 302
- B. Section 404
- C. Section 409
- D. Section 802

Q20. Which scenario BEST requires a SOC 1 report?

- A. Cloud email service
- B. Payroll processing service
- C. Website hosting provider
- D. Antivirus vendor

Q21. SOX compliance failures MOST often result in:

- A. Technical downtime
- B. Legal and financial penalties
- C. Reduced system speed
- D. Fewer audits

Q22. Internal controls under SOX are designed to provide:

- A. Absolute assurance
- B. Reasonable assurance
- C. Zero fraud guarantee
- D. Technical perfection

Q23. Which governance body oversees SOX compliance within an organization?

- A. IT department
- B. Audit committee
- C. Security operations
- D. HR department

Q24. SOC reports primarily support which risk area?

- A. Market risk
- B. Third-party risk
- C. Physical risk
- D. Environmental risk

Q25. SOX compliance strengthens which governance principle MOST?

- A. Transparency and accountability
 - B. Availability
 - C. Performance optimization
 - D. Automation
-

△ HARD (Q26–Q40)

Q26. A company compliant with SOX but lacking IT access controls MOST likely faces:

- A. No risk
- B. Increased financial reporting risk
- C. Improved security
- D. Audit exemption

Q27. Which failure MOST undermines reliability of SOX reports?

- A. Excessive documentation
- B. Weak internal controls
- C. External audits
- D. Control automation

Q28. SOC reports do NOT:

- A. Provide assurance on controls
- B. Replace customer due diligence
- C. Support vendor risk management
- D. Enhance transparency

Q29. Which factor MOST influences the scope of a SOX audit?

- A. Auditor preference
- B. Financial reporting risk
- C. IT infrastructure size
- D. Number of employees

Q30. Which control is MOST critical for SOX compliance in ERP systems?

- A. Backup controls
- B. Access and segregation of duties
- C. Antivirus deployment
- D. Encryption only

Q31. An organization relying only on SOC reports without internal controls MOST likely:

- A. Achieves compliance
- B. Transfers accountability
- C. Retains responsibility for controls
- D. Eliminates audit scope

Q32. Which governance weakness MOST increases SOX audit findings?

- A. Strong board oversight
- B. Poor documentation of controls
- C. Regular monitoring
- D. Automated controls

Q33. SOC reports complement SOX by addressing:

- A. Financial audits only
- B. Third-party control assurance
- C. Internal employee behavior
- D. Incident response

Q34. Which SOX-related risk increases with extensive outsourcing?

- A. Reduced compliance effort
- B. Loss of accountability
- C. Improved assurance
- D. Lower audit costs

Q35. Which statement BEST reflects the limitation of SOC reports?

- A. They are legally binding
- B. They cover a point-in-time (Type I) or limited period
- C. They eliminate vendor risk
- D. They certify security

Q36. Which SOX control failure MOST often leads to material weaknesses?

- A. Minor policy gaps
- B. Ineffective change management
- C. Antivirus issues
- D. Training delays

Q37. SOX and COSO frameworks are related because COSO:

- A. Replaces SOX
- B. Provides the internal control model used by SOX
- C. Certifies organizations
- D. Is optional

Q38. Which SOX section requires timely disclosure of material changes?

- A. Section 302
- B. Section 404
- C. Section 409
- D. Section 802

Q39. A SOC 2 report with security and availability criteria MOST benefits:

- A. Payroll processors
- B. Cloud service providers
- C. Accounting firms
- D. Stock exchanges

Q40. The PRIMARY objective of SOX is to:

- A. Improve cybersecurity maturity
- B. Ensure trust in financial reporting
- C. Replace IT governance
- D. Eliminate fraud completely