◇ EASY (Q1–Q10)

Q1. ISO/IEC 27001 primarily specifies requirements for:
A. Network security tools
B. Information Security Management System (ISMS)
C. Software development lifecycle
D. Cloud service certification

Q2. The ISO/IEC 2700x series mainly deals with:
A. Software quality
B. Information security standards
C. Financial auditing
D. Data analytics

Q3. Which standard in the ISO/IEC 2700x family is certifiable?
A. ISO/IEC 27002
B. ISO/IEC 27003
C. ISO/IEC 27001
D. ISO/IEC 27005

Q4. The core objective of ISO/IEC 27001 is to ensure:
A. Maximum encryption
B. Risk-based information security
C. Zero cyber incidents
D. Tool standardization

Q5. ISO/IEC 27001 is applicable to:
A. Only IT companies
B. Only government organizations
C. Organizations of all types and sizes
D. Only cloud service providers

Q6. Which concept forms the foundation of ISO/IEC 27001?
A. Compliance checklist
B. Risk management
C. Incident response
D. Network segmentation

Q7. ISMS stands for:
A. Integrated Security Management System
B. Information Security Management System
C. Internal System Management Standard
D. Internet Security Monitoring Service

Q8. Which property is NOT part of the CIA triad emphasized in ISO 27001?
A. Confidentiality
B. Integrity
C. Availability
D. Accountability

Q9. ISO/IEC 27001 focuses primarily on:
A. Technical controls only
B. Management system and governance
C. Software testing
D. Penetration testing

Q10. ISO/IEC 27001 certification provides:
A. Absolute security guarantee
B. Risk-based assurance
C. Legal immunity
D. Technical accreditation

◇ MEDIUM (Q11–Q25)

Q11. The ISMS lifecycle in ISO/IEC 27001 is based on which model?
A. Waterfall
B. Agile
C. PDCA (Plan–Do–Check–Act)
D. Spiral

Q12. Risk assessment in ISO/IEC 27001 is used to:
A. Eliminate all risks
B. Identify and evaluate information security risks
C. Select vendors
D. Automate security

Q13. Which document maps selected controls to identified risks?
A. Risk register
B. Statement of Applicability (SoA)
C. Security policy
D. Audit plan

Q14. Which ISO/IEC 27001 clause emphasizes leadership responsibility?
A. Context of organization
B. Leadership
C. Support
D. Operation

Q15. ISO/IEC 27002 mainly provides:
A. ISMS requirements
B. Control implementation guidance
C. Certification criteria
D. Audit rules

Q16. Management commitment in ISO/IEC 27001 is critical because it:
A. Reduces audit time
B. Ensures governance and accountability
C. Eliminates risks
D. Replaces controls

Q17. Which activity is part of the “Check” phase of PDCA?
A. Risk treatment
B. Control implementation
C. Internal audit and monitoring
D. Asset identification

Q18. ISO/IEC 27001 requires organizations to:
A. Implement all controls
B. Select controls based on risk
C. Follow a fixed checklist
D. Use specific tools

Q19. Which concept ensures continuous improvement in ISO/IEC 27001?
A. Certification audit
B. Risk elimination
C. PDCA cycle
D. External compliance

Q20. ISO/IEC 27001 aligns MOST closely with which governance objective?
A. Performance optimization
B. Risk management and assurance
C. System automation
D. Cost reduction

Q21. Which domain existed in ISO/IEC 27001:2005 but was later restructured?
A. Asset management
B. Security policy
C. Business continuity management
D. All of the above

Q22. Surveillance audits in ISO/IEC 27001 are conducted to:
A. Reissue certificates
B. Ensure ongoing ISMS effectiveness
C. Redesign controls
D. Perform penetration tests

Q23. Which role typically owns information security risk in ISO 27001?
A. External auditor
B. Risk owner within the organization
C. Certification body
D. IT vendor

Q24. The main output of an ISO/IEC 27001 audit is:
A. Vulnerability report
B. Audit findings and assurance
C. Incident logs
D. Configuration baselines

Q25. ISO/IEC 27001 documentation is required mainly to:
A. Satisfy auditors only
B. Demonstrate control and accountability
C. Increase paperwork
D. Replace technical controls

△ HARD (Q26–Q40)

Q26. Which scenario BEST reflects ISO/IEC 27001's risk-based approach?
A. Implementing all controls regardless of context
B. Selecting controls based on business risk assessment
C. Following vendor recommendations
D. Applying identical controls across all departments

Q27. An organization certified to ISO/IEC 27001 but experiencing a breach indicates that:
A. Certification guarantees security
B. Risk management failed conceptually
C. Certification provides reasonable assurance, not immunity
D. Audits are ineffective

Q28. Which key difference distinguishes ISO/IEC 27001 from NIST CSF?
A. Risk focus
B. Governance orientation
C. Certification capability
D. Control mapping

Q29. The Statement of Applicability (SoA) is MOST critical because it:
A. Lists all possible controls
B. Justifies control inclusion or exclusion
C. Acts as an audit checklist
D. Replaces risk assessment

Q30. Which governance failure MOST undermines ISO/IEC 27001 effectiveness?
A. Regular audits
B. Lack of top management support
C. Risk documentation
D. Control monitoring

Q31. Continuous improvement in ISO/IEC 27001 requires:
A. Static risk treatment
B. Periodic review and corrective actions
C. One-time certification
D. Tool replacement

Q32. Which aspect of ISO/IEC 27001 MOST supports regulatory compliance?
A. Certification logo
B. Risk-based control selection
C. Fixed control list
D. Automation

Q33. An organization treating ISO 27001 as a checklist MOST likely results in:
A. Optimized security posture
B. Superficial compliance
C. Improved assurance
D. Reduced audit findings

Q34. Which clause ensures alignment of ISMS with business objectives?
A. Support
B. Operation
C. Context of organization
D. Improvement

Q35. ISO/IEC 27001 integrates information security into governance by requiring:
A. Technical audits only
B. Management reviews and accountability
C. Vendor certification
D. External enforcement

Q36. Which control domain in ISO/IEC 27001:2005 focused on incident handling?
A. Access control
B. Information security incident management
C. Communications management
D. Compliance

Q37. ISO/IEC 27001 certification lifecycle MOST closely aligns with:
A. One-time validation
B. Continuous assurance model
C. Penetration testing cycle
D. Software release cycle

Q38. Which factor MOST influences control selection in ISO/IEC 27001?
A. Auditor preference
B. Risk assessment outcomes
C. Budget only
D. Industry trends

Q39. Which statement BEST reflects ISO/IEC 27001's limitation?
A. It is outdated
B. It cannot be audited
C. It does not guarantee breach prevention
D. It lacks governance focus

Q40. The PRIMARY value of ISO/IEC 27001 certification is:
A. Tool standardization
B. Risk-based information security assurance
C. Regulatory exemption
D. Zero incidents