◇ EASY (Q1–Q10)

Q1. The CIS Critical Security Controls are developed by:
A. ISO
B. NIST
C. Center for Internet Security
D. ISACA

Q2. CIS Controls primarily focus on:
A. Legal compliance
B. Prioritized cyber defense actions
C. Financial auditing
D. Software development

Q3. CIS Controls are best described as:
A. Certification standards
B. Prescriptive best practices
C. Legal requirements
D. Vendor tools

Q4. CIS Controls are applicable to:
A. Only government organizations
B. Only large enterprises
C. Organizations of all sizes
D. Only cloud providers

Q5. CIS Controls are MOST effective when implemented using a:
A. Tool-centric approach
B. Risk-based approach
C. Random approach
D. Compliance-only approach

Q6. CIS Controls are designed primarily to help organizations:
A. Eliminate all cyber risks
B. Prevent, detect, and respond to attacks
C. Replace governance frameworks
D. Avoid audits

Q7. CIS Controls are organized into how many high-level controls (current versions)?
A. 12
B. 15
C. 18
D. 20

Q8. Which term refers to specific actions within a CIS Control?
A. Categories
B. Domains
C. Safeguards
D. Clauses

Q9. CIS Controls are updated based on:
A. Academic theory only
B. Vendor feedback
C. Real-world threat data
D. Legal mandates

Q10. CIS Controls are primarily aimed at reducing:
A. Compliance cost
B. Attack surface
C. Network latency
D. Storage usage

◇ MEDIUM (Q11–Q25)

Q11. CIS Implementation Groups (IGs) are used to:
A. Certify organizations
B. Classify control complexity
C. Align controls with organizational maturity
D. Replace risk assessments

Q12. Which Implementation Group represents basic cyber hygiene?
A. IG0
B. IG1
C. IG2
D. IG3

Q13. CIS Controls emphasize “know what you have” through which control area?
A. Data protection
B. Asset inventory and management
C. Incident response
D. Logging and monitoring

Q14. CIS Benchmarks primarily address:
A. Network architecture design
B. Secure configuration baselines
C. Legal compliance
D. Risk appetite

Q15. CIS Controls are MOST useful for organizations that:
A. Have unlimited budgets
B. Need prioritized security actions
C. Require certification
D. Want to replace audits

Q16. Which CIS Control category focuses on detecting security events?
A. Access control
B. Logging and monitoring
C. Data recovery
D. Asset inventory

Q17. CIS Compliance is best described as:
A. Mandatory legal adherence
B. Voluntary alignment with best practices
C. Certification requirement
D. Regulatory enforcement

Q18. CIS Controls complement NIST CSF by providing:
A. Governance structure
B. Prescriptive safeguards
C. Legal authority
D. Certification

Q19. CIS Benchmarks are best used during:
A. Software development
B. System configuration and hardening
C. Financial audits
D. Incident response

Q20. Which CIS Control MOST directly supports incident response capability?
A. Inventory of assets
B. Incident response management
C. Secure configuration
D. Email protection

Q21. CIS Controls are often mapped to which frameworks?
A. ISO, NIST, PCI DSS
B. TCP/IP model only
C. OSI model
D. ITIL only

Q22. Which Implementation Group is suitable for organizations handling sensitive data?
A. IG1 only
B. IG2
C. IG3
D. IG0

Q23. CIS Controls primarily address which type of security posture?
A. Reactive only
B. Preventive only
C. Preventive, detective, and corrective
D. Administrative only

Q24. CIS Benchmarks are developed through:
A. Vendor mandates
B. Community consensus
C. Regulatory enforcement
D. Proprietary research

Q25. Which challenge MOST affects CIS Controls adoption?
A. Lack of frameworks
B. Resource constraints
C. Excessive certification
D. Legal restrictions

🔺 HARD (Q26–Q40)

Q26. Which scenario BEST demonstrates the value of CIS Controls over a generic framework?
A. Legal compliance reporting
B. Prioritizing controls based on active attack trends
C. Annual audit preparation
D. Certification audits

Q27. An organization implementing IG1 only MOST likely aims to:
A. Achieve full maturity
B. Establish basic cyber hygiene
C. Protect national infrastructure
D. Eliminate all risks

Q28. Which limitation MOST distinguishes CIS Controls from ISO/IEC 27001?
A. Risk-based approach
B. Governance focus
C. Lack of certification
D. Control mapping

Q29. CIS Controls effectiveness depends MOST on:
A. Number of tools deployed
B. Quality of implementation and prioritization
C. Certification audits
D. Legal enforcement

Q30. CIS Benchmarks help reduce which type of vulnerability MOST?
A. Social engineering
B. Configuration-based vulnerabilities
C. Insider threats
D. Regulatory gaps

Q31. Which governance weakness MOST undermines CIS Controls adoption?
A. Strong leadership
B. Lack of asset inventory
C. Absence of risk ownership
D. Regular monitoring

Q32. CIS Controls support continuous improvement by:
A. Static requirements
B. Threat-driven updates
C. Annual certification
D. Fixed control sets

Q33. Which CIS Control area MOST supports forensic investigations?
A. Asset management
B. Secure configuration
C. Logging and audit trails
D. Email security

Q34. CIS Controls are MOST effective when integrated with:
A. Only technical tools
B. Governance and risk management frameworks
C. Vendor contracts
D. Legal compliance programs only

Q35. Treating CIS Controls as a checklist MOST likely results in:
A. Improved cyber resilience
B. Superficial implementation
C. Optimized governance
D. Reduced audit findings

Q36. Which CIS Control MOST directly reduces lateral movement risk?
A. Network segmentation and access control
B. Backup and recovery

C. Security awareness training
D. Incident response

Q37. CIS Controls maturity progression MOST closely resembles:
A. OSI model
B. Capability maturity models
C. Network layers
D. SDLC phases

Q38. CIS Controls help boards MOST by:
A. Providing technical configurations
B. Translating cyber risk into prioritized actions
C. Eliminating audits
D. Guaranteeing security

Q39. Which statement BEST reflects CIS Controls' role in compliance?
A. They replace regulations
B. They support and map to regulations
C. They are legally binding
D. They enforce penalties

Q40. The PRIMARY objective of CIS Critical Security Controls is to:
A. Replace cybersecurity frameworks
B. Provide prioritized, effective cyber defense
C. Guarantee zero incidents
D. Ensure certification