? EASY (Q1–Q10)

Q1. Information security management primarily focuses on:
A. Hardware maintenance
B. Protecting information assets
C. Software development
D. Network performance

Q2. Which factor is considered the weakest link in security?
A. Hardware
B. Software
C. Network
D. Human

Q3. Social engineering attacks mainly exploit:
A. Encryption weaknesses
B. Human behavior
C. Network protocols
D. Hardware faults

Q4. Malware is an example of:
A. Physical threat
B. Logical threat
C. Environmental threat
D. Natural threat

Q5. Which security objective ensures data accuracy?
A. Confidentiality
B. Integrity
C. Availability
D. Authentication

Q6. A threat is best defined as:
A. A system weakness
B. A potential cause of harm
C. An implemented control
D. A security policy

Q7. Which document defines acceptable security behavior?
A. Audit report
B. Security policy
C. Incident log
D. Threat register

Q8. Insider threats originate from:
A. External hackers
B. Trusted internal users
C. Unknown attackers
D. Internet bots

Q9. Phishing is classified as a:
A. Physical attack
B. Network attack
C. Social engineering attack
D. Hardware attack

Q10. Which framework is widely used for security governance?
A. TCP/IP
B. ISO 27001
C. HTTP
D. DNS

□ MEDIUM (Q11–Q25)

Q11. The human side of security includes:
A. Firewalls and IDS
B. Policies and training
C. Encryption algorithms
D. Network topology

Q12. Awareness training primarily helps to reduce:
A. Malware creation
B. Social engineering attacks
C. Hardware failure
D. Network latency

Q13. External cyber threats originate from:
A. Employees
B. Contractors
C. Internet-based attackers
D. Internal auditors

Q14. Which attack spreads malicious code without user interaction?
A. Trojan
B. Worm
C. Phishing
D. Spyware

Q15. Threat classification helps organizations to:
A. Improve performance
B. Prioritize risks
C. Eliminate all threats
D. Encrypt systems

Q16. Network-based attacks primarily target:
A. Human psychology
B. Communication channels
C. Physical infrastructure
D. Policies

Q17. Application-based attacks exploit:
A. Business logic and code flaws
B. Network routing
C. Power supply
D. Environmental conditions

Q18. Risk assessment evaluates:
A. Asset value only
B. Threat likelihood and impact
C. Vulnerability count only
D. Security tools

Q19. Which is an example of logical threat?
A. Fire
B. Flood
C. Virus infection
D. Earthquake

Q20. Ransomware primarily affects:
A. Confidentiality
B. Integrity
C. Availability
D. Authentication

Q21. Policies in security management are:
A. Optional guidelines
B. Mandatory rules
C. Technical tools
D. Monitoring systems

Q22. Which attack uses deceptive messages to steal information?
A. Sniffing
B. Phishing
C. Flooding
D. Spoofing

Q23. Threat severity depends on:
A. Number of users
B. Likelihood and impact
C. Code size
D. System speed

Q24. Risk management lifecycle includes:
A. Risk identification
B. Risk mitigation
C. Risk monitoring
D. All of the above

Q25. Which security objective ensures system uptime?
A. Confidentiality
B. Integrity
C. Availability
D. Authorization

🟥 HARD (Q26–Q40)

Q26. Human factor risks are difficult to control because they:
A. Are predictable
B. Depend on behavior and awareness
C. Are hardware-based
D. Use encryption

Q27. Social engineering attacks are effective because they:
A. Exploit software bugs
B. Bypass technical controls
C. Require malware
D. Depend on encryption flaws

Q28. Malware introduced via email attachments is an example of:
A. Physical threat
B. Logical threat
C. Environmental threat
D. Natural threat

Q29. Threat modeling in security management helps to:
A. Eliminate all attacks
B. Identify threat sources and impacts
C. Configure firewalls automatically
D. Encrypt sensitive data

Q30. Which control type focuses on reducing attack impact after occurrence?
A. Preventive
B. Detective
C. Corrective
D. Administrative

Q31. Security culture in an organization refers to:
A. Use of antivirus
B. Employee attitudes toward security
C. Network architecture
D. Encryption strength

Q32. Insider threats are especially dangerous because insiders:
A. Lack access
B. Have legitimate privileges
C. Are always malicious
D. Use advanced malware

Q33. Classification of threats improves:
A. Network speed
B. Risk prioritization
C. Hardware utilization
D. Application performance

Q34. Which type of threat exploits trust relationships?
A. Network attacks
B. Social engineering
C. Physical attacks
D. Environmental threats

Q35. Security governance ensures alignment between:
A. Security and performance
B. Security and business objectives
C. Security and hardware
D. Security and software versions

Q36. Malware, phishing, and ransomware are categorized as:
A. Physical threats
B. Logical threats
C. Environmental threats
D. Natural threats

Q37. Human error contributes significantly to:
A. Zero-day exploits
B. Security breaches
C. Network latency
D. Hardware failures

Q38. Effective threat management requires:
A. One-time assessment
B. Continuous monitoring
C. No documentation
D. Ignoring low risks

Q39. Which attack specifically targets user trust?
A. Buffer overflow
B. SQL Injection
C. Social engineering
D. DoS

Q40. Security awareness programs aim to:
A. Replace technical controls
B. Eliminate malware
C. Reduce human-related risks
D. Improve system performance