◇ EASY (Q1–Q10)

Q1. Information Security primarily aims to protect:
A. Only hardware resources
B. Only software applications
C. Information assets
D. Network bandwidth

Q2. Which of the following represents the core objectives of Information Security?
A. AAA Model
B. CIA Triad
C. OSI Model
D. TCP/IP Model

Q3. Confidentiality in the CIA triad ensures:
A. Data is always available
B. Data is not modified
C. Data is accessed only by authorized users
D. Data is backed up

Q4. Integrity refers to:
A. Preventing unauthorized access
B. Ensuring data accuracy and consistency
C. Ensuring system uptime
D. Encrypting communication

Q5. Availability ensures that information is:
A. Encrypted at rest
B. Accessible when required
C. Hidden from attackers
D. Authenticated

Q6. A vulnerability is best described as:
A. A malicious action
B. A system weakness
C. A potential attacker
D. A security policy

Q7. Which of the following is an example of a threat?
A. Unpatched operating system
B. Weak password
C. Malware attack
D. Misconfigured firewall

Q8. Risk is the result of:
A. Threat only

B. Vulnerability only
C. Threat exploiting vulnerability
D. Asset value only

Q9. QoS primarily focuses on:
A. Data confidentiality
B. Network performance
C. Malware detection
D. User authentication

Q10. Which QoS metric measures delay in packet delivery?
A. Throughput
B. Jitter
C. Latency
D. Packet loss

◇ MEDIUM (Q11–Q25)

Q11. Which security objective is most affected by a Denial-of-Service attack?
A. Confidentiality
B. Integrity
C. Availability
D. Authentication

Q12. Why is Information Security considered a business requirement?
A. It improves hardware speed
B. It reduces software cost
C. It minimizes financial and reputational loss
D. It increases internet bandwidth

Q13. Which factor directly influences the cost of a security breach?
A. Number of users
B. Duration of downtime
C. Network topology
D. Programming language

Q14. Which organization publishes the OWASP Top 10?
A. ISO
B. IEEE
C. OWASP
D. NIST

Q15. From a security perspective, internet statistics help organizations to:
A. Increase bandwidth

B. Predict attack trends
C. Improve coding speed
D. Reduce CPU usage

Q16. Which of the following best represents the risk equation?
A. Risk = Threat + Asset
B. Risk = Vulnerability + Impact
C. Risk = Threat × Vulnerability × Impact
D. Risk = Threat − Control

Q17. An unpatched web server exposed to the internet represents:
A. Threat
B. Vulnerability
C. Risk
D. Asset

Q18. Which QoS metric represents variation in packet delay?
A. Latency
B. Throughput
C. Jitter
D. Bandwidth

Q19. High packet loss in a network most directly affects:
A. Data confidentiality
B. Application performance
C. Encryption strength
D. User authentication

Q20. Which of the following tools is commonly used for vulnerability scanning?
A. Wireshark
B. OpenVAS
C. Nagios
D. tcpdump

Q21. Which factor is NOT part of security ROI calculation?
A. Cost of security controls
B. Loss avoided
C. Risk reduction
D. Programming effort

Q22. Which QoS metric reflects actual data transfer rate?
A. Bandwidth
B. Latency
C. Throughput
D. Jitter

Q23. Antivirus software mainly addresses which security goal?
A. Confidentiality
B. Integrity
C. Availability
D. All of the above

Q24. Which of the following best describes a threat actor?
A. Weak system configuration
B. Malicious entity
C. Security control
D. Network protocol

Q25. Why is risk never completely eliminated?
A. Security tools are expensive
B. Threats constantly evolve
C. Networks are slow
D. Users lack training

🔺 HARD (Q26–Q40)

Q26. An organization accepts a known security risk because mitigation cost is higher than potential loss. This is known as:
A. Risk avoidance
B. Risk mitigation
C. Risk transfer
D. Risk acceptance

Q27. Which scenario best represents a vulnerability without an immediate threat?
A. Ransomware infection
B. Exposed service with no exploit available
C. Active DDoS attack
D. Credential theft

Q28. Why does high latency severely affect VoIP services?
A. Encryption fails
B. Packet size increases
C. Real-time communication is disrupted
D. Authentication is delayed

Q29. From a security economics perspective, ROI is best used to:
A. Measure attack frequency
B. Justify security investments
C. Replace risk assessment
D. Detect intrusions

Q30. Which QoS parameter is most critical for video conferencing?
A. Throughput only
B. Jitter and latency
C. Packet loss only
D. Bandwidth only

Q31. Which combination most accurately reflects Information Security goals?
A. Speed, Cost, Quality
B. Prevention, Detection, Recovery
C. Confidentiality, Integrity, Availability
D. Authentication, Authorization, Accounting

Q32. A zero-day exploit primarily increases which component of risk?
A. Asset value
B. Threat likelihood
C. Vulnerability exposure
D. Control effectiveness

Q33. Why is risk assessment considered a continuous process?
A. Logs expire
B. Attacks never stop evolving
C. Hardware fails frequently
D. Bandwidth changes

Q34. Which security breach cost is hardest to quantify?
A. Legal penalties
B. Incident response cost
C. Reputational damage
D. Hardware replacement

Q35. In QoS workflows, traffic classification occurs before:
A. Packet capture
B. Scheduling and queuing
C. Transmission medium selection
D. Encryption

Q36. Which lab activity directly helps analyze QoS parameters?
A. Antivirus scan
B. OpenVAS scan
C. Wireshark packet capture
D. Firewall rule creation

Q37. Why does increased bandwidth alone not guarantee better QoS?
A. Latency may still exist
B. Encryption becomes weak

C. Routing tables increase
D. Firewalls block traffic

Q38. A threat exploiting multiple vulnerabilities increases:
A. Availability
B. Control efficiency
C. Overall risk
D. Asset value

Q39. Which security principle ensures accountability?
A. Confidentiality
B. Non-repudiation
C. Availability
D. Integrity

Q40. Why is Information Security considered a strategic investment?
A. It eliminates all attacks
B. It improves hardware lifespan
C. It reduces long-term business loss
D. It replaces compliance requirements