◇ EASY (Q1–Q10)

Q1. Security evaluation primarily focuses on assessing the:
A. Cost of security tools
B. Effectiveness of security controls
C. Speed of system performance
D. Number of incidents

Q2. Security evaluation differs from auditing mainly because it emphasizes:
A. Compliance reporting
B. Control effectiveness and maturity
C. Financial accuracy
D. Regulatory penalties

Q3. Assurance in security evaluation refers to:
A. Guarantee of zero breaches
B. Degree of confidence in controls
C. Automation of controls
D. Elimination of risk

Q4. Which element is assessed FIRST in a security evaluation?
A. Controls
B. Risks
C. Assets and scope
D. Incident response

Q5. Security evaluation outcomes are MOST useful for:
A. Hackers
B. End users only
C. Management and governance bodies
D. Developers

Q6. Which term refers to remaining risk after controls are applied?
A. Inherent risk
B. Residual risk
C. Compliance risk
D. Audit risk

Q7. Evaluation methodology provides:
A. Technical tools
B. A structured assessment approach
C. Incident response plans
D. Penetration testing steps

Q8. Security evaluation is BEST described as:
A. A one-time activity
B. A continuous governance process
C. A technical scan
D. A legal requirement

Q9. Which assurance level reflects undocumented and informal controls?
A. Optimized
B. Managed
C. Ad hoc
D. Predictive

Q10. Security evaluation is MOST closely aligned with:
A. Software testing
B. Risk management
C. Financial accounting
D. Network optimization

◇ MEDIUM (Q11–Q25)

Q11. Which activity distinguishes security evaluation from compliance audits?
A. Evidence collection
B. Risk-based prioritization
C. Documentation review
D. Policy verification

Q12. A risk-based security evaluation prioritizes controls based on:
A. Cost of implementation
B. Auditor preference
C. Likelihood and impact of threats
D. Number of users

Q13. Which evaluation phase involves gap identification?
A. Planning
B. Assessment
C. Analysis
D. Reporting

Q14. Which assurance level indicates standardized and documented controls?
A. Repeatable
B. Defined
C. Managed
D. Optimized

Q15. Evaluation methodologies are MOST effective when they are:
A. Tool-driven
B. Risk-aligned
C. Compliance-only
D. Incident-based

Q16. Which factor MOST influences selection of evaluation methodology?
A. Organization size
B. Auditor certification
C. Risk profile
D. IT budget

Q17. Security evaluation supports governance primarily by:
A. Replacing audits
B. Providing confidence to stakeholders
C. Enforcing penalties
D. Reducing IT costs

Q18. Which of the following BEST represents an evaluation process flow?
A. Detect → Protect → Recover
B. Scope → Assess → Analyze → Assure
C. Design → Build → Test
D. Identify → Patch → Deploy

Q19. Evaluation evidence should be:
A. Informal and verbal
B. Subjective
C. Objective and documented
D. Assumed

Q20. Which assurance level reflects proactive and anticipatory security?
A. Defined
B. Managed
C. Predictive
D. Repeatable

Q21. Security evaluation maturity is MOST closely related to:
A. Number of tools deployed
B. Process consistency and control
C. Network speed
D. User satisfaction

Q22. Which role benefits MOST directly from assurance reporting?
A. Security attackers
B. System users
C. Board and senior management
D. Developers

Q23. Evaluation phases help reduce:
A. Security cost
B. Subjectivity in assessments
C. Audit frequency
D. Compliance scope

Q24. Which approach focuses on control design and operation?
A. Threat-based evaluation
B. Control-based evaluation
C. Incident-based evaluation
D. Cost-based evaluation

Q25. Security evaluation outcomes typically feed into:
A. Marketing strategy
B. Risk registers and governance reviews
C. Software design documents
D. End-user training only

🔺 HARD (Q26–Q40)

Q26. Which scenario BEST demonstrates security evaluation rather than audit?
A. Checking compliance with a regulation
B. Measuring control effectiveness across maturity levels
C. Verifying policy existence
D. Performing certification assessment

Q27. An organization at “Managed” assurance level is MOST likely to have:
A. Informal controls
B. Measured and monitored controls
C. No documentation
D. Reactive security only

Q28. Continuous assurance implies:
A. Annual evaluation
B. Event-driven audits
C. Near real-time confidence in controls
D. Elimination of evaluation

Q29. Which limitation is inherent to security evaluation?
A. Lack of frameworks
B. Dependence on evaluator judgment
C. No governance value
D. Mandatory certification

Q30. Security evaluation complements audits by focusing on:
A. Regulatory penalties
B. Effectiveness and improvement
C. Legal enforcement
D. Certification scope

Q31. A highly compliant organization with low assurance maturity indicates:
A. Strong governance
B. Compliance-driven security
C. Optimized controls
D. Predictive risk handling

Q32. Which evaluation level reflects institutionalized continuous improvement?
A. Defined
B. Managed
C. Optimized
D. Repeatable

Q33. Risk-based evaluation is MOST beneficial when resources are:
A. Unlimited
B. Fixed and constrained
C. Abundant
D. Irrelevant

Q34. Which evaluation focus BEST supports strategic decision-making?
A. Tool performance
B. Risk-ranked assurance outcomes
C. Technical vulnerabilities only
D. Incident logs

Q35. Which governance weakness MOST reduces assurance credibility?
A. Clear documentation
B. Lack of management involvement
C. Risk ownership
D. Control monitoring

Q36. Security evaluation maturity levels are MOST similar to:
A. Network layers
B. Capability maturity models
C. Compliance checklists
D. Audit phases

Q37. Which factor MOST differentiates “Defined” from “Managed” assurance levels?
A. Presence of policies
B. Measurement and monitoring
C. Documentation
D. Awareness training

Q38. Evaluation methodology selection that ignores risk context will MOST likely result in:
A. Optimized security
B. Ineffective assurance
C. Lower costs
D. Faster evaluation

Q39. Security evaluation findings are MOST valuable when they are:
A. Tool-generated
B. Risk-prioritized and contextualized
C. Generic
D. Confidential only

Q40. The PRIMARY objective of security evaluation is to:
A. Replace audits
B. Certify compliance
C. Provide confidence in security effectiveness
D. Eliminate cyber threats