◇ EASY (Q1–Q10)

Q1. SSE-CMM stands for:
A. Secure Software Engineering Capability Model
B. Systems Security Engineering – Capability Maturity Model
C. Security Services Evaluation Capability Model
D. Software Security Enhancement Control Model

Q2. SSE-CMM primarily focuses on:
A. Network penetration testing
B. Security engineering process maturity
C. Compliance certification
D. Incident response automation

Q3. SSE-CMM is MOST closely related to which type of model?
A. OSI model
B. Capability maturity model
C. Network architecture model
D. Risk assessment model

Q4. SSE-CMM was developed to address security in:
A. Operational systems only
B. Software coding only
C. Systems engineering lifecycle
D. Network devices only

Q5. SSE-CMM evaluates security capability at the level of:
A. Individual tools
B. Technical controls
C. Organizational processes
D. Single applications

Q6. SSE-CMM maturity focuses on improving:
A. Technology speed
B. Security processes and practices
C. Hardware performance
D. Audit frequency

Q7. SSE-CMM is BEST described as:
A. A compliance regulation
B. A maturity assessment framework
C. A technical security standard
D. A certification authority

Q8. SSE-CMM primarily supports which security discipline?
A. Network security
B. Systems security engineering
C. Application testing
D. Digital forensics

Q9. SSE-CMM is MOST useful for organizations that want to:
A. Achieve ISO certification quickly
B. Improve security engineering capability
C. Replace audits
D. Eliminate cyber risks

Q10. SSE-CMM focuses on security as a:
A. Technical add-on
B. End-user responsibility
C. Engineering discipline
D. Compliance requirement

◇ MEDIUM (Q11–Q25)

Q11. The primary goal of SSE-CMM is to:
A. Identify vulnerabilities
B. Measure and improve security engineering processes
C. Enforce regulations
D. Automate controls

Q12. SSE-CMM maturity levels indicate:
A. Number of tools deployed
B. Degree of process capability
C. Compliance score
D. Risk rating

Q13. SSE-CMM assesses security practices across:
A. Isolated departments
B. Entire systems lifecycle
C. Network perimeter only
D. Incident response phase

Q14. Which organization type MOST benefits from SSE-CMM?
A. Small retail shops
B. Organizations developing complex systems
C. Individual developers
D. End users

Q15. SSE-CMM differs from ISO 27001 because it focuses MORE on:
A. Certification
B. Governance controls
C. Engineering process maturity
D. Legal compliance

Q16. Which activity is central to SSE-CMM assessments?
A. Penetration testing
B. Process evaluation
C. Configuration hardening
D. Log analysis

Q17. SSE-CMM supports security governance by:
A. Enforcing penalties
B. Providing process capability insights
C. Eliminating audits
D. Issuing certifications

Q18. SSE-CMM maturity improvement is achieved through:
A. One-time assessment
B. Continuous process improvement
C. Tool replacement
D. Annual audits only

Q19. SSE-CMM primarily addresses which security dimension?
A. Technical safeguards
B. Process capability
C. Legal compliance
D. User behavior

Q20. Which concept is fundamental to SSE-CMM?
A. Defense-in-depth
B. Capability maturity
C. Zero trust
D. Encryption

Q21. SSE-CMM assessments are MOST useful for identifying:
A. Software bugs
B. Process strengths and weaknesses
C. Malware infections
D. Regulatory gaps

Q22. SSE-CMM can be applied during which phase of system development?
A. Design only
B. Implementation only
C. Entire system lifecycle
D. Deployment only

Q23. SSE-CMM maturity results are BEST used to:
A. Replace audits
B. Plan process improvements
C. Certify compliance
D. Enforce discipline

Q24. SSE-CMM encourages security to be:
A. Reactive
B. Tool-driven
C. Built-in from early stages
D. Outsourced

Q25. SSE-CMM aligns MOST closely with which improvement philosophy?
A. Ad-hoc security
B. Continuous improvement
C. Incident-driven response
D. Compliance checklist

△ HARD (Q26–Q40)

Q26. Which scenario BEST illustrates SSE-CMM application?
A. Conducting vulnerability scans
B. Measuring maturity of security engineering processes
C. Performing SOC audits
D. Enforcing regulatory compliance

Q27. An organization with low SSE-CMM maturity MOST likely exhibits:
A. Consistent security practices
B. Ad-hoc and inconsistent security engineering
C. Optimized governance
D. Predictive risk management

Q28. Which limitation MOST applies to SSE-CMM?
A. Lack of security focus
B. High implementation complexity
C. No relevance to engineering
D. Mandatory certification

Q29. SSE-CMM complements ISO 27001 by addressing:
A. Financial reporting
B. Security engineering maturity
C. Compliance enforcement
D. Network monitoring

Q30. Which factor MOST influences SSE-CMM assessment outcomes?
A. Organization size
B. Process documentation and consistency
C. Number of security tools
D. External regulations

Q31. SSE-CMM maturity levels MOST closely resemble:
A. OSI layers
B. CMMI levels
C. TCP/IP stack
D. ITIL practices

Q32. Treating SSE-CMM as a checklist MOST likely results in:
A. Optimized engineering
B. Superficial maturity claims
C. Improved assurance
D. Reduced risk

Q33. SSE-CMM is MOST valuable for organizations building:
A. Simple websites
B. Mission-critical systems
C. Personal applications
D. Static content

Q34. Which governance weakness MOST reduces SSE-CMM effectiveness?
A. Strong leadership
B. Lack of management commitment
C. Clear process ownership
D. Continuous review

Q35. SSE-CMM primarily measures capability at which level?
A. Individual employee
B. Organizational process
C. Single system
D. External vendor

Q36. SSE-CMM maturity improvement requires:
A. Tool upgrades only
B. Cultural and process change
C. External certification
D. Regulatory enforcement

Q37. Which security principle is reinforced MOST by SSE-CMM?
A. Zero trust
B. Security by design
C. Encryption everywhere
D. Network isolation

Q38. SSE-CMM adoption without metrics MOST likely leads to:
A. Clear improvement tracking
B. Inability to measure progress
C. Reduced assessment effort
D. Guaranteed maturity

Q39. SSE-CMM findings are MOST useful for:
A. End users
B. Senior management and engineering leadership
C. Attackers
D. Customers only

Q40. The PRIMARY objective of SSE-CMM is to:
A. Certify security products
B. Improve security engineering process maturity
C. Replace security audits
D. Eliminate cyber threats