CISSP Practice Question Bank

Comprehensive 400-Question Set
Covering All 8 Domains of the CISSP Common Body of Knowledge (CBK)
with Integrated AI/ML Security, Cloud Infrastructure, ISO 42001 Governance, and Compliance Frameworks

Prepared by:
Manoj Kumar
Agentic Security, Trust, Infrastructure | Security, Privacy, Compliance, Governance, and Risk Management Expert

Edition: 2025

(ISC)² Disclaimer

CISSP® is a registered trademark of (ISC)², Inc.
This independently prepared material is not endorsed, sponsored, or affiliated with (ISC)².
It is intended solely for educational and review purposes to assist learners in preparing for the CISSP examination.
Always reference the official (ISC)² materials and Common Body of Knowledge (CBK) for authoritative and up-to-date content.

DOMAIN 1 – Security and Risk Management (Questions 1–50)

Q1. What is the primary purpose of information security governance?
A. Manage user access controls
B. Align security with business objectives
C. Monitor intrusion detection systems
D. Ensure firewalls are configured
Answer: B
Explanation: Governance aligns security strategy with business goals and risk appetite.

Q2. Which of the following best describes residual risk?
A. Risk eliminated by controls
B. Risk remaining after controls are applied
C. Risk that cannot be measured
D. Risk transferred to a third party
Answer: B
Explanation: Residual risk is what remains after mitigation or control efforts.

Q3. The NIST Cybersecurity Framework is organized into which five core functions?
A. Identify, Protect, Detect, Respond, Recover
B. Plan, Do, Check, Act, Improve
C. Assess, Control, Audit, Remediate, Report
D. Prevent, Detect, Correct, Review, Report
Answer: A
Explanation: NIST CSF's five pillars structure enterprise cybersecurity programs.

Q4. Which step must precede building an AI/ML risk program?
A. Deploying GPU clusters
B. Defining governance, ethics, and accountability principles
C. Procuring cloud storage
D. Automating ML pipelines
Answer: B

Explanation: AI governance starts with ethical and accountable foundations (ISO 42001 Clause 5).

Q5. Which term defines research performed prior to a business decision?
A. Due care
B. Due diligence
C. Risk analysis
D. Audit planning
Answer: B
Explanation: Due diligence = investigation before commitment (e.g., vendor review).

Q6. What does a risk register document?
A. Only audit findings
B. Identified risks, owners, mitigation, and status
C. Network topology
D. Password policy
Answer: B
Explanation: Risk register tracks all risk elements and treatments.

Q7. ISO 27005 primarily guides:
A. Software testing
B. Information-security risk management
C. Data privacy controls
D. Incident forensics
Answer: B
Explanation: It provides methods for assessing and treating risks per ISO 27001.

Q8. "Defense in Depth" is based on:
A. One control layer
B. Multiple independent safeguards
C. Outsourced security only
D. Minimal control sets
Answer: B
Explanation: Stacking independent controls limits single-point failures.

Q9. Accepting a risk means:
A. Taking no further action but documenting justification
B. Eliminating the threat
C. Transferring to insurance
D. Avoiding the activity
Answer: A
Explanation: Risk acceptance = informed decision to live with risk.

Q10. Recovery Time Objective (RTO) represents:
A. Max tolerable data loss

B. Targeted restoration time after disruption
C. Backup start time
D. Cost of downtime
Answer: B
Explanation: RTO defines allowable outage duration.

Q11. ISO 27701 extends ISO 27001 to manage:
A. Business continuity
B. Privacy information management
C. Financial risk
D. Cloud infrastructure
Answer: B
Explanation: ISO 27701 establishes a Privacy Information Management System (PIMS).

Q12. In quantitative analysis, SLE = ?
A. Asset Value × Exposure Factor
B. Exposure Factor × ARO
C. ALE × ARO
D. Asset Value ÷ ARO
Answer: A
Explanation: Single Loss Expectancy = expected loss per incident.

Q13. Risk transfer commonly involves:
A. Security training
B. Insurance or outsourcing
C. Stronger controls
D. Risk avoidance
Answer: B
Explanation: Transfer shifts impact via contracts or insurance.

Q14. Least-privilege helps:
A. Simplify policy
B. Minimize potential damage from compromise
C. Increase availability
D. Centralize admin
Answer: B
Explanation: Restricting access lowers attack surface.

Q15. A control objective is:
A. A detailed configuration
B. A high-level desired outcome
C. An audit procedure
D. A policy exception
Answer: B
Explanation: It states what controls should achieve.

Q16. Under FISMA, who defines federal control requirements?
A. ISO
B. NIST
C. ISC²
D. OWASP
Answer: B
Explanation: NIST SP 800-53 specifies mandatory controls.

Q17. Integrated GRC (Governance Risk Compliance) means:
A. Separate reporting
B. Unified oversight linking policies, risks, controls
C. Manual spreadsheets
D. Isolated automation
Answer: B
Explanation: Integration connects governance objectives to risk data and evidence.

Q18. Secure AI Framework (SAIF) focuses on:
A. Dataset encryption only
B. Secure and accountable AI lifecycle
C. Model disabling
D. Avoiding testing
Answer: B
Explanation: SAIF covers security across AI development and deployment phases.

Q19. Risk appetite is:
A. Risk an organization is willing to accept
B. Residual risk level
C. Probability metric
D. Control efficiency
Answer: A
Explanation: Defines tolerance threshold for risk exposure.

Q20. ISC² Code of Ethics first canon requires members to:
A. Protect organization only
B. Protect society and common good
C. Ignore privacy
D. Prioritize profit
Answer: B
Explanation: Canon 1 – protect society and the infrastructure.

Q21. What is “due care”?
A. Continuous monitoring
B. Ongoing maintenance after due diligence
C. Performing risk analysis
D. Purchasing insurance

Answer: B
Explanation: Due care = actions taken to maintain security after initial assessment.

Q22. Business Impact Analysis (BIA) helps:
A. Quantify threat probability
B. Prioritize critical functions and recovery timelines
C. Implement controls
D. Select vendors
Answer: B
Explanation: BIA identifies process criticality and recovery targets.

Q23. Which control type detects violations after they occur?
A. Preventive
B. Detective
C. Compensating
D. Directive
Answer: B
Explanation: Detective controls identify incidents post-event.

Q24. Quantitative risk analysis benefit is:
A. Ease of execution
B. Provides monetary impact values
C. Uses subjective scoring
D. Ignores probability
Answer: B
Explanation: Enables financial comparison and ROI calculations.

Q25. Security policies should be:
A. Technical manuals
B. High-level statements of intent
C. Step-by-step procedures
D. Vendor guidelines
Answer: B
Explanation: Policies set direction and authority for security programs.

Q26. Which law regulates privacy for EU citizens?
A. GLBA
B. GDPR
C. HIPAA
D. SOX
Answer: B
Explanation: GDPR protects personal data of EU individuals.

Q27. Risk avoidance means:
A. Sharing risk

B. Eliminating the activity causing risk
C. Reducing impact
D. Accepting risk
Answer: B
Explanation: Avoidance = stop doing the risky process entirely.

Q28. The primary goal of security awareness training is to:
A. Eliminate human error
B. Influence behavior and reduce user risk
C. Provide technical skills
D. Test controls
Answer: B
Explanation: Awareness targets human behavior and culture.

Q29. COSO ERM framework focuses on:
A. Audit sampling
B. Enterprise risk management and internal control
C. Data classification
D. Encryption
Answer: B
Explanation: COSO integrates risk with strategic governance.

Q30. The primary driver for AI ethics policies is:
A. GPU availability
B. Accountability and bias mitigation
C. Speed of training
D. Model compression
Answer: B
Explanation: Ethical AI ensures fairness and trust.

Q31. Separation of duties prevents:
A. Resource optimization
B. Fraud and error
C. Performance bottlenecks
D. Access denials
Answer: B
Explanation: Divides tasks to avoid collusion or mistakes.

Q32. Which document defines management intent and direction?
A. Policy
B. Standard
C. Procedure
D. Baseline
Answer: A
Explanation: Policies express executive intent.

Q33. Business continuity plans should be tested:
A. Once per five years
B. Regularly with realistic scenarios
C. Only after an incident
D. When requested by auditors
Answer: B
Explanation: Periodic testing validates plan effectiveness.

Q34. ISO 31000 is a standard for:
A. Environmental management
B. Enterprise risk management
C. Data privacy
D. Network security
Answer: B
Explanation: Provides principles for any organizational risk framework.

Q35. Security baseline defines:
A. Ideal future state
B. Minimum required security configurations
C. Risk acceptance criteria
D. Budget allocation
Answer: B
Explanation: Baselines set minimum acceptable control levels.

Q36. Which is a directive control?
A. Firewall
B. Policy statement
C. IDS
D. Encryption
Answer: B
Explanation: Directive controls guide actions through policy.

Q37. Quantitative risk formula for ALE is:
A. SLE × ARO
B. SLE ÷ ARO
C. ARO − SLE
D. ARO × EF
Answer: A
Explanation: Annualized Loss Expectancy = expected yearly loss.

Q38. Data classification should be based on:
A. Data format
B. Value and sensitivity
C. File type
D. Owner’s preference

Answer: B
Explanation: Sensitivity drives classification and handling.

Q39. Which document grants authority for ISMS implementation?
A. Charter or policy statement
B. Procedure
C. Risk matrix
D. Control catalog
Answer: A
Explanation: Executive charter authorizes program execution.

Q40. What does MTO represent in continuity planning?
A. Maximum Tolerable Outage
B. Minimum Time Objective
C. Manual Transition Operation
D. Mean Time to Operate
Answer: A
Explanation: MTO = maximum downtime before irreversible impact.

Q41. Key advantage of qualitative risk analysis is:
A. Precision
B. Simplicity and speed
C. Requires exact data
D. Monetary output
Answer: B
Explanation: Uses scoring and expert judgment when data is limited.

Q42. The primary purpose of security metrics and KRIs is to:
A. Replace audits
B. Provide measurable insight into control effectiveness
C. Serve as marketing material
D. Meet HR targets
Answer: B
Explanation: Metrics quantify performance and risk levels.

Q43. Which framework focuses on IT governance and management?
A. COBIT 2019
B. ISO 9001
C. ITIL v4
D. NIST CSF
Answer: A
Explanation: COBIT links IT processes to business governance.

Q44. Ethics violations by CISSP members can result in:
A. Training requirement only

B. Suspension or revocation of certification
C. Fine from NIST
D. Termination of employment by ISC²
Answer: B
Explanation: ISC² enforces ethics through peer review and sanctions.

Q45. The chief purpose of a risk assessment is to:
A. Eliminate all risk
B. Identify and prioritize risks for treatment
C. Prove compliance
D. Satisfy auditors
Answer: B
Explanation: Assessment guides mitigation priorities.

Q46. Control maturity models (such as CMMI) help to:
A. Eliminate risk
B. Measure process capability and improvement levels
C. Certify auditors
D. Replace standards
Answer: B
Explanation: Shows how well processes are defined and optimized.

Q47. Which standard addresses Business Continuity Management Systems?
A. ISO 22301
B. ISO 27001
C. ISO 9001
D. ISO 42001
Answer: A
Explanation: ISO 22301 specifies BCMS requirements.

Q48. A control that reduces likelihood of incident is called:
A. Detective
B. Preventive
C. Corrective
D. Recovery
Answer: B
Explanation: Preventive controls stop events before they occur.

Q49. Which term describes formal acceptance of risk by senior management?
A. Risk acknowledgment
B. Risk authorization
C. Risk sign-off
D. Risk tolerance
Answer: B
Explanation: Management authorization is required for risk acceptance.

Q50. Security culture within an organization is best built through:
A. Mandatory technical tests only
B. Continuous education and leadership example
C. Punitive policies
D. Annual audit reviews
Answer: B
Explanation: Culture requires ongoing awareness and executive support.

DOMAIN 2 – Asset Security (Questions 51–100)

Q51. What is the primary goal of asset classification?
A. Simplify data storage
B. Assign value and protection requirements
C. Support financial accounting
D. Enable backups
Answer: B
Explanation: Classification ties security controls to an asset's sensitivity and business value.

Q52. Data ownership is best assigned to:
A. System administrators
B. Business units responsible for the data
C. Security team
D. End users
Answer: B
Explanation: Owners determine classification and authorized use.

Q53. Custodians are responsible for:
A. Determining data value
B. Implementing protection mechanisms
C. Approving data use
D. Performing risk assessments
Answer: B
Explanation: Custodians apply controls defined by owners.

Q54. What is the key difference between data at rest and data in transit?
A. Encryption applicability
B. Storage location
C. Threat type

D. Transmission medium
Answer: B
Explanation: At rest = stored; in transit = moving across networks.

Q55. Sanitization aims to:
A. Backup information
B. Permanently remove sensitive data
C. Encrypt data
D. Compress files
Answer: B
Explanation: Sanitization ensures irrecoverable data destruction.

Q56. Which media destruction method is suitable for solid-state drives?
A. Degaussing
B. Cryptographic erasure or physical shredding
C. Overwriting with zeros once
D. Formatting
Answer: B
Explanation: SSDs require crypto-erase or destruction, as degaussing is ineffective.

Q57. Data remanence refers to:
A. Backup copies
B. Residual data remaining after erasure
C. Encrypted archives
D. Deleted log entries
Answer: B
Explanation: Residual information may remain on media after deletion.

Q58. The most important factor when classifying information is:
A. File type
B. Sensitivity and impact if disclosed
C. Storage cost
D. Age of data
Answer: B
Explanation: Classification is driven by confidentiality, integrity, and availability impact.

Q59. Labeling data supports which control principle?
A. Separation of duties
B. Accountability and handling consistency
C. Least privilege
D. Non-repudiation
Answer: B
Explanation: Labels communicate handling requirements to all users.

Q60. Who determines retention requirements?
A. Legal, compliance, and data owners jointly
B. Database administrators
C. Network engineers
D. HR department only
Answer: A
Explanation: Retention periods must meet legal and business obligations.

Q61. What defines how long evidence must be preserved?
A. Policy
B. Retention schedule
C. Service-level agreement
D. Asset inventory
Answer: B
Explanation: Retention schedules define duration based on regulation.

Q62. Which ISO standard provides privacy-by-design guidance for cloud processors?
A. ISO 27018
B. ISO 22301
C. ISO 42001
D. ISO 9001
Answer: A
Explanation: ISO 27018 governs PII protection in public clouds.

Q63. Asset inventories must include:
A. Asset ID, owner, classification, and location
B. Only hardware serial numbers
C. Employee preferences
D. Vendor price list
Answer: A
Explanation: Comprehensive inventories support accountability and control coverage.

Q64. Which method ensures data integrity in storage?
A. Hashing and checksums
B. Compression
C. DLP tagging
D. Backup rotation
Answer: A
Explanation: Hashing detects unauthorized modification.

Q65. What is the best protection for highly sensitive PII stored in cloud?
A. Tokenization and strong encryption
B. Shared keys across tenants
C. Public exposure for transparency
D. Single-factor authentication

Answer: A
Explanation: Tokenization + encryption mitigate disclosure risk.

Q66. The chain of custody ensures:
A. Encryption strength
B. Evidence integrity from collection to presentation
C. Data retention period
D. Backup restoration
Answer: B
Explanation: It maintains documented control of evidence handling.

Q67. Media reuse requires:
A. Format command only
B. Proper sanitization before reassignment
C. Simple overwrite
D. None if same owner
Answer: B
Explanation: Sanitize to remove residual data before reuse.

Q68. Cloud data portability focuses on:
A. Vendor-lock avoidance and data retrieval standards
B. Hardware upgrades
C. Cryptographic strength
D. Audit frequency
Answer: A
Explanation: Supports compliance and business continuity during provider changes.

Q69. What is data sovereignty?
A. Encryption algorithm selection
B. Jurisdictional control over data based on location
C. Data ownership transfer
D. DRM enforcement
Answer: B
Explanation: Data is subject to laws of its physical storage region.

Q70. Classification labels should be:
A. Secretly maintained
B. Visible to authorized users handling the data
C. Hidden in metadata only
D. Optional
Answer: B
Explanation: Clear labeling guides correct handling.

Q71. The first step in asset management lifecycle is:
A. Disposal

B. Identification and inventory
C. Classification
D. Maintenance
Answer: B
Explanation: You must know what exists before securing it.

Q72. Which regulation governs retention of financial audit records in the U.S.?
A. HIPAA
B. SOX (Sarbanes-Oxley Act)
C. FERPA
D. FISMA
Answer: B
Explanation: SOX mandates preservation of financial documentation.

Q73. Data masking is primarily used to:
A. Encrypt backups
B. Obscure sensitive fields in non-production environments
C. Destroy PII
D. Improve compression
Answer: B
Explanation: Masking preserves data format while hiding real values.

Q74. What is a key control for data minimization in AI pipelines?
A. Collect all available data
B. Retain only necessary features for model training
C. Store every log forever
D. Disable encryption
Answer: B
Explanation: Minimization reduces privacy and compliance risk.

Q75. Asset valuation methods include:
A. Qualitative ranking or quantitative dollar value
B. Only depreciation tables
C. Random assignment
D. None; classification only
Answer: A
Explanation: Value drives protection priority.

Q76. Backups of classified data must:
A. Use equivalent protection as originals
B. Be unencrypted
C. Be stored offsite without controls
D. Have lower classification
Answer: A
Explanation: Backup copies inherit same classification level.

Q77. When disposing of cloud storage volumes, ensure:
A. Cryptographic key destruction
B. Formatting
C. DNS flush
D. Manual deletion of logs
Answer: A
Explanation: Crypto-erase renders data unreadable even if media persists.

Q78. What ensures data availability in distributed systems?
A. Replication and redundancy
B. DLP
C. Classification
D. Watermarking
Answer: A
Explanation: Replication protects against node failures.

Q79. System of Record (SoR) identifies:
A. Authoritative source for data element
B. Secondary copy
C. Log file
D. Test dataset
Answer: A
Explanation: SoR defines the master dataset used for compliance accuracy.

Q80. Which process defines who can access specific data elements?
A. Access control policy
B. Data inventory
C. Encryption management
D. Degaussing
Answer: A
Explanation: Access policy enforces ownership rules.

Q81. What should occur before moving data to a lower classification?
A. Management authorization and sanitization review
B. Immediate re-labeling
C. Backup deletion
D. None needed
Answer: A
Explanation: Downgrading requires formal approval.

Q82. Which is a physical protection for asset confidentiality?
A. Locked cabinets and restricted rooms
B. Digital signatures
C. Access logs
D. VPN tunnels

Answer: A
Explanation: Physical controls prevent unauthorized viewing or removal.

Q83. The best approach for identifying shadow data assets in SaaS?
A. Manual discovery
B. CASB (Cloud Access Security Broker) scanning
C. Firewalls only
D. User reports
Answer: B
Explanation: CASBs detect unsanctioned storage locations.

Q84. Information classification is usually performed by:
A. Data owner
B. Custodian
C. Security auditor
D. End user
Answer: A
Explanation: Owner defines classification level and handling.

Q85. Which control prevents data leakage via screenshots or printing?
A. DLP endpoint controls
B. IDS
C. Antivirus
D. VPN
Answer: A
Explanation: Endpoint DLP monitors copy/print actions.

Q86. When decommissioning hardware with encrypted drives, what simplifies sanitization?
A. Destroying encryption keys
B. Firmware upgrade
C. Reformat
D. Disk imaging
Answer: A
Explanation: Key destruction instantly renders data unrecoverable.

Q87. Data aggregation increases:
A. Accuracy
B. Sensitivity and risk
C. Compression
D. Auditability
Answer: B
Explanation: Combining datasets can expose new privacy risks.

Q88. The term “Data Lifecycle Management (DLM)” covers:
A. Creation → Storage → Use → Archive → Disposal

B. Only backups
C. Encryption process
D. Patch management
Answer: A
Explanation: DLM manages protection across entire asset lifespan.

Q89. Which privacy principle restricts use of data beyond original purpose?
A. Purpose limitation
B. Integrity
C. Openness
D. Collection limitation
Answer: A
Explanation: GDPR mandates data used only for specified lawful purposes.

Q90. Cloud customers remain accountable for:
A. Data classification and access control
B. Physical datacenter security
C. Hardware lifecycle
D. ISP routing
Answer: A
Explanation: In shared-responsibility model, data governance stays with customer.

Q91. Asset tagging benefits include:
A. Traceability and loss prevention
B. Encryption
C. Power management
D. Faster printing
Answer: A
Explanation: Tags link physical and logical inventories.

Q92. Critical asset loss should trigger:
A. Incident response + forensics
B. Firewall rule change
C. Vendor audit
D. Network scan
Answer: A
Explanation: Immediate IR to contain and assess impact.

Q93. Which standard defines AI asset accountability within organizations?
A. ISO 42001 (Artificial Intelligence Management System)
B. ISO 27001
C. NIST SP 800-30
D. PCI-DSS
Answer: A
Explanation: ISO 42001 introduces governance for AI-related assets.

Q94. The “right to be forgotten” applies primarily to:
A. GDPR compliance
B. SOX records
C. PCI cardholder data
D. HIPAA logs
Answer: A
Explanation: GDPR Article 17 grants individuals deletion rights.

Q95. To ensure confidentiality of printed classified reports:
A. Secure print release + locked bins
B. Automatic shredders disabled
C. Color printing only
D. Public printers
Answer: A
Explanation: Physical document control prevents leakage.

Q96. Data owners should review classifications:
A. Periodically or upon major change
B. Once at creation only
C. Every decade
D. Never
Answer: A
Explanation: Periodic review keeps classifications current.

Q97. What is “data lineage”?
A. The historical flow of data through systems
B. Encryption method
C. Access pattern
D. User group
Answer: A
Explanation: Lineage tracks data origin and transformations.

Q98. A media control policy should cover:
A. Labeling, transport, storage, and destruction
B. Procurement
C. Power use
D. Hiring practices
Answer: A
Explanation: Controls life-cycle of physical and digital media.

Q99. Which process validates third-party handling of your organization’s data?
A. Vendor risk assessment
B. Security awareness
C. Patch audit
D. DR testing

Answer: A
Explanation: Assess vendors for compliance with contractual data protection.

Q100. Data classification directly supports which CIA component?
A. Confidentiality
B. Integrity
C. Availability
D. Non-repudiation
Answer: A
Explanation: Classification dictates confidentiality safeguards.

DOMAIN 3 – Security Architecture and Engineering (Questions 101–150)

Q101. Which security model enforces “no read-up, no write-down”?
A. Bell-LaPadula
B. Biba
C. Clark-Wilson
D. Brewer-Nash
Answer: A
Explanation: Bell-LaPadula maintains confidentiality.

Q102. “No write-up, no read-down” describes:
A. Biba Integrity Model
B. Bell-LaPadula
C. Clark-Wilson
D. Lattice Model
Answer: A
Explanation: Biba preserves integrity hierarchy.

Q103. Clark-Wilson model emphasizes:
A. Mandatory Access Control
B. Well-formed transactions and separation of duties
C. Multilevel confidentiality
D. Non-interference
Answer: B
Explanation: Prevents fraud through integrity controls.

Q104. Trusted Computing Base (TCB) consists of:
A. All protection mechanisms enforcing policy
B. Entire OS code
C. User applications
D. Network firewalls
Answer: A
Explanation: TCB = hardware, firmware, and software ensuring security.

Q105. Security kernel function:
A. Enforce reference monitor concept
B. Handle GUI
C. Encrypt traffic
D. Manage power
Answer: A
Explanation: Kernel mediates all access per policy.

Q106. Reference monitor must be:
A. Tamper-proof, always invoked, verifiable
B. Optional, invisible
C. Application-level only
D. Randomly audited

Answer: A
Explanation: Three properties define trusted enforcement.

Q107. TOC/TOU (Time-of-Check/Time-of-Use) flaw relates to:
A. Race conditions
B. Buffer overflow
C. Injection
D. Privilege escalation only
Answer: A
Explanation: Occurs when state changes between check & use.

Q108. Which control mitigates electromagnetic emanation risk?
A. TEMPEST shielding
B. TLS
C. VPN
D. VLAN
Answer: A
Explanation: TEMPEST standards limit signal leakage.

Q109. Which hardware security module provides cryptographic key isolation?
A. TPM/HSM
B. CPU cache
C. SSD controller
D. BIOS
Answer: A
Explanation: HSMs protect keys from exposure.

Q110. A side-channel attack exploits:
A. Timing or power usage patterns
B. Source code defects
C. Social engineering
D. DNS misconfigurations
Answer: A
Explanation: Observes indirect information from hardware.

Q111. What design principle ensures minimal exposure?
A. Economy of mechanism and least privilege
B. Obfuscation
C. Complexity
D. Denial by default
Answer: A
Explanation: Simpler, minimal designs reduce risk.

Q112. Layering and abstraction contribute to:
A. Defense in depth

B. Performance only
C. Usability
D. AI bias testing
Answer: A
Explanation: Multiple layers enhance resilience.

Q113. Which security mode allows users with the same clearance but different need-to-know?
A. Compartmented Mode
B. System High
C. Dedicated Mode
D. Multilevel Mode
Answer: A
Explanation: Compartments restrict by category.

Q114. EAL levels in Common Criteria measure:
A. Assurance strength from 1 to 7
B. Encryption strength
C. OS versions
D. Confidentiality classification
Answer: A
Explanation: Higher EAL = greater evaluation rigor.

Q115. Security by design principle means:
A. Integrating controls early in SDLC
B. Testing after deployment
C. Outsourcing security
D. Manual patching
Answer: A
Explanation: Embed security throughout architecture.

Q116. Which cryptographic module validation program is required for U.S. federal use?
A. FIPS 140-3
B. ISO 9001
C. SOC 2
D. PCI
Answer: A
Explanation: FIPS 140-3 certifies cryptographic modules.

Q117. Which architecture isolates workloads via hardware virtualization?
A. Hypervisor-based VM isolation
B. Monolithic kernel
C. Mesh networking
D. Blockchain
Answer: A
Explanation: Hypervisors enforce guest separation.

Q118. Cloud security architecture must ensure:
A. Isolation, trust boundaries, encryption, and IAM integration
B. Public access to management plane
C. Shared keys
D. Flat networks
Answer: A
Explanation: Architecture defines multitenant segregation.

Q119. AI model poisoning occurs when:
A. Training data is maliciously altered
B. GPU overheats
C. Logs are deleted
D. Model weights compress
Answer: A
Explanation: Poisoning manipulates learning outcomes.

Q120. Secure enclave technology (e.g., Intel SGX) provides:
A. Encrypted execution environments
B. Faster CPU scheduling
C. Memory overclocking
D. Redundant power
Answer: A
Explanation: Enclaves isolate sensitive operations.

Q121. Which architecture pattern separates data, control, and presentation?
A. MVC (Model–View–Controller)
B. Monolith
C. Ring 0 kernel
D. Pipeline
Answer: A
Explanation: Supports modular security enforcement.

Q122. Security domains are defined by:
A. Common security policies and trust levels
B. Data formats
C. Server vendors
D. Subnet IDs
Answer: A
Explanation: Domains share identical rules and clearance.

Q123. The Orange Book (TCSEC) introduced:
A. Security evaluation classes (D through A1)
B. GDPR compliance
C. OWASP Top 10
D. ISO 27001

Answer: A
Explanation: Defined formal U.S. system evaluation criteria.

Q124. The concept “fail secure” means:
A. Maintain security when failures occur
B. Stay available at all cost
C. Allow guest access
D. Disable encryption
Answer: A
Explanation: Systems default to secure states under failure.

Q125. Which concept ensures every subject/object access checked?
A. Complete mediation
B. Open design
C. Least privilege
D. Economy of mechanism
Answer: A
Explanation: Every access request must be validated.

Q126. What is the main purpose of a security perimeter?
A. Define trusted boundaries between zones
B. Store logs
C. Enhance bandwidth
D. Replace authentication
Answer: A
Explanation: Segmentation reduces exposure.

Q127. In AI model architecture, differential privacy protects:
A. Individual training data records
B. GPU firmware
C. Cloud costs
D. Log files
Answer: A
Explanation: DP adds noise to prevent reverse identification.

Q128. Which term defines resistance to change under duress?
A. Fault tolerance
B. Resilience
C. Availability
D. Redundancy
Answer: B
Explanation: Resilience covers adaptive recovery from disruptions.

Q129. What is an example of physical security control?
A. CCTV monitoring

B. Encryption
C. Firewall
D. Authentication
Answer: A
Explanation: Physical layer controls deter intrusion.

Q130. Electromagnetic shielding prevents:
A. Emanation eavesdropping
B. Hardware overheating
C. Cable cuts
D. Network congestion
Answer: A
Explanation: TEMPEST or Faraday cages protect signals.

Q131. Which control enforces need-to-know?
A. Discretionary Access Control (DAC)
B. Mandatory Access Control (MAC)
C. Role-Based Access Control (RBAC)
D. Attribute-Based Access Control (ABAC)
Answer: B
Explanation: MAC enforces policy via labels and clearances.

Q132. In layered defense, a firewall is:
A. Perimeter preventive control
B. Detective
C. Directive
D. Recovery
Answer: A
Explanation: Firewalls prevent unauthorized traffic.

Q133. Security architecture diagrams should include:
A. Trust zones and control layers
B. Marketing content
C. Budget
D. HR data
Answer: A
Explanation: Visualizing boundaries helps risk analysis.

Q134. Single point of failure violates:
A. Availability principle
B. Confidentiality
C. Integrity
D. Non-repudiation
Answer: A
Explanation: SPOFs reduce system uptime.

Q135. Tokenization differs from encryption by:
A. Substituting tokens instead of reversible cipher
B. Using keys
C. Storing ciphertext
D. Integrity focus only
Answer: A
Explanation: Tokens map to data without revealing content.

Q136. What protects firmware integrity on boot?
A. Secure boot + signed images
B. BIOS password only
C. RAID
D. TPM disabled
Answer: A
Explanation: Verifies digital signatures before load.

Q137. The principle of “open design” suggests:
A. Security should not rely on secrecy of design
B. Keep algorithms hidden
C. Use proprietary logic
D. Avoid peer review
Answer: A
Explanation: Transparency enables stronger assurance.

Q138. In fault-tolerant systems, MTBF represents:
A. Mean Time Between Failures
B. Maximum Time Before Failure
C. Mean Time Backup Frequency
D. Minimum Testing Baseline
Answer: A
Explanation: MTBF measures component reliability.

Q139. AI model explainability supports:
A. Transparency and trust in decisions
B. Speed optimization
C. Encryption
D. DR readiness
Answer: A
Explanation: Interpretability enables accountable governance.

Q140. Cloud hardware root-of-trust ensures:
A. Verified boot and cryptographic integrity
B. Performance boost
C. Data replication
D. Storage compression

Answer: A
Explanation: Hardware trust anchors integrity checks.

Q141. ISO 42001 complements which management system?
A. ISO 27001 (Information Security Management System)
B. ISO 9001
C. ISO 22301
D. ISO 50001
Answer: A
Explanation: It extends ISMS to AI governance.

Q142. Air-gapped systems provide:
A. Physical network isolation
B. Remote connectivity
C. Performance tuning
D. Cloud access
Answer: A
Explanation: Disconnected systems prevent remote compromise.

Q143. A secure design review should focus on:
A. Threat modeling and control validation
B. UI colors
C. Marketing
D. Cost saving
Answer: A
Explanation: Identifies vulnerabilities early.

Q144. AI adversarial examples exploit:
A. Model prediction weaknesses via crafted inputs
B. Network latency
C. Key reuse
D. Backup schedules
Answer: A
Explanation: Attackers manipulate model outputs.

Q145. Homomorphic encryption allows:
A. Computation on encrypted data
B. Keyless encryption
C. Token substitution
D. Only decryption in memory
Answer: A
Explanation: Enables secure processing without revealing data.

Q146. Zero Trust Architecture principle:
A. Never trust, always verify

B. Trust perimeter
C. Default open access
D. Flat network
Answer: A
Explanation: Every request is authenticated and authorized.

Q147. Which is a security domain bridging AI and cloud?
A. Confidential computing
B. Open Wi-Fi
C. Shared GPUs without encryption
D. Unmonitored APIs
Answer: A
Explanation: Protects workloads during computation.

Q148. In system design, economy of mechanism means:
A. Keep designs simple and small
B. Add redundancy
C. Use complex controls
D. Obfuscate code
Answer: A
Explanation: Simplicity enhances assurance.

Q149. Microkernel architecture improves:
A. Isolation and fault tolerance
B. Speed by disabling security
C. Single-point control
D. UI experience
Answer: A
Explanation: Minimal kernel reduces attack surface.

Q150. Trusted path ensures:
A. Secure communication between user and TCB
B. Backup copies
C. Patch verification
D. Logging
Answer: A
Explanation: Prevents interception of authentication inputs.

DOMAIN 4 – Communication and Network Security (Questions 151–200)

Q151. The primary goal of network segmentation is:
A. Improve bandwidth
B. Reduce attack surface and contain breaches
C. Simplify routing
D. Support VLAN naming
Answer: B
Explanation: Segmentation limits lateral movement and isolates sensitive systems.

Q152. The function of a DMZ (demilitarized zone) is to:
A. Host public-facing services isolated from internal networks
B. Provide VPN access
C. Store backups
D. Manage logs
Answer: A
Explanation: DMZ separates external and internal traffic boundaries.

Q153. Which protocol operates at the transport layer?
A. TCP
B. IP
C. ARP
D. ICMP
Answer: A
Explanation: TCP and UDP are Layer 4 transport protocols.

Q154. Which OSI layer handles encryption and session establishment?
A. Session and Presentation
B. Application
C. Transport
D. Network
Answer: A
Explanation: Session manages connections; presentation manages encryption/encoding.

Q155. Which device filters packets based on Layer 3 addresses?
A. Router
B. Switch
C. Firewall
D. Bridge
Answer: A
Explanation: Routers route traffic based on IP addressing.

Q156. Stateful firewalls differ from stateless because they:
A. Track connection states and context
B. Only inspect headers
C. Never inspect traffic
D. Use static rules only

Answer: A
Explanation: Stateful firewalls analyze session state.

Q157. A proxy server primarily provides:
A. Traffic mediation and content caching
B. Encryption
C. VLAN trunking
D. Bandwidth control only
Answer: A
Explanation: Proxies intercept and relay requests for security and caching.

Q158. VPNs secure remote connections via:
A. Encrypted tunnels over public networks
B. Air gaps
C. Open ports
D. None of the above
Answer: A
Explanation: VPNs use encryption protocols like IPsec or SSL/TLS.

Q159. Which wireless security protocol provides the strongest protection?
A. WPA3
B. WEP
C. WPA
D. WPA2
Answer: A
Explanation: WPA3 uses SAE and 192-bit encryption.

Q160. The primary weakness of WEP was:
A. Reuse of IVs and weak RC4 implementation
B. AES key size
C. MAC filtering
D. WPA compatibility
Answer: A
Explanation: WEP's static IVs led to key recovery attacks.

Q161. Which device prevents MAC flooding on switches?
A. Port security limiting MAC addresses
B. Firewalls
C. IDS
D. Routers
Answer: A
Explanation: Port security restricts learned MACs.

Q162. Network Access Control (NAC) ensures:
A. Only compliant devices connect to network

B. File sharing
C. Email relay
D. Backup transfer
Answer: A
Explanation: NAC enforces posture assessment and authorization.

Q163. Which security architecture principle applies to cloud network design?
A. Zero Trust segmentation and identity enforcement
B. Flat network topology
C. Shared admin keys
D. Default open ports
Answer: A
Explanation: Cloud security relies on microsegmentation and least privilege.

Q164. The term “man-in-the-middle attack” means:
A. Intercepting communications between endpoints
B. Denying service
C. Spoofing MAC addresses only
D. SQL injection
Answer: A
Explanation: MITM compromises data confidentiality/integrity.

Q165. DNSSEC prevents:
A. Cache poisoning
B. DDoS
C. Traffic flooding
D. SQL injection
Answer: A
Explanation: DNSSEC uses digital signatures to verify records.

Q166. Which technology inspects encrypted traffic at enterprise gateways?
A. SSL/TLS decryption proxy
B. IDS
C. VLAN trunk
D. Load balancer
Answer: A
Explanation: SSL inspection proxies terminate and re-encrypt traffic.

Q167. Which of the following is a Layer 2 attack?
A. ARP spoofing
B. DNS poisoning
C. SYN flood
D. SQL injection
Answer: A
Explanation: ARP spoofing exploits Ethernet address resolution.

Q168. IPsec transport mode encrypts:
A. Payload only
B. Header and payload
C. Application data only
D. Metadata
Answer: A
Explanation: Transport mode protects data between hosts, not outer IP header.

Q169. The purpose of NAT (Network Address Translation) is:
A. Map internal private IPs to public IPs
B. Encrypt traffic
C. Route based on domain
D. Filter spam
Answer: A
Explanation: NAT masks internal addressing.

Q170. VLANs improve security by:
A. Logically segmenting broadcast domains
B. Encrypting traffic
C. Replacing firewalls
D. Enabling DHCP
Answer: A
Explanation: VLANs separate networks logically.

Q171. Port 443 is used for:
A. HTTPS
B. HTTP
C. FTP
D. SSH
Answer: A
Explanation: HTTPS uses TLS on port 443.

Q172. SIEM systems primarily provide:
A. Correlation and analysis of security events
B. VPN management
C. Backup control
D. Email relay
Answer: A
Explanation: SIEM aggregates logs for detection and compliance.

Q173. A honeypot is used to:
A. Divert attackers and gather intelligence
B. Secure production data
C. Test backups
D. Scan ports

Answer: A
Explanation: Honeypots attract adversaries for monitoring.

Q174. Which protocol provides message integrity and authentication in IPsec?
A. AH (Authentication Header)
B. ESP
C. TLS
D. SSH
Answer: A
Explanation: AH ensures integrity/authentication only.

Q175. For high-security remote admin, use:
A. SSH with key authentication
B. Telnet
C. FTP
D. HTTP
Answer: A
Explanation: SSH provides encrypted command-line sessions.

Q176. A DDoS attack targets:
A. Availability
B. Confidentiality
C. Integrity
D. Non-repudiation
Answer: A
Explanation: Flooding resources denies service to legitimate users.

Q177. What control mitigates eavesdropping on wireless networks?
A. WPA3 encryption
B. Open authentication
C. MAC broadcast
D. SSID hiding
Answer: A
Explanation: WPA3 ensures encrypted communication.

Q178. SSL/TLS handshake authenticates:
A. Server (and optionally client) identity
B. Only encryption algorithms
C. Application payload
D. IP addresses
Answer: A
Explanation: Certificates validate endpoint identities.

Q179. What is the primary purpose of a VPN concentrator?
A. Aggregate multiple secure tunnels

B. Route email
C. Host web apps
D. Monitor logs
Answer: A
Explanation: VPN concentrators manage large-scale connections.

Q180. A network IDS functions by:
A. Monitoring and analyzing network traffic for anomalies
B. Blocking packets
C. Enforcing policies
D. Encrypting data
Answer: A
Explanation: IDS detects suspicious activities.

Q181. IPS differs from IDS because it:
A. Takes active response to block malicious traffic
B. Only logs events
C. Works offline
D. Uses signatures only
Answer: A
Explanation: IPS actively prevents intrusions.

Q182. MPLS improves:
A. Traffic engineering and performance in WANs
B. Application security
C. Firewall management
D. Encryption
Answer: A
Explanation: MPLS routes efficiently using labels.

Q183. A broadcast storm occurs when:
A. Loops cause repeated broadcasts
B. DNS is down
C. Firewall fails
D. Encryption fails
Answer: A
Explanation: Layer 2 loops overwhelm bandwidth.

Q184. Network forensics focuses on:
A. Capturing, preserving, and analyzing packet evidence
B. Malware disassembly
C. AI training
D. Patching
Answer: A
Explanation: Forensics reconstructs events from traffic logs.

Q185. TLS uses which handshake process?
A. Public key exchange to derive session keys
B. Hashing only
C. Symmetric encryption without negotiation
D. None
Answer: A
Explanation: TLS handshake establishes symmetric keys securely.

Q186. AI red-teaming in networked AI systems focuses on:
A. Testing AI model endpoints for abuse
B. Stress testing routers
C. Training data labeling
D. Wi-Fi tuning
Answer: A
Explanation: Validates resilience of AI-enabled APIs and inference endpoints.

Q187. SDN (Software Defined Networking) enhances security by:
A. Centralized control and dynamic policy enforcement
B. Hard-coded routing
C. Manual rule sets
D. Flat networks
Answer: A
Explanation: SDN controllers adaptively manage flow rules.

Q188. Which protocol secures email transmission between servers?
A. STARTTLS
B. FTP
C. POP3
D. IMAP
Answer: A
Explanation: STARTTLS upgrades SMTP connections to encrypted channels.

Q189. DNS amplification is a type of:
A. DDoS attack
B. Spoofing
C. Social engineering
D. SQL injection
Answer: A
Explanation: Attackers exploit open resolvers for reflection.

Q190. VLAN hopping exploits:
A. Misconfigured trunk ports
B. Strong segmentation
C. TLS encryption
D. DNSSEC

Answer: A
Explanation: Attackers inject frames to bypass VLAN boundaries.

Q191. What ensures email message integrity?
A. DKIM signatures
B. SPF
C. MX record
D. DNS cache
Answer: A
Explanation: DKIM adds cryptographic validation.

Q192. The function of a CASB in network security is to:
A. Monitor and control cloud app usage
B. Manage routers
C. Replace antivirus
D. Encrypt drives
Answer: A
Explanation: CASB enforces SaaS visibility and policy compliance.

Q193. In Zero Trust networking, perimeter security is replaced by:
A. Continuous identity-based verification
B. Flat VLANs
C. Firewalls only
D. VPN tunnels alone
Answer: A
Explanation: Every access is contextually validated.

Q194. AI model inference APIs should enforce:
A. API authentication and input validation
B. Public open endpoints
C. Data caching
D. Disabling logs
Answer: A
Explanation: Prevent prompt or injection attacks.

Q195. Secure email gateways typically perform:
A. Spam filtering, malware scanning, and DLP
B. File storage
C. DNS translation
D. IP routing
Answer: A
Explanation: SEG protects email flows.

Q196. What is the best protection against replay attacks?
A. Nonce and timestamp validation

B. Encryption only
C. NAT
D. Proxy servers
Answer: A
Explanation: Unique session tokens prevent reuse.

Q197. A reverse proxy is used to:
A. Protect backend servers and load balance traffic
B. Inspect outbound traffic
C. Encrypt data at rest
D. Filter spam
Answer: A
Explanation: Reverse proxies hide internal hosts.

Q198. IPSec ESP mode provides:
A. Confidentiality and integrity
B. Authentication only
C. Compression
D. Key exchange
Answer: A
Explanation: ESP encrypts and authenticates IP payloads.

Q199. Which standard governs network device secure management?
A. NIST SP 800-115
B. ISO 27033
C. ISO 27701
D. ISO 9001
Answer: B
Explanation: ISO 27033 details network security design and management.

Q200. Network egress filtering ensures:
A. Unauthorized data doesn’t leave the network
B. Faster internet
C. DNS caching
D. Load balancing
Answer: A
Explanation: Monitors outbound traffic for data exfiltration.

DOMAIN 5 – Identity and Access Management (IAM) (Questions 201–250)

Q201. What is the primary objective of Identity and Access Management (IAM)?
A. Simplify user training
B. Ensure that the right individuals access the right resources at the right time
C. Increase network throughput
D. Monitor physical entry points
Answer: B
Explanation: IAM enforces authentication, authorization, and accountability.

Q202. Which authentication factor is represented by a fingerprint?
A. Something you know
B. Something you have
C. Something you are
D. Somewhere you are
Answer: C
Explanation: Biometrics are “something you are.”

Q203. Multi-factor authentication (MFA) must use:
A. Two or more independent factors from different categories

B. Multiple passwords
C. Two usernames
D. Time-based OTP only
Answer: A
Explanation: MFA increases assurance by combining independent factors.

Q204. The principle of least privilege states:
A. Users get minimal necessary access
B. All users get admin rights
C. No user gets any access
D. Access is assigned randomly
Answer: A
Explanation: Least privilege limits potential misuse or compromise.

Q205. Role-Based Access Control (RBAC) assigns permissions based on:
A. Job function or role
B. User location
C. Device ID
D. Network address
Answer: A
Explanation: RBAC groups access according to organizational roles.

Q206. Discretionary Access Control (DAC) gives control to:
A. Data owner
B. Security officer
C. System administrator only
D. Vendor
Answer: A
Explanation: DAC allows resource owners to decide access.

Q207. Mandatory Access Control (MAC) enforces:
A. Access decisions based on labels and clearances
B. Discretion of users
C. Network segments
D. Time of day
Answer: A
Explanation: MAC uses classification and sensitivity labels.

Q208. Attribute-Based Access Control (ABAC) decisions depend on:
A. Subject, object, and environmental attributes
B. Role names only
C. Group memberships
D. Usernames
Answer: A
Explanation: ABAC evaluates contextual attributes dynamically.

Q209. Federated identity allows:
A. Users to access multiple systems using a single digital identity across domains
B. Each app to maintain separate credentials
C. Shared admin passwords
D. No authentication
Answer: A
Explanation: Federation enables single sign-on across trusted organizations.

Q210. Which protocol supports federated identity exchange?
A. SAML
B. ICMP
C. BGP
D. FTP
Answer: A
Explanation: Security Assertion Markup Language (SAML) enables identity federation.

Q211. Single Sign-On (SSO) primarily improves:
A. Usability and user experience while maintaining security
B. Firewall filtering
C. DNS resolution
D. VPN throughput
Answer: A
Explanation: SSO reduces password fatigue and administrative burden.

Q212. OAuth 2.0 is primarily used for:
A. Authorization delegation
B. Authentication only
C. Encryption
D. Token encryption
Answer: A
Explanation: OAuth authorizes applications to access user data without credentials.

Q213. OpenID Connect (OIDC) adds what to OAuth 2.0?
A. Authentication layer using ID tokens
B. Encryption only
C. Load balancing
D. Session logging
Answer: A
Explanation: OIDC extends OAuth to include user identity verification.

Q214. Which type of access control lists explicitly defines “deny” rules?
A. Discretionary ACL
B. Mandatory ACL
C. Role matrix
D. Network routing table

Answer: A
Explanation: DAC-based ACLs may contain both allow and deny entries.

Q215. Identity proofing refers to:
A. Verifying an individual's claimed identity using trusted evidence
B. Generating encryption keys
C. Approving role changes
D. Network configuration
Answer: A
Explanation: Identity proofing ensures that a user is legitimate before credential issuance.

Q216. Which directory protocol uses port 389 by default?
A. LDAP
B. SAML
C. RADIUS
D. Kerberos
Answer: A
Explanation: Lightweight Directory Access Protocol operates on port 389 (or 636 for LDAPS).

Q217. Kerberos prevents credential replay by using:
A. Time-stamped tickets and symmetric encryption
B. Digital certificates
C. Plaintext passwords
D. Static keys
Answer: A
Explanation: Kerberos tickets include timestamps to prevent reuse.

Q218. The function of an Identity Provider (IdP) in federation is to:
A. Authenticate users and issue assertions
B. Host target applications
C. Store audit logs
D. Enforce NAC
Answer: A
Explanation: IdPs confirm user identity for relying parties.

Q219. The main security risk with SSO is:
A. Single credential compromise grants broad access
B. Harder user onboarding
C. Too many passwords
D. Redundant credentials
Answer: A
Explanation: Compromise of SSO token can breach multiple systems.

Q220. RADIUS primarily provides:
A. Centralized authentication, authorization, and accounting for network access

B. Local password storage
C. Network routing
D. Encryption
Answer: A
Explanation: RADIUS servers manage AAA for network devices.

Q221. TACACS+ differs from RADIUS by:
A. Encrypting full payload and separating AAA functions
B. Being open source
C. Operating over UDP
D. Lack of accounting
Answer: A
Explanation: TACACS+ offers full-payload encryption and TCP-based communication.

Q222. Identity federation between cloud providers relies on:
A. SAML, OAuth 2.0, and OIDC standards
B. FTP transfer
C. IPSec
D. VPN chaining
Answer: A
Explanation: Federation protocols enable cross-domain authentication.

Q223. JIT (Just-In-Time) access improves:
A. Privileged access management by granting temporary credentials
B. Static admin privileges
C. VPN routing
D. Continuous password reuse
Answer: A
Explanation: JIT limits exposure by issuing time-bound elevation.

Q224. Privileged Access Management (PAM) solutions provide:
A. Session control, credential vaulting, and audit for admins
B. File encryption only
C. Web filtering
D. Cloud provisioning
Answer: A
Explanation: PAM secures high-value administrative accounts.

Q225. Biometric false acceptance rate (FAR) measures:
A. Likelihood of incorrectly accepting an impostor
B. Legitimate user rejection
C. Enrollment speed
D. Template size
Answer: A
Explanation: FAR quantifies false positive matches.

Q226. The false rejection rate (FRR) indicates:
A. Legitimate users denied access
B. Impostors accepted
C. System uptime
D. Key exchange failures
Answer: A
Explanation: FRR measures user convenience impact.

Q227. Crossover Error Rate (CER) is:
A. Point where FAR = FRR
B. Biometrics calibration time
C. Failure of authentication
D. System timeout
Answer: A
Explanation: Lower CER means better biometric accuracy.

Q228. Which biometric method has the highest permanence?
A. Iris recognition
B. Voice
C. Signature
D. Gait
Answer: A
Explanation: Iris patterns remain stable over lifetime.

Q229. Contextual access control in AI systems considers:
A. User identity, device risk, and behavioral analytics
B. Static password only
C. Username alone
D. None of these
Answer: A
Explanation: Adaptive AI-driven IAM uses behavioral signals.

Q230. The concept of “non-repudiation” ensures:
A. Users cannot deny their actions
B. Confidentiality only
C. Availability
D. Speed
Answer: A
Explanation: Achieved via digital signatures and audit trails.

Q231. A “service account” differs from a user account because it:
A. Runs automated system processes
B. Has personal data
C. Is limited to physical access
D. Uses biometrics

Answer: A
Explanation: Service accounts operate applications or jobs.

Q232. Which of the following is a risk with shared accounts?
A. Lack of individual accountability
B. Faster login
C. Stronger audit
D. Enhanced compliance
Answer: A
Explanation: Shared credentials obscure responsibility.

Q233. In federated identity, the relying party (RP):
A. Consumes authentication assertions
B. Issues credentials
C. Acts as IdP
D. Stores passwords
Answer: A
Explanation: RP trusts IdP for identity verification.

Q234. The primary purpose of a credential vault is:
A. Securely store and rotate privileged credentials
B. Log network traffic
C. Encrypt hard drives
D. Enforce password reuse
Answer: A
Explanation: Vaults centralize and protect secret storage.

Q235. Which access control model is most dynamic and suited for AI-driven systems?
A. Attribute-Based Access Control (ABAC)
B. MAC
C. DAC
D. RBAC
Answer: A
Explanation: ABAC evaluates context dynamically, enabling AI policy enforcement.

Q236. Identity federation in cloud reduces:
A. Credential sprawl and administrative overhead
B. Encryption
C. Network bandwidth
D. Patching
Answer: A
Explanation: Federation consolidates identity management.

Q237. Account recertification ensures:
A. Periodic review of user access rights

B. New password creation
C. Device updates
D. None of these
Answer: A
Explanation: Prevents access creep and orphaned privileges.

Q238. Risk of orphan accounts occurs when:
A. Employees leave but accounts remain active
B. Accounts use MFA
C. Passwords rotate
D. Logs are deleted
Answer: A
Explanation: Orphaned accounts pose insider threat risks.

Q239. Centralized IAM enhances:
A. Consistency and easier auditability
B. Manual operations
C. Fragmentation
D. Downtime
Answer: A
Explanation: Central management simplifies compliance and enforcement.

Q240. Directory replication ensures:
A. Availability and consistency across identity stores
B. Data loss
C. Password resets only
D. Backup recovery
Answer: A
Explanation: Replication maintains identical user data across sites.

Q241. Step-up authentication requires:
A. Additional verification for high-risk transactions
B. Automatic session logout
C. Fewer factors
D. Certificate removal
Answer: A
Explanation: Step-up adapts security to transaction risk.

Q242. Digital certificates are issued by:
A. Certificate Authorities (CAs)
B. ISPs
C. Cloud tenants
D. DNS servers
Answer: A
Explanation: CAs bind identities to public keys.

Q243. PKI revocation lists (CRL/OCSP) are used to:
A. Verify certificate status
B. Encrypt data
C. Store passwords
D. Manage DNS
Answer: A
Explanation: CRL/OCSP indicate revoked certificates.

Q244. Identity governance integrates:
A. Provisioning, review, and compliance reporting
B. Network segmentation
C. SIEM
D. SDN control
Answer: A
Explanation: IGA automates life cycle and compliance oversight.

Q245. Service account sprawl can be mitigated by:
A. Role-based and automated account provisioning
B. Manual spreadsheets
C. Shared passwords
D. Decentralization
Answer: A
Explanation: Automation ensures minimal, controlled accounts.

Q246. Cloud IAM best practice includes:
A. Using unique identities per service and least privilege
B. Reusing root credentials
C. Allowing public buckets
D. Hardcoding secrets
Answer: A
Explanation: Separate scoped credentials reduce blast radius.

Q247. Federated SSO in enterprise often uses:
A. SAML assertions or OIDC tokens
B. FTP login
C. SSH key copies
D. VPN split tunnels
Answer: A
Explanation: SSO tokens authenticate across services.

Q248. Which factor enhances identity assurance?
A. Hardware-based authenticators (FIDO2 keys)
B. Static passwords
C. CAPTCHA
D. Anonymous login

Answer: A
Explanation: Hardware MFA resists phishing and replay.

Q249. The purpose of access reviews in governance is to:
A. Verify appropriateness of privileges
B. Lock all accounts
C. Reset passwords
D. Issue new roles
Answer: A
Explanation: Reviews ensure access aligns with job functions.

Q250. Identity lifecycle management includes:
A. Provisioning → Maintenance → Deprovisioning
B. Encryption → Backup → Restore
C. Logging → Scanning → Reporting
D. Routing → Filtering → Forwarding
Answer: A
Explanation: Manages full user account lifecycle.

DOMAIN 6 – Security Assessment and Testing (Questions 251–300)

Q251. The primary objective of security testing is to:
A. Identify and validate vulnerabilities in systems and processes
B. Replace controls
C. Create compliance reports only
D. Reduce network latency
Answer: A
Explanation: Testing validates the effectiveness of implemented controls.

Q252. A vulnerability assessment differs from a penetration test because it:
A. Identifies and rates vulnerabilities but does not exploit them
B. Exploits systems for proof-of-concept
C. Tests physical controls only
D. Focuses only on compliance
Answer: A
Explanation: Vulnerability scanning enumerates and prioritizes weaknesses.

Q253. Penetration testing phases include:
A. Planning, discovery, attack, and reporting
B. Only scanning
C. Documentation only
D. Remediation only
Answer: A
Explanation: Pen tests follow structured attack simulation lifecycle.

Q254. Black-box testing assumes:
A. No prior knowledge of the system
B. Full source code access
C. Insider knowledge
D. Test of only internal networks
Answer: A
Explanation: Black-box mimics an external attacker’s view.

Q255. White-box testing involves:
A. Full knowledge of architecture and source code
B. External attacks only
C. Random fuzzing
D. No information

Answer: A
Explanation: White-box allows comprehensive code-level testing.

Q256. Gray-box testing provides:
A. Partial system knowledge
B. No knowledge
C. Full access
D. Random access
Answer: A
Explanation: Gray-box simulates insider with limited access.

Q257. Dynamic Application Security Testing (DAST) analyzes:
A. Running applications for runtime vulnerabilities
B. Source code without execution
C. Architecture design
D. Logs only
Answer: A
Explanation: DAST scans applications during execution.

Q258. Static Application Security Testing (SAST) is used for:
A. Source code analysis without executing the program
B. Dynamic testing
C. Network scanning
D. Penetration
Answer: A
Explanation: SAST detects code flaws pre-runtime.

Q259. Software Composition Analysis (SCA) detects:
A. Vulnerabilities in open-source components
B. Binary obfuscation
C. Physical tampering
D. User errors
Answer: A
Explanation: SCA identifies outdated or risky third-party libraries.

Q260. Fuzz testing identifies:
A. Application input handling issues by providing invalid data
B. Correct business logic
C. Encryption strength
D. Compliance violations
Answer: A
Explanation: Fuzzers reveal crashes and input flaws.

Q261. Interactive Application Security Testing (IAST):
A. Combines SAST and DAST techniques in runtime

B. Tests only static code
C. Replaces QA
D. Evaluates firewalls
Answer: A
Explanation: IAST instruments applications for deeper coverage.

Q262. Security audits evaluate:
A. Compliance against defined criteria
B. Hardware performance
C. Employee happiness
D. Cost savings
Answer: A
Explanation: Audits compare evidence to policy and standards.

Q263. Continuous monitoring provides:
A. Real-time visibility of control effectiveness and risk indicators
B. Annual review
C. Manual sampling
D. Snapshot reports
Answer: A
Explanation: Continuous monitoring detects deviations promptly.

Q264. The goal of an internal audit is to:
A. Provide independent assurance to management
B. Punish employees
C. Replace external audit
D. Install controls
Answer: A
Explanation: Internal audit evaluates controls' adequacy and performance.

Q265. Separation of test and production environments prevents:
A. Unauthorized access and data leakage between environments
B. Network loops
C. Code reusability
D. Latency
Answer: A
Explanation: Segregation reduces data contamination risk.

Q266. Regression testing ensures:
A. New changes do not reintroduce vulnerabilities
B. Performance is slower
C. Encryption keys rotate
D. Only new features work
Answer: A
Explanation: Confirms existing functionality remains secure.

Q267. Vulnerability scanning should be performed:
A. Regularly and after major changes
B. Once a year
C. Only before audits
D. On user demand
Answer: A
Explanation: Frequent scanning ensures timely detection.

Q268. Authenticated scans are preferred because they:
A. Provide deeper insight into patch and configuration status
B. Require less setup
C. Avoid false positives
D. Skip credentials
Answer: A
Explanation: Authenticated scans reveal internal weaknesses.

Q269. Code review benefits include:
A. Early detection of logic and security flaws
B. Faster compilation
C. Reduced licensing costs
D. Automated testing only
Answer: A
Explanation: Peer review improves software assurance.

Q270. A control self-assessment (CSA) enables:
A. Business process owners to evaluate their own control effectiveness
B. Independent auditor review
C. Firewall deployment
D. Backup validation
Answer: A
Explanation: CSAs embed accountability within business units.

Q271. Red teaming focuses on:
A. Simulating adversarial tactics to test detection and response
B. Routine vulnerability scanning
C. Policy writing
D. Asset inventory
Answer: A
Explanation: Red teams emulate realistic attack scenarios.

Q272. Blue teaming's main function is to:
A. Defend, detect, and respond to attacks
B. Exploit vulnerabilities
C. Write policy
D. Disable firewalls

Answer: A
Explanation: Blue teams enhance detection capabilities.

Q273. Purple teaming integrates:
A. Offensive and defensive teams for continuous improvement
B. Only penetration testers
C. Threat hunters
D. Compliance auditors
Answer: A
Explanation: Collaboration accelerates security maturity.

Q274. Bug bounty programs:
A. Encourage ethical hackers to report vulnerabilities
B. Hire permanent staff
C. Focus on phishing
D. Replace audits
Answer: A
Explanation: Crowdsourced testing extends coverage.

Q275. Baseline configuration testing ensures:
A. Systems remain aligned to approved secure standards
B. All controls disabled
C. Performance tuning
D. User training
Answer: A
Explanation: Maintains compliance and reduces drift.

Q276. Security metrics and KPIs are useful to:
A. Measure control performance and risk posture
B. Replace audits
C. Hide results
D. Delay management reporting
Answer: A
Explanation: Metrics quantify progress and maturity.

Q277. A penetration test scope document must include:
A. Authorized targets, schedule, and escalation contacts
B. List of users
C. Company history
D. None of these
Answer: A
Explanation: Scope prevents disruption and defines boundaries.

Q278. AI model testing should include:
A. Bias, fairness, and robustness evaluations

B. Only latency testing
C. Random fuzzing
D. Hardware audits
Answer: A
Explanation: AI assessments verify ethical and secure performance.

Q279. Log review frequency should be:
A. Risk-based and continuous for critical systems
B. Annual only
C. Monthly for all
D. None
Answer: A
Explanation: High-risk systems require near real-time log review.

Q280. A false positive in testing means:
A. A reported vulnerability that does not actually exist
B. Missed issue
C. Confirmed exploit
D. Correct detection
Answer: A
Explanation: False positives waste analyst time.

Q281. Metrics That Matter (MTM) dashboards track:
A. Key performance and key risk indicators for security programs
B. System uptime only
C. HR data
D. Software licenses
Answer: A
Explanation: MTM provides visibility into control efficiency.

Q282. Configuration compliance scans check:
A. System settings against security baselines
B. Network latency
C. Financial transactions
D. User preferences
Answer: A
Explanation: Validates hardened configurations.

Q283. Threat hunting is:
A. Proactive search for unknown threats using intelligence and analytics
B. Incident recovery
C. Log deletion
D. Training exercise
Answer: A
Explanation: Hunts uncover hidden compromises.

Q284. The primary input to a risk-based test plan is:
A. Criticality and likelihood of asset compromise
B. User feedback
C. Random schedule
D. License data
Answer: A
Explanation: Focus on high-impact risk areas.

Q285. Security test results should be:
A. Documented, validated, and tracked to closure
B. Ignored if minor
C. Shared publicly
D. Deleted
Answer: A
Explanation: Proper handling ensures accountability and remediation.

Q286. Continuous integration (CI) pipelines benefit from:
A. Automated security testing (DevSecOps)
B. Manual patching
C. Paper reports
D. Disable controls
Answer: A
Explanation: Integrates security early and continuously.

Q287. OWASP ZAP and Burp Suite are examples of:
A. Web application testing tools
B. IDS sensors
C. Antivirus
D. Firewalls
Answer: A
Explanation: Used for web application security scanning.

Q288. The term “test coverage” measures:
A. Percentage of code or components assessed during testing
B. Number of testers
C. Duration of tests
D. Log entries
Answer: A
Explanation: Higher coverage means better assurance.

Q289. A SOC 2 audit tests:
A. Controls related to Security, Availability, Processing Integrity, Confidentiality, Privacy
B. Financial reporting
C. Network speed
D. Software quality

Answer: A
Explanation: SOC 2 reports evaluate trust service criteria.

Q290. AI red teaming differs from pentesting by:
A. Targeting AI behavior, misuse, and bias
B. Focusing on firewalls
C. Ignoring ethics
D. Testing performance only
Answer: A
Explanation: AI red teams probe model misuse and manipulation.

Q291. Evidence collection during testing must ensure:
A. Integrity, chain of custody, and reproducibility
B. Minimal documentation
C. Encryption only
D. No analysis
Answer: A
Explanation: Ensures validity in audit trails.

Q292. Which standard provides guidance for information security testing?
A. NIST SP 800-115
B. ISO 9001
C. ISO 14000
D. COBIT
Answer: A
Explanation: NIST 800-115 defines technical testing methodologies.

Q293. Benchmark frameworks such as CIS are used to:
A. Establish secure configuration baselines
B. Encrypt traffic
C. Backup logs
D. Train staff
Answer: A
Explanation: CIS Benchmarks define system hardening settings.

Q294. False negatives in testing represent:
A. Missed vulnerabilities that exist
B. Nonexistent findings
C. Test success
D. Duplicate alerts
Answer: A
Explanation: They undermine security confidence.

Q295. Security maturity assessments rate:
A. Capability level of processes and governance

B. Number of incidents
C. Size of IT team
D. Audit cost
Answer: A
Explanation: Maturity models evaluate control optimization.

Q296. Regression scanning post-remediation confirms:
A. Fix effectiveness and absence of prior findings
B. Patch installation speed
C. Audit trail deletion
D. Employee training
Answer: A
Explanation: Verifies issues are resolved.

Q297. What is the goal of continuous control monitoring (CCM)?
A. Automate evidence collection and detect control deviations in real time
B. Replace auditors
C. Increase paperwork
D. Delay detection
Answer: A
Explanation: CCM integrates monitoring with GRC automation.

Q298. AI vulnerability testing should check for:
A. Prompt injection, data leakage, and model tampering
B. Only compute usage
C. GPU speed
D. Cloud cost
Answer: A
Explanation: AI-specific flaws must be tested systematically.

Q299. Security dashboards should visualize:
A. KRIs, KPIs, and control compliance metrics
B. Marketing data
C. Random events
D. Developer commits
Answer: A
Explanation: Dashboards communicate risk posture to leadership.

Q300. What is the final step of the audit lifecycle?
A. Follow-up and continuous improvement
B. Reporting only
C. Fieldwork
D. Planning
Answer: A
Explanation: Ensures corrective actions are implemented.

DOMAIN 7 – Security Operations (Questions 301–350)

Q301. The primary goal of security operations is to:
A. Detect, respond, and recover from incidents to maintain resilience
B. Eliminate all risk
C. Replace management
D. Manage HR data
Answer: A
Explanation: Security operations ensure ongoing protection and quick recovery.

Q302. The first step in incident response is:
A. Preparation
B. Eradication
C. Containment
D. Recovery

Answer: A
Explanation: Preparation ensures readiness before incidents occur.

Q303. The primary purpose of a SIEM system is to:
A. Aggregate and correlate security logs for analysis
B. Encrypt databases
C. Replace antivirus
D. Store backups
Answer: A
Explanation: SIEMs centralize event data for detection and compliance.

Q304. The principle of least privilege is most critical for:
A. Privileged and administrative accounts
B. Regular users only
C. Guests
D. Developers
Answer: A
Explanation: Admin accounts have the highest potential for abuse.

Q305. Mean Time to Detect (MTTD) measures:
A. Average time between intrusion and detection
B. Incident duration
C. Recovery cost
D. Backup latency
Answer: A
Explanation: MTTD helps evaluate detection capability.

Q306. Mean Time to Respond (MTTR) represents:
A. Average time from detection to containment or recovery
B. Outage frequency
C. Audit frequency
D. Risk score
Answer: A
Explanation: MTTR measures response efficiency.

Q307. Evidence collected during an incident must be:
A. Preserved with integrity and chain of custody
B. Stored without tracking
C. Shared publicly
D. Discarded
Answer: A
Explanation: Preserving evidence ensures admissibility.

Q308. Which backup strategy copies all files changed since last full backup?
A. Incremental

B. Differential
C. Mirror
D. Continuous
Answer: B
Explanation: Differential backups include changes since last full backup.

Q309. Business Continuity Planning (BCP) ensures:
A. Essential functions continue during disruption
B. Marketing campaigns run
C. Only physical security
D. Regulatory compliance only
Answer: A
Explanation: BCP maintains critical operations under stress.

Q310. Disaster Recovery (DR) primarily focuses on:
A. Restoring IT systems and data after an incident
B. Managing employees
C. Public relations
D. Training
Answer: A
Explanation: DR restores infrastructure and data quickly.

Q311. A hot site provides:
A. Fully equipped and ready-to-operate environment
B. Empty space
C. Tape storage
D. Manual operations
Answer: A
Explanation: Hot sites enable immediate failover.

Q312. Cold sites differ because they:
A. Lack pre-installed hardware and data
B. Are identical to production
C. Replicate data continuously
D. Use clustering
Answer: A
Explanation: Cold sites require setup time before use.

Q313. Warm sites include:
A. Partially configured infrastructure ready for activation
B. No equipment
C. Manual controls only
D. Alternate processes only
Answer: A
Explanation: Warm sites balance cost and readiness.

Q314. What is the primary function of change management?
A. Ensure modifications are documented, approved, and tested
B. Block all updates
C. Avoid change
D. Simplify HR tasks
Answer: A
Explanation: Structured change process prevents disruptions.

Q315. Configuration management tracks:
A. Baseline configurations and authorized changes
B. Employee performance
C. Backups only
D. Costs
Answer: A
Explanation: Maintains control over system state and integrity.

Q316. The “order of volatility” principle dictates collecting:
A. Most volatile evidence first
B. Hard drives first
C. Backups last
D. Random data
Answer: A
Explanation: Capture data that changes quickly (e.g., memory).

Q317. Chain of custody includes:
A. Who handled evidence, when, and under what conditions
B. Log timestamps only
C. File names
D. Software licenses
Answer: A
Explanation: Ensures accountability and evidence integrity.

Q318. Data retention policies are designed to:
A. Define how long data is kept and securely destroyed
B. Improve performance
C. Encrypt data
D. Create redundancy
Answer: A
Explanation: Aligns storage practices with regulations.

Q319. Sanitization of digital media ensures:
A. Irrecoverable removal of sensitive data
B. Backup compression
C. Random overwriting
D. Formatting only

Answer: A
Explanation: Prevents data leakage upon disposal.

Q320. The purpose of a forensics readiness policy is to:
A. Prepare systems to collect admissible evidence efficiently
B. Conduct postmortem
C. Random testing
D. Disable logging
Answer: A
Explanation: Enables efficient, lawful investigation.

Q321. Incident eradication involves:
A. Removing the root cause of the incident
B. Monitoring alerts
C. Writing reports only
D. Backups
Answer: A
Explanation: Restores systems to clean state.

Q322. During containment, the goal is to:
A. Limit damage and prevent spread
B. Identify root cause
C. Collect lessons learned
D. Archive evidence
Answer: A
Explanation: Stops incident escalation.

Q323. Post-incident review purpose:
A. Identify lessons learned and improve future responses
B. Assign blame
C. Erase logs
D. Terminate staff
Answer: A
Explanation: Drives process improvement.

Q324. Security monitoring includes:
A. Collecting and analyzing telemetry for anomalies
B. Updating HR data
C. Adjusting payroll
D. None
Answer: A
Explanation: Detects deviations from normal behavior.

Q325. Which law governs breach notifications for personal data in the EU?
A. GDPR

B. SOX
C. FISMA
D. HIPAA
Answer: A
Explanation: GDPR mandates notification within 72 hours.

Q326. Escalation procedures define:
A. When and how to notify stakeholders during incidents
B. Termination policy
C. Risk acceptance
D. Encryption
Answer: A
Explanation: Structured escalation ensures timely communication.

Q327. An operational log retention policy helps:
A. Maintain evidence for auditing and forensics
B. Delete historical data
C. Reduce visibility
D. Simplify access
Answer: A
Explanation: Retention supports compliance and investigations.

Q328. The function of a fault-tolerant system is to:
A. Continue operation despite hardware/software failures
B. Reboot faster
C. Increase speed
D. Add complexity
Answer: A
Explanation: Fault tolerance ensures high availability.

Q329. What metric measures downtime impact?
A. Mean Time Between Failures (MTBF)
B. Recovery Time Objective (RTO)
C. Residual risk
D. CVSS
Answer: B
Explanation: RTO defines acceptable outage duration.

Q330. What ensures employees understand their incident response duties?
A. Regular training and tabletop exercises
B. Annual vacation
C. New hire forms
D. Automated alerts only
Answer: A
Explanation: Exercises validate readiness.

Q331. The most critical phase of DR testing is:
A. Review and lessons learned
B. Power off
C. Backup rotation
D. Data labeling
Answer: A
Explanation: Post-test review improves future recovery.

Q332. Forensic duplication requires:
A. Bit-for-bit copy with hash verification
B. Normal backup
C. ZIP archive
D. Encrypted email
Answer: A
Explanation: Preserves evidence without alteration.

Q333. A root cause analysis (RCA) identifies:
A. Fundamental reason an incident occurred
B. Temporary fix
C. None
D. Budget issue
Answer: A
Explanation: RCA guides long-term prevention.

Q334. Insider threat programs aim to:
A. Detect and prevent malicious or negligent employee activity
B. Monitor external attackers only
C. Replace HR
D. Manage payroll
Answer: A
Explanation: Monitors insider behaviors and anomalies.

Q335. The main risk of log aggregation is:
A. Central point of failure and sensitive data exposure
B. Performance gain
C. Simplified compliance
D. None
Answer: A
Explanation: Centralized logs must be secured properly.

Q336. Security automation tools (SOAR) are used for:
A. Orchestrating response actions automatically
B. Manual investigations
C. Only vulnerability scanning
D. Patching

Answer: A
Explanation: SOAR integrates playbooks for rapid response.

Q337. DRP and BCP plans should be:
A. Tested, updated, and reviewed regularly
B. Archived only
C. Written once
D. Outsourced
Answer: A
Explanation: Ongoing updates maintain relevance.

Q338. MTBF primarily indicates:
A. Average reliability between failures
B. Recovery cost
C. Incident count
D. Log frequency
Answer: A
Explanation: Measures component longevity.

Q339. Mean Time to Repair (MTTR) measures:
A. Average time to restore service after failure
B. Detection time
C. Failure frequency
D. Audit time
Answer: A
Explanation: MTTR quantifies recovery speed.

Q340. What is a “tabletop exercise”?
A. Discussion-based simulated scenario to test response
B. Hardware drill
C. Backup test
D. Compliance review
Answer: A
Explanation: Tabletop tests improve coordination and preparedness.

Q341. Cloud provider incident response must include:
A. Shared responsibility coordination and SLA-based notification
B. Full access to hardware
C. Ignoring customers
D. None
Answer: A
Explanation: IR must align responsibilities in contracts.

Q342. Key challenge in AI system operations:
A. Monitoring for model drift and bias over time

B. Encrypting databases
C. Disabling GPUs
D. Hardware tuning
Answer: A
Explanation: Model drift impacts reliability and fairness.

Q343. Security orchestration improves:
A. Consistency and speed in repetitive operational tasks
B. Manual approvals
C. Compliance audits only
D. Latency
Answer: A
Explanation: Automation enhances operational scalability.

Q344. Insider threat indicators include:
A. Privilege misuse, abnormal file transfers, disgruntlement
B. Regular logins
C. Patch updates
D. Firewall rule change
Answer: A
Explanation: Behavior analytics detect anomalies.

Q345. What does the term “playbook” refer to in SOCs?
A. Predefined sequence of actions for incident types
B. Audit checklist
C. Backup job
D. Change ticket
Answer: A
Explanation: Playbooks standardize response workflows.

Q346. Digital forensics volatility order starts with:
A. CPU registers and cache
B. Disk drives
C. Archives
D. Backups
Answer: A
Explanation: Volatile evidence disappears fastest.

Q347. The most common first step in ransomware containment:
A. Isolate affected systems from the network
B. Pay ransom immediately
C. Notify marketing
D. Delete files
Answer: A
Explanation: Isolation limits spread.

Q348. Continuous operations monitoring ensures:
A. Early anomaly detection and reduced MTTD
B. Annual compliance only
C. Manual testing
D. Static defense
Answer: A
Explanation: Continuous monitoring enhances visibility.

Q349. Metrics like MTTR, MTTD, and incident volume support:
A. SOC performance and capacity planning
B. HR analytics
C. Financial audit
D. None
Answer: A
Explanation: They measure detection and response maturity.

Q350. “Lessons learned” reports should include:
A. Root cause, impact, and corrective actions
B. Blame
C. System uptime
D. Cost only
Answer: A
Explanation: Provides closure and continuous improvement.

DOMAIN 8 – Software Development Security (Questions 351–400)

Q351. The main objective of software security is to:
A. Prevent vulnerabilities throughout the software lifecycle
B. Speed up releases only
C. Shift risk to vendors
D. Focus on hardware security
Answer: A
Explanation: Integrating security across the SDLC reduces design and coding flaws.

Q352. The Secure Development Life Cycle (SDLC) begins with:
A. Security requirements gathering
B. Implementation
C. Deployment
D. Maintenance
Answer: A
Explanation: Security requirements define baseline expectations early.

Q353. Threat modeling identifies:
A. Potential threats, attack vectors, and mitigations
B. Coding style
C. Server performance
D. Encryption keys
Answer: A
Explanation: Threat modeling ensures proactive defense design.

Q354. The STRIDE model analyzes threats by:
A. Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
B. Security, Testing, Reporting, Integration, Deployment, Evaluation
C. Storage, Tokens, Risk, Identity, Data, Encryption
D. None of these
Answer: A
Explanation: STRIDE maps threat types to mitigation categories.

Q355. Secure coding practices aim to:
A. Prevent common vulnerabilities like injection and buffer overflows
B. Obfuscate code
C. Reduce file size
D. Increase development time
Answer: A
Explanation: Coding standards reduce exploitable flaws.

Q356. OWASP Top 10 represents:
A. The ten most critical web application security risks
B. Testing tools
C. Network protocols
D. Pen test methods
Answer: A
Explanation: OWASP maintains awareness of key web risks.

Q357. Injection attacks occur when:
A. Unvalidated user input is executed as a command or query
B. Encryption fails
C. Ports are open
D. Code compiles
Answer: A
Explanation: Validation prevents untrusted command execution.

Q358. The most effective defense against SQL injection is:
A. Parameterized queries and input validation
B. Disabling logging
C. Hashing
D. Firewalls
Answer: A
Explanation: Prepared statements prevent malicious queries.

Q359. Cross-site scripting (XSS) allows attackers to:
A. Execute scripts in users' browsers
B. Access physical servers
C. Modify firewalls
D. None
Answer: A
Explanation: XSS manipulates client-side code execution.

Q360. Cross-site request forgery (CSRF) exploits:
A. User's authenticated session to perform unwanted actions
B. SQL databases
C. Encryption
D. DNS

Answer: A
Explanation: CSRF tricks users into submitting malicious requests.

Q361. Input validation should occur:
A. On both client and server sides
B. Client side only
C. Database only
D. UI only
Answer: A
Explanation: Redundant validation ensures integrity.

Q362. Output encoding prevents:
A. Cross-site scripting (XSS)
B. Denial of Service
C. Buffer overflow
D. SQL injection
Answer: A
Explanation: Encoding neutralizes malicious output.

Q363. Secure coding guidelines should be:
A. Documented, enforced, and reviewed regularly
B. Optional
C. One-time only
D. Separate from policy
Answer: A
Explanation: Continuous improvement maintains secure software culture.

Q364. Security testing should be integrated into:
A. Every stage of the SDLC
B. Only at deployment
C. Only post-release
D. Maintenance only
Answer: A
Explanation: Continuous validation ensures resilience throughout lifecycle.

Q365. The Agile methodology affects security by:
A. Requiring iterative security integration (“shift-left”)
B. Ignoring security
C. Removing reviews
D. Extending release cycles
Answer: A
Explanation: Security adapts to iterative releases in Agile environments.

Q366. DevSecOps emphasizes:
A. Embedding security in development and operations workflows

B. Manual pen testing
C. Only compliance reporting
D. Network segmentation
Answer: A
Explanation: DevSecOps integrates automation, CI/CD, and security checks.

Q367. Secure coding standards examples include:
A. CERT Secure Coding, MISRA, OWASP ASVS
B. ISO 9001
C. COBIT
D. COSO ERM
Answer: A
Explanation: Coding standards enforce consistent security patterns.

Q368. Buffer overflows occur when:
A. Data exceeds memory bounds of a variable
B. CPU overheats
C. Log files rotate
D. Encryption fails
Answer: A
Explanation: Overflows can overwrite adjacent memory and execute code.

Q369. Race conditions can be mitigated by:
A. Proper synchronization and locking mechanisms
B. Weak randomization
C. Disabling threading
D. Encryption
Answer: A
Explanation: Synchronization ensures data integrity under concurrency.

Q370. The purpose of code signing is to:
A. Ensure code integrity and authenticity
B. Encrypt all code
C. Obfuscate algorithms
D. Improve performance
Answer: A
Explanation: Signed code verifies trusted origin.

Q371. Configuration management in software security includes:
A. Version control, build integrity, and environment consistency
B. Encryption
C. Network ACLs
D. Database tuning
Answer: A
Explanation: Ensures traceability and integrity across versions.

Q372. Software escrow agreements protect:
A. Source code availability if vendor fails to support
B. Encryption keys
C. Test data
D. User credentials
Answer: A
Explanation: Escrow ensures business continuity in vendor dependency.

Q373. The main principle of secure design is:
A. Fail securely, least privilege, and defense in depth
B. Obfuscate functions
C. Use default passwords
D. Hide documentation
Answer: A
Explanation: Secure design reduces vulnerability exposure.

Q374. AI/ML model security requires protecting:
A. Training data, model weights, and inference APIs
B. Network only
C. Users
D. GPUs
Answer: A
Explanation: Models and datasets are valuable intellectual assets.

Q375. Adversarial machine learning targets:
A. Model manipulation and evasion attacks
B. Network routing
C. Database schema
D. IAM
Answer: A
Explanation: Attackers craft inputs to deceive models.

Q376. Data poisoning attacks affect:
A. Training data integrity
B. Network latency
C. Disk redundancy
D. GPU health
Answer: A
Explanation: Compromised data corrupts model behavior.

Q377. Model inversion allows attackers to:
A. Reconstruct sensitive training data from model outputs
B. Decrypt traffic
C. Replace datasets
D. Increase performance

Answer: A
Explanation: Inversion violates confidentiality.

Q378. Secure API development requires:
A. Authentication, authorization, rate limiting, and input validation
B. Plain HTTP
C. Open endpoints
D. No logging
Answer: A
Explanation: APIs are common attack vectors.

Q379. Using open-source software requires:
A. Reviewing licenses and vulnerabilities
B. Automatic trust
C. Avoiding version control
D. Ignoring dependencies
Answer: A
Explanation: OSS components must be monitored for risks.

Q380. Continuous integration pipelines should include:
A. Automated security scanning before build deployment
B. Manual deployment
C. Static logging only
D. None
Answer: A
Explanation: CI/CD automation ensures early issue detection.

Q381. Security regression tests ensure:
A. Previous vulnerabilities remain fixed after updates
B. Features added
C. Costs lowered
D. Logs cleared
Answer: A
Explanation: Prevents reintroduction of flaws.

Q382. In secure SDLC, maintenance phase includes:
A. Patch management, monitoring, and vulnerability review
B. Product marketing
C. Risk avoidance
D. Manual testing only
Answer: A
Explanation: Ensures ongoing protection after deployment.

Q383. Input sanitization prevents:
A. Injection and format string attacks

B. CPU overheating
C. Encryption
D. Privilege escalation
Answer: A
Explanation: Cleans input to enforce safe patterns.

Q384. AI model lifecycle security includes:
A. Governance, validation, monitoring, and retraining
B. Static storage
C. Firewalls only
D. Code review
Answer: A
Explanation: Models require continuous oversight to mitigate drift.

Q385. Source code repositories must enforce:
A. Access control, integrity checks, and branch protection
B. Anonymous write access
C. Unencrypted commits
D. Shared credentials
Answer: A
Explanation: Repositories hold intellectual property and must be protected.

Q386. Continuous delivery differs from continuous deployment by:
A. Requiring manual approval before release
B. Automatic production push
C. Code compilation
D. Automated rollback
Answer: A
Explanation: Continuous delivery stops before auto-release.

Q387. The main function of Software Bill of Materials (SBOM) is to:
A. List all components and dependencies for transparency
B. Optimize build time
C. Track licenses only
D. Encrypt binaries
Answer: A
Explanation: SBOMs support vulnerability and supply chain management.

Q388. Supply chain attacks exploit:
A. Compromise of third-party components or build processes
B. End-user password
C. Encryption weakness
D. Firewalls
Answer: A
Explanation: Third-party code introduces external risk.

Q389. Secure code repositories should enforce:
A. MFA and signed commits
B. Anonymous commits
C. Plaintext passwords
D. None
Answer: A
Explanation: Signed commits verify code authorship.

Q390. Waterfall SDLC models are:
A. Sequential with late security integration
B. Agile
C. Continuous
D. None
Answer: A
Explanation: Traditional waterfall adds risk of late vulnerability detection.

Q391. The purpose of “peer review” in development is to:
A. Catch defects early through collaboration
B. Reduce development speed
C. Replace testing
D. Archive code
Answer: A
Explanation: Peer review increases quality and security awareness.

Q392. Secure libraries should be:
A. Updated frequently and validated via digital signatures
B. Static forever
C. Modified manually
D. Ignored
Answer: A
Explanation: Updated libraries patch known vulnerabilities.

Q393. Secure error handling must:
A. Avoid exposing sensitive details in error messages
B. Display stack traces to users
C. Log plaintext passwords
D. Stop logging
Answer: A
Explanation: Errors should be generic to users and detailed in logs.

Q394. The best way to verify security compliance before release is:
A. Conduct pre-production security review and sign-off
B. Skip QA
C. Trust developer judgment
D. Run marketing test

Answer: A
Explanation: Gate reviews validate readiness for deployment.

Q395. Memory-safe languages like Rust and Go reduce:
A. Buffer overflows and memory corruption
B. Encryption
C. Logging
D. SQL errors
Answer: A
Explanation: Memory safety prevents class of low-level vulnerabilities.

Q396. Secure session management includes:
A. Random session IDs, timeout, and secure cookie flags
B. Static tokens
C. Plain HTTP cookies
D. Shared keys
Answer: A
Explanation: Prevents hijacking and fixation.

Q397. AI software testing should validate:
A. Bias, explainability, and resilience under adversarial inputs
B. GPU temperature
C. Network latency
D. Data backup
Answer: A
Explanation: Ethical and robust AI requires multidimensional validation.

Q398. Which ISO standard provides secure SDLC guidance?
A. ISO/IEC 27034
B. ISO 9001
C. ISO 22301
D. ISO 42001
Answer: A
Explanation: ISO 27034 defines application security lifecycle processes.

Q399. Secure DevOps pipelines should include:
A. Code scanning, secret detection, and dependency checks
B. Plaintext credentials
C. Unrestricted builds
D. Manual approval only
Answer: A
Explanation: Automation ensures consistent protection.

Q400. Final step of secure software development is:
A. Deployment with continuous monitoring and feedback loops

B. Archiving source code only
C. Deleting repositories
D. Granting admin rights
Answer: A
Explanation: Continuous feedback maintains long-term software security.