CISSP®

Practice Assessment

1. Alice runs a small online retail company; many of her customers are from the United States. Currently, she accepts only blockchain-based payment, but she is considering the use of credit cards. After investigating Payment Card Industry Data Security Standard (PCI DSS) requirements, she decides that the cost of compliance would outweigh the additional revenue. Which of the following best describes this decision?
   A. Social engineering
   B. PCI DSS Merchant Level 3
   C. Card verification value (CVV)
   D. Risk avoidance

2. According to the (ISC)² ethics policy, complaints must be submitted _____.
   A. through the (ISC)² website
   B. in writing
   C. anonymously
   D. within one year of the accused infraction

3. The business impact analysis (BIA) should consider all of the following *except*:
   A. The value of the organization's assets
   B. Industry standards
   C. Threats specific to the organization
   D. The likelihood of loss

4. The _____ is the length of time an organization can suffer the loss of its critical path before ceasing to be a viable enterprise.
   A. recovery time objective (RTO)
   B. recovery point objective (RPO)
   C. maximum allowable downtime (MAD)
   D. annual loss expectancy (ALE)

5. Which of the following security instruction options offers the most potential for real-time feedback?
   A. Computer-based training
   B. Rote memorization
   C. Live training
   D. Reward mechanisms

6. Which of the following is a formal, detailed description of the responsibilities between an organization and an employee?
   A. Nondisclosure agreement (NDA)
   B. Employment contract
   C. Acceptable use policy (AUP)
   D. Security policy

7. Which of the following is promulgated by senior management and outlines the organization's strategic vision and goals?
   A. Policy
   B. Procedures
   C. Guidelines
   D. Standards

8. Which of the following entities is the individual human associated with a particular set of personally identifiable information (PII)?
   A. Data owner
   B. Data controller
   C. Data subject
   D. Data processor

9. Organizations in which of the following countries are not allowed to process EU citizen personal data?
   A. Germany
   B. Argentina
   C. Singapore
   D. United States

10. Which of the following is not a common trait of DRM solutions?
    A. Persistence
    B. Continuous audit trail
    C. Automatic expiration
    D. Virtual licensing

11. All of the following are common intellectual property licensing options *except*:
    A. Site license
    B. Creative commons
    C. Shareware
    D. Trademark

12. What is the term for the criminal practice of extorting victims by encrypting their data?
    A. Malware
    B. Hacktivism
    C. Ransomware
    D. Trojan horse

13. Which of the following is not a common facet of data privacy laws?
    A. Scope limitation
    B. Subject notification
    C. Enhancement provision
    D. Participation option

14. Which of the following is the American law governing protection of medical-related privacy information?
    A. Sarbanes–Oxley Act (SOX)
    B. Gramm–Leach–Bliley Act (GLBA)
    C. Personal Information Protection and Electronic Documents Act (PIPEDA)
    D. Health Insurance Portability and Accountability Act (HIPAA)

15. Which of the following is not an industry standard for data security?
    A. Payment Card Industry Data Security Standard (PCI DSS)
    B. Cloud Security Alliance Security Trust and Assurance Registry (CSA-STAR)
    C. General Data Protection Regulation (GDPR)
    D. ISO 27001

16. Which of the following is a contractual industry standard?
    A. Payment Card Industry Data Security Standard (PCI DSS)
    B. Federal Risk and Authorization Management Program (FedRAMP)
    C. HIPAA is the Health Information Portability and Accountability Act (HIPAA)
    D. General Data Protection Regulation (GDPR)

17. Which of the following enforcement mechanisms is best used for regularly occurring, repeated common activities?
    A. Service contract
    B. Service-level agreement (SLA)
    C. Nondisclosure agreement (NDA)
    D. Background check

18. Which of the following is not included in the STRIDE threat model? Which of the following is not included in the STRIDE threat model?
    A. Repudiation
    B. Denial of service (DoS)/distributed denial of service (DDoS)
    C. Simulation
    D. Tampering with data

19. Which of the following is not a common audit methodology?
    A. ISO certification
    B. Cloud Security Alliance Security Trust and Assurance Registry (CSA-STAR) evaluation
    C. Statement on Standards for Attestation Engagement Service Organization Control (SSAE SOC) reports
    D. Gramm–Leach–Bliley Act (GLBA) transactions

20. Which of the following is not a common security control category?
    A. Destructive
    B. Preventative
    C. Deterrent
    D. Directive

21. In security management, the need-to-know element should be provided by the
    A. Operating system
    B. Information owner
    C. System owner
    D. Data custodian

22. How can an asset classification program enhance access controls?
    A. By satisfying the requirements of internal audit
    B. By allowing the source to be modified through a rigorous process
    C. By ensuring that all relevant security events are logged
    D. By setting controls to protect assets

23. The main benefit of a data classification program is
    A. To meet military and government compliance requirements
    B. To allow data to receive the appropriate level of protection
    C. To allow the organization to be cost-effective
    D. To meet privacy requirements

24. The network security administrator has submitted her request to implement additional security controls to an application. Her request should be reviewed and approved by
    A. The operations manager
    B. The audit function
    C. The owner
    D. The controller

25. The role of the information custodian should not include which of the following?
    A. Classification of information
    B. Restoration of corrupted or lost information
    C. Regular backup of information
    D. Ensuring availability of information

26. Privileged users should be subject to periodic recertification to maintain the level of privileges that have been assigned. The rationale for the recertification should be based on all of the following EXCEPT
    A. The duration of time needed for access
    B. Organizational politics
    C. A business or operational need that requires privileged access
    D. The requirements of auditors

27. Asset classification is the accountability of the
    A. Asset owner
    B. Asset custodian
    C. Asset steward
    D. Asset processor

28. The correct amount of security is dictated by
    A. More is better
    B. The level of risk that exists
    C. The level determined by the subjects
    D. The level of value of the asset

29. When establishing the value of information, the least important factor is
    A. Trade secrets
    B. Operational impact
    C. Quantity of information
    D. Value to outsiders

30. Who normally operates technology systems?
    A. Custodians
    B. Owners
    C. Controllers
    D. IT function

31. Which of the following is the BEST definition of a baseline?
    A. Images of configurations parameter
    B. Minimum levels of protection requirements
    C. Step-by-step required actions
    D. Specific hardware recommendations

32. Which of the following is the BEST method for destroying data on magnetic media without destroying the media itself?
    A. Using a commercially graded cleanser
    B. Using the erase or delete function of technology systems
    C. Subjecting the media to reinitialization
    D. Using a overwriting utility program

33. The decision to encrypt information over a network is driven by
    A. The estimated monetary value of the information
    B. The classification level as determined by the owner
    C. The qualitative value of the information
    D. The requirements of legal commitments

34. What is the proper method of disposing of data on optical media?
    A. Degaussing
    B. Overwriting
    C. Destruction
    D. Purging

35. Information ethics and compliance deem that an organization has an obligation to protect information, this accountability includes ensuring that the
    A. Subject has complete control over the content
    B. Information is kept current
    C. Information is stored and processed securely
    D. Subject controls the destruction of the information

36. Which of the following is a key responsibility of the custodian of data?
    A. Data content and backup
    B. Integrity and security of the data
    C. Authentication of user access
    D. Classification of data elements

37. When personal data is maintained about a natural or legal person, that person is defined under privacy laws as a
    A. Data subject
    B. Data controlee
    C. Data controller
    D. Data processor

38. Which of the following needs to be intelligible with end-to-end encryption?
    A. Private key
    B. Encryption algorithm
    C. Time to live parameter
    D. Network routing information

39. An advantage of link encryption in a network might be
    A. Encrypts all information including routing and header information
    B. Protects data from start to finish through the entire network segment
    C. Makes key distribution between end points easier
    D. Allows more efficient transmission across networks

40. Which of the following is the BEST definition of data remanence?
    A. The data that has been magnetically written onto the media by altering the magnetic media sector
    B. The residual physical representation of the data that has in some way been erased
    C. The data that has been degaussed by using proper technology
    D. The data rendered unusable through overwriting technologies

41. The four types of system and system security engineering processes are:
    A. Technology processes, technology management processes, enabling processes, agreement processes
    B. Technical processes, technical management processes, enabling processes, agreement processes
    C. Technical processes, technical management processes, augmentation processes, acquisition processes
    D. Technology processes, technical management processes, acquisition processes, supply processes

42. The Bell–LaPadula (BLP) security model is an example of a security model that is focused on protecting _____.
    A. Information deletion
    B. Integrity
    C. Confidentiality
    D. Against improper modification

43. Three types of security controls are:
    A. Preventative, operating, corrective
    B. Preventative, detective, technology
    C. Preventative, detective, corrective
    D. Policy, preventative, corrective

44. The process of customizing security controls to fit the specific security needs of a particular system in a particular operating environment is known as:
    A. Tailoring controls
    B. An unauthorized activity that must be reported
    C. Adequate security
    D. Control tweaking

45. Which of the following are security capabilities integrated to some extent into most major information systems:
    A. Access control
    B. Memory management
    C. Process isolation
    D. All of the above

46. A TPM is a _____ component known as the _____.
    A. Software, Trusted Platform Module
    B. Firmware, Technical Partition Manager
    C. Hardware, Trusted Platform Module
    D. Hardware, Technical Partition Manager

47. Software as a service (SaaS) is considered to be what type of system?
    A. Exclusively operated in private data centers
    B. Mainframe-based
    C. Cloud-based
    D. Outmoded and obsolete

48. Select the best answer: A private cloud deployment:
    A. Can exist only within the direct control of the user
    B. Supports a single organization
    C. Is open for use by the general public
    D. Is restricted to a particular community of users

49. Select the best system type based on the following characteristics: small form factor, low power utilization, may interface with the physical world, pervasively deployed in consumer products.
    A. Supervisory control and data acquisition (SCADA)
    B. Programmable logic controller (PLC)
    C. Internet of Things (IoT)
    D. Client-based

50. Select the system type most susceptible to the following vulnerabilities: loss, theft, weak access controls, communication interception, limited function operation system.
    A. Embedded
    B. Control
    C. Mobile
    D. Server-based

51. Pick the best response. Site and facility design should include consideration for:
    A. Firewall placement
    B. Personnel screening
    C. Security architectural models
    D. Security inherited from telecommunications providers

52. Select the best response. When designing exterior lighting, you should consider:
    A. Impact on video surveillance, possible shadowed areas
    B. Infrared illumination
    C. Impact on cut/break sensors
    D. Impact on motion sensors

53. Select the best answer item from the list below. Two primary types of fire suppression systems are:
    A. Water-based, Halon
    B. Halon, sprinkler
    C. Water-based, gas-based
    D. Water-based, sprinkler

54. Select the best response from the lists below. Environmental issues to consider as part of a site or facility plan include:
    A. Hurricane, tornado, flooding, mudslide
    B. Insider threat, natural threat
    C. Power, internet service provider (ISP)
    D. Personnel screening, sprinkler placement

55. Encrypting a message with a private key in an asymmetric system provides?
    A. Confidentiality
    B. Proof of receipt
    C. Proof of origin
    D. Message availability

56. One of the largest disadvantages of symmetric key cryptography is?
    A. Scalability
    B. Availability
    C. Computing resource requirements
    D. Confidentiality

57. A hybrid cryptography system uses?
    A. Symmetric algorithms for key distribution
    B. Asymmetric algorithms for message confidentiality
    C. Symmetric algorithms for proof of origin
    D. Symmetric algorithms for fast encryption

58. Digital Signatures do not allow for?
    A. Unauthorized modifications to a message
    B. Authentication of the signatory
    C. Third-party verification of a sender
    D. Confidentiality of a document

59. The process of hiding characters of plaintext with non-cipher characters is referred to as?
    A. Steganography
    B. Optimal Asymmetric Encryption (OAE)
    C. Null cipher
    D. Expansion

60. For what application would Electronic Code Book (ECB) mode of symmetric block ciphers be MOST desirable?
    A. When multiple sub-keys are going to be used
    B. When more efficient operation is a high priority
    C. Where the plaintext to be encrypted is very small
    D. When other block cipher modes are unavailable

61. Hash collisions are?
    A. Failures of a given cryptographic hash function to complete successfully
    B. Two different input messages that result in the same message digest value
    C. Repetitions within a message digest that indicate weaknesses in the hash algorithm
    D. Matching message digests found during the verification of a digital signature

62. Where parties do not have a shared secret, and large quantities of sensitive information must be transmitted; the most efficient means of transferring information is to use a hybrid encryption technique. What does this mean?
    A. Use of public key encryption to secure a secret key, and message encryption using the secret key
    B. Use of the recipient's public key for encryption and decryption based on the recipient's private key
    C. Use of software encryption assisted by a hardware encryption accelerator
    D. Use of elliptic curve encryption

63. You come into work on Monday and your workstation is booting up after being turned off over the weekend. When your system starts up, you note that you can't access any resources. When you look at your network configuration, you note that your workstation has an IP address of 169.254.1.1. What is most likely the cause?
    A. Your computer has a virus.
    B. A Dynamic Host Configuration Protocol (DHCP) is not responding.
    C. The Domain Name System (DNS) server is not responding.
    D. None of the above.

64. You are trying to use an external Domain Name System (DNS) server as a forward lookup on your internal network, but you cannot get it to resolve a name to an IP address. What is the probable cause?
    A. Port 67 is being blocked outbound on your network.
    B. Port 67 is being blocked inbound on your network.
    C. Port 53 is being blocked inbound on your network.
    D. Port 53 is being blocked outbound on your network.

65. At what layer of the Open Systems Interconnection (OSI) model are segments transmitted?
    A. Layer 4 or Transport
    B. Layer 1 or Physical
    C. Layer 2 or Data-Link
    D. Layer 0 or Operational

66. A Simple Network Management Protocol (SNMP) system is monitoring services and systems on your network. You discover a breach in the network management system. What might be the cause?
    A. The default public community string was never changed.
    B. The public community string was left unprotected.
    C. The public community string was passed out to the users on your network.
    D. The default private community string was never changed.

67. What statement is true about software-defined networks (SDNs)?
    A. The control plane has no network operating system support.
    B. The infrastructure plane manages the forwarding of data.
    C. The management plane is designed for applications.
    D. All planes have the same function.

68. What is a benefit of Network Function Virtualization (NFV)?
    A. Manage application pools
    B. Mitigate attack vectors
    C. Support transition from Capital Expenditure (CapEx) to Operational Expenditure (OpEx)
    D. Process data overflow

69. A workstation has made a request to synchronize (SYN) with your workstation, and your workstation responds with an acknowledgement (ACK) and a request to SYN with the requesting workstation. The next message you receive is a request to SYN. Explain "What could this be the beginning of"?
    A. Normal three-way handshake
    B. Teardrop attack
    C. Smurf attack
    D. SYN flood

70. Company X was on alert that they could be under attack after they referred to a baseline of activity that appeared higher than normal but without any service outage, disruption, or manipulation of services. What dynamic analysis engine put them on alarm?
    A. Protocol anomaly
    B. Traffic anomaly
    C. Signature matching
    D. None of the above

71. What Voice over Internet Protocol (VoIP) concern is tied to variation of traffic timing?
    A. Jitter
    B. Sequence errors
    C. Traffic delay
    D. Reverse traffic delay

72. Two users are making decisions on how they want to create an IPSEC connection. Their most important concern is to ensure that when the connection is created, they are certain that it is made between the two of them. How should the connection be created?
    A. Encapsulating Security Payload (ESP)
    B. Authentication Header (AH)
    C. Diffie Hellman
    D. Star Property

73. What is the tunneling in Layer 2 Tunneling Protocol (L2TP)?
    A. High level encryption
    B. Encapsulation
    C. Low level encryption
    D. Medium level encryption

74. A user has need to keep their transmission contents secret from their computer to another computer node at another location. What is the mode that should be selected for the stations to run?
    A. Symmetric
    B. Transport
    C. Tunnel
    D. Asymmetric

75. A request has been made to a web application by means of a URL and within the request it contains "../", what should the system do with this request?
    A. Process the request
    B. Wait for the next instruction
    C. Reject the request
    D. Embed the request into another request

76. Which ISO document address the 7-layer OSI model?
    A. 27001
    B. 27002
    C. 31000
    D. 7498

77. A rogue wireless device has been found on a network, and the way it was discovered is that individuals were not able to get a DHCP address. What should be done to prevent this in the future?
    A. Turn on port authentication on the host switches.
    B. Create reservation on the DHCP server.
    C. Set the clients to Bootstrap Protocol (BootP).
    D. Expand the reservation pool on the DHCP server.

78. Your organization has made the decision to implement a software-defined network (SDN). What equipment will be managed within the new environment?
    A. Routers and switches
    B. Switches and servers
    C. Switches, servers, and routers
    D. All systems in the data center

79. Your organization must still manage a Multiprotocol Label Switching (MPLS) network while converting their internal network system to SDN. You want to have a better understanding of your prioritized traffic flows on the MPLS to match your SDN design. What field in the header will provide the information of a MPLS label?
    A. Stack
    B. TTL
    C. Class of Service
    D. QoS Bit

80. Which "Generation" of cellular service is being designed to accommodate software-defined network (SDN)?
    A. 2G
    B. 4G
    C. 5G
    D. 6G

81. In which cellular service is each call encoded with a unique key?
    A. Startec Service X
    B. Global System for Mobiles (GSM)
    C. Code Division Multiple Access (CDMA)
    D. 3G

82. In what attack can a user on one VLAN connect to another unauthorized VLAN via Dynamic Trunking Protocol (DTP) link?
    A. Arp attack
    B. MAC flood
    C. 802.1Q and Inter-Switch Link Protocol (ISL) Tagging attack
    D. Double-Encapsulated 802.1Q/Nested VLAN attack

83. Your organization maintains a wide range of intellectual property that includes digital documents, audio files, and video content. To support requirements of access control methodologies that can maintain what groups can access resources based upon job descriptions, what access control tool type should be implemented?
    A. Role-based access control (RBAC)
    B. Mandatory access control (MAC)
    C. Discretionary access control (DAC)
    D. Attribute-based access control (ABAC)

84. Which document specifies access control models as "formal presentations of the security policies enforced by access control systems?"
    A. NIST SP 800-53
    B. NIST SP 800-192
    C. NIST SP 1-2
    D. ISO 27001

85. Which of the following could represent an identity management risk?
    A. Provisioning a third-party identity as a service (IDaaS) without a proper SOC 2 report providing an opinion of the organization's management of the trust principles.
    B. Using Kerberos as a single-sign-on solution.
    C. Reviewing business policy before choosing a solution.
    D. Curtailing logging into a system during non-business hours.

86. When the data owner manages classification of data, what control is being envisioned?
    A. Authentication
    B. Authorization
    C. Accountability
    D. Identification

87. Which biometric reader has the most rapid authentication?
    A. Retinal scanning
    B. Iris recognition
    C. Voice recognition
    D. Rapid eye movement scanner

88. What is Open Web Application Security Project (OWASP) Top 10 number 2 threat?
    A. Relational engineering
    B. Injection
    C. Weak authentication and session management
    D. Using components with known vulnerabilities

89. The Digital Identity Guidelines of NIST SP 800-63-3 contain recommendations to support
    A. Role-based access controls (RBACs)
    B. Maintenance of a security policy
    C. Maintenance of governance
    D. Requirements for identity proofing and registration

90. A Credential Service Provider is responsible for
    A. Teaming network interface cards for redundancy
    B. In-person identity proofing
    C. Retroactive account deletion
    D. Proactive account deletion

91. What are the four components of Security Assertion Markup Language (SAML)?
    A. Attributes, bindings, protocols, profiles
    B. Attributes, bindings, protocols, pending items
    C. Attributes, bindings, protocols, pin-types
    D. Attributes, bindings, profiles, people

92. A claimant is asked to provide in-person proof of their identity. What minimum level of assurance does the in-person proofing request satisfy?
    A. Identity Assurance Level 1 (IAL1)
    B. Identity Assurance Level 2 (IAL2)
    C. Identity Assurance Level 3 (IAL3)
    D. Identity Assurance Level 4 (IAL4)

93. Federation Assurance Level (FAL) refers to the strength of an assertion in a
    A. Federal institution
    B. Federated environment
    C. An SQL environment
    D. Wireless access point

94. NIST SP 800-63-3 enrollment process allows for credential production to made in the following forms
    A. Symmetric keys
    B. Public keys
    C. Personal keys
    D. Smart keys

95. An organization has various forms of intellectual property that are labeled as confidential trade secrets. They need to keep the trade secrets with the highest level of protection available. The trade secrets are kept in various media types: audio, video, and digital documents. Some of the access control methodology can be represented by traditional groups, some of the access control methodology can be represented by specific conditions of access like time and location, and some of the access control methodology is purely left to individual data owners. Which access control methodology best fits the organization need?
    A. Rule-based access control (RBAC)
    B. Attribute-based access control (ABAC)
    C. Role-based access control (RBAC)
    D. Discretionary access control (DAC)

96. Which of the following is a part of the creation, management, and disposal of system user accounts?
    A. Identity and referral services
    B. Identity and access management
    C. Identity and identity destruction
    D. Identity and access referral

97. NIST SP 800-145 defines three cloud service models. Which one of the three would Identity-as-a-Service (IDaaS) be closely identified with?
    A. Software as a service (SaaS)
    B. Platform as a service (PaaS)
    C. People as a service (PeaaS)
    D. Infrastructure as a service (IaaS)

98. What activity would represent an outcome of identity and access management accountability process?
    A. Delete a user account
    B. Review user ID access
    C. Receiving a request to provision a new user ID
    D. Calibrating a time division multiplexing chain

99. What role is authentication information based upon that is utilized during the identity proofing process?
    A. Authorized entity
    B. Claimant
    C. Monitor
    D. Revealer

100. A primary goal of federated identity management (FIM) is to
    A. Allow ease of collusion
    B. Facilitate the ease of ID creation
    C. Reconcile the identity proofing process
    D. Allow disparate organizations to share resources

101. When Type I errors are equal to Type II errors on a biometric system, what state has been reached?
    A. Crossover Elusive Rate
    B. Crossover Elliptic Rate
    C. Crossover Error Rate
    D. Crossover Erudite Rate

102. What scenario below represents multi-factor authentication?
    A. User ID and a statically assigned numeric pin
    B. An iris scan and signature dynamics
    C. Geo-location and a password
    D. A type I and type II device

103. Your organization has system administrators that have management control of server systems that contain highly confidential data which is critical to business continuity. What type of test is most appropriate to reveal your risk?
    A. External
    B. Internal
    C. Third-party
    D. None of the above

104. Vulnerability scanning could be used to determine_____.
    A. System portability
    B. Process improvement
    C. Patch levels
    D. Lack of training

105. A company is hosting a web front-end service that has users that access services from around the world. In recent weeks, they've noticed a drop in the amount of "clicks" to their website. For the users that are still accessing the website, they would like to understand what their experiences are. What tool would you suggest they use?
    A. Website monitoring
    B. Near real monitoring
    C. TCP monitoring
    D. Real user monitoring

106. What method should be used to test the thoroughness of the logic of code?
    A. Black-box
    B. Red box
    C. Automated testing
    D. Static testing

107. What are proper considerations to make when selecting a testing method?
    A. Attack surface and application type
    B. Attack surface and program readiness
    C. Attack surface and process types
    D. Attack surface and relationship sets

108. Code-based testing is also known as _____
    A. Black-box testing
    B. Structural testing
    C. Grey-box testing
    D. None of the above

Scenario for Questions 109–111

A service desk maintains a mandatory availability window of 24 × 7 × 365. The executive management within the organization notices that employees within the company tend to let service desk issues develop with customer satisfaction until they are escalated up to executive management level. Many of the issues are related to what is perceived to be the unaccepted amount of time it takes to resolve calls and the lack of communication of call status. This puts the organization at risk for losing clients. Executive management would like to adopt an approach to this problem, and they come to you for assistance.

109. What would you recommend to the executive management of this company for being able to foresee problems as they describe above?
    A. Terminate employees whose names come up in the complaints
    B. Rewrite the security policy and re-evaluate business mission
    C. Develop key risk indicators (KRIs)
    D. Develop key performance indicators (KPIs)

110. What action should be taken to address the perceived response of the employees at the service desk?
    A. Terminate employees whose names come up in the complaints
    B. Create a training program
    C. Create an awareness program
    D. Stop all activity and regroup.

111. What would be a way to discern if the desired change is being achieved?
    A. Get on the phone with the service desk and listen in
    B. Review the 360 feedback reports on the managers
    C. Increase of positive comments
    D. Develop and implement KPIs

112. What should be avoided in test output data?
    A. Metadata
    B. Simulated data
    C. Sensitive data
    D. None of the above

Scenario for Questions 113–116

Your company is seeking to outsource business process services to a service provider. Although the service provider has only been in business for nine months, they have several recommendations from industry leaders in the field. This service provider of choice has made a competitive bid for the request for proposal that was published by your company. Your company has a need to maintain the materials that they will process with a high degree of confidentiality for the data, and your most critical business process data has an maximum tolerable downtime (MTD) of three hours. Your company wants the highest proof possible that the controls the processing company maintains are adequate to meet your company needs.

113. Which audit should be done to address the concern about the length of time the service provider has been in business?
    A. SOC 2
    B. SOC 1
    C. SOC 3
    D. None of the above

114. What audit should be done to provide assurance about the availability and confidentiality of the service provider?
    A. SOC 1
    B. SOC 2
    C. SOC 3
    D. SOC 4

115. What *type* of audit should be done on the service provider?
    A. Type I
    B. Type II
    C. Type III
    D. Type IV

116. Which trust services principles are most appropriate for the auditor to focus on?
    A. Confidentiality and availability
    B. Processing integrity and privacy
    C. Privacy and confidentiality
    D. Security and processing integrity

117. List examples of security awareness sources for an awareness program.
    A. Job skills development
    B. Posters with reminders to change password
    C. Procedures to test a system
    D. Accreditation of a tested system

118. What control is specified in ISO 27002 concerning test data?
    A. Test should not be done in production environments
    B. Test data are always a clear path to test schemes
    C. Test data are necessary in DevOps
    D. Test data should avoid containing personally identifiable information (PII)

119. Third-party assessments are _____
    A. Too costly
    B. Slow and ineffective
    C. Driven by some regulations
    D. Always necessary.

120. What is the primary purpose of a negative test?
    A. To verify the operating power of a system
    B. To ensure graceful handling of unexpected input
    C. Reconcile the identity proofing process
    D. Allow disparate organizations to share resources

121. Interface testing can be used to _____
    A. Check and verify if all the interactions between the application and a server are executed properly
    B. Check the connections between fail-safe and fail-secure
    C. Run test in a loop till errors are made evident.
    D. none of the above

122. Once code inspection is complete, what kind of software testing occurs?
    A. User acceptance testing
    B. Business case testing
    C. Unit level testing
    D. Test sophistication

123. Which of the following terms is *most* associated with the concept of need-to-know?
    A. Static testing
    B. Social engineering
    C. Compartmentalization
    D. Nondisclosure agreements

124. Which of the following is *not* true about privileged accounts?
    A. Privileged account holders should be subject to more extensive background checks than regular account holders.
    B. They should be temporary.
    C. They should be subject to more extensive auditing.
    D. They should be granted only for remote access.

125. Which of the following is *not* a benefit the organization realized from job rotation?
    A. Improved employee morale
    B. Reduction in single points of failure in staffing
    C. Elimination of the possibility of social engineering
    D. Aids in detecting internal threats

126. In which phase of the information lifecycle is data moved from the production environment into long-term storage?
    A. Create
    B. Share
    C. Store
    D. Archive

127. What is usually the enforcement mechanism of a service-level agreement (SLA)?
    A. Incarceration
    B. Regulatory capture
    C. Early withdrawal
    D. Financial penalties

128. Which of the following is *not* typically reflected in the asset inventory?
    A. The asset owner
    B. The asset size
    C. The asset location
    D. The asset value

129. All of the following departments typically will be represented on the Change Management Board (CMB) *except*:
    A. Sales/marketing
    B. Accounting/finance
    C. Security office
    D. The user community

130. What should always be included in the patch process?
    A. The option to roll back to the last known good system state
    B. Contacting the patch issuer to seek clarification
    C. Instant and immediate application of patches to all affected systems
    D. Regulator notification

131. Patches should be tested _____.
    A. daily
    B. in a test bed that mimics the production environment
    C. only on external, off-premise systems
    D. in the jurisdiction in which they were issued

132. Which of the following is a *preventative* measure to counter the possibility of lost/stolen media?
    A. Digital watermarking
    B. Proper and thorough labeling
    C. Online tracking mechanisms
    D. Secure disposal

133. Which of the following is *not* an acceptable, suggested practice in dealing with third-party security vendors?
    A. The use of nondisclosure agreements
    B. Regulator participation
    C. The use of service-level agreements (SLAs)
    D. Insurance/bonding

134. One of the best benefits of anti-malware systems is _____.
    A. evidence of due diligence
    B. prevent social engineering attacks
    C. no financial cost
    D. no impact on productivity

135. Which of the following entities/activities is *not* usually involved in incident detection?
    A. Log analysis
    B. Firewalls
    C. Users
    D. Human resource (HR)

136. Which of the following is *not* one of the main variables affecting how an organization initially addresses an incident?
    A. Time
    B. Risk
    C. Impact
    D. Location

137. All incident management actions should be _____.
    A. instantaneous
    B. expensive
    C. contracted
    D. documented

138. Who should decide how an incident would be addressed?
    A. Security officer
    B. Law enforcement
    C. Senior management
    D. Regulators

139. Which kind of investigation should be performed if the organization does not want to involve law enforcement, external parties, or a court action?
    A. Civil
    B. Criminal
    C. Regulatory
    D. Administrative

140. Which of the following is used to ensure evidence collected is evidence presented to a court?
    A. Nondisclosure agreement
    B. Job rotation
    C. Chain of custody
    D. Forensic analysis

141. Which of the following is *not* a trait expected of evidence presented to a court?
    A. Irrefutable
    B. Admissible
    C. Comprehensive
    D. Objective

142. Which of the following is *not* a typical location for placement of an intrusion detection system/intrusion prevention system (IDS/IPS)?
    A. Network perimeter
    B. Fire suppression monitoring systems
    C. Individual hosts
    D. Network devices

143. How should buffer overflow vulnerabilities be addressed?
    A. By using blacklists that contain all characters that can be potentially harmful
    B. By installing patches to fix buffer overflow vulnerabilities
    C. By using the latest programming development methodologies that resist well-known vulnerabilities
    D. By using strongly typed programming languages, implementing bounds and input checking controls, and using safe functions

144. How is an interpreted language application different from a compiled language application?
    A. Interpreted languages do not require the entire source code to be compiled to machine code before the application can run.
    B. Interpreted applications are limited to specific platform; compiled applications can run on any platform.
    C. Compiled applications are limited to a specific platform; interpreted applications can run on any platform.
    D. Interpreted applications execute faster than compiled applications.

145. Why is it important to build security into the application as opposed to adding it later?
    A. It is not, both approaches are equally appropriate.
    B. It conforms to the concept of “security by obscurity,” which provides adequate security by hiding it within the application itself.
    C. Building security into the application provides more layers of security and can be harder to circumvent.
    D. Building security into the application can reduce development time, allowing the application to be released to production sooner.

146. What is a common issue to consider regarding the cryptographic protection of data in applications?
    A. Using cryptography also requires the careful and appropriate key management, including key creation, key storage, and key handling.
    B. Cryptography requires the proper licensing for the algorithms used.
    C. Using cryptography for data protection requires potentially expensive hardware security modules (HSM) to store the keys securely.
    D. Smart cards are required to store encryption keys securely.

147. What are the reasons that testing applications with live data or testing in a production environment is not advocated?
    A. If the application processes confidential or sensitive data, the testing process may result in need-to-know or privacy violations.
    B. The testing process might not provide realistic results because the live data cannot be sanitized.
    C. Based on the concept of need-to-know, the developers are not authorized to view live data.
    D. Testing with live data violates privacy regulation compliance.

148. What is the purpose of the Capability Maturity Model Integration for Development (CMMI-DEV)?
    A. CMMI-DEV measures the maturity and capability levels of the organization's development processes.
    B. CMMI-DEV measures the maturity and capability levels of system integration in the organization.
    C. CMMI-DEV help organizations improve their development and maintenance processes for both products and services.
    D. CMMI-DEV is a process improvement maturity model for the development of products and services.

149. What is the PRIMARY security issue with application backdoors?
    A. They are a form of malicious software that can allow an attacker to gain unauthorized access to the application.
    B. Backdoors are implanted in code by malicious developers to allow them to circumvent the application's access controls.
    C. Backdoors are legitimate development tools that should be removed from the application before release to production to avoid their abuse by unauthorized users or attackers.
    D. Backdoors can lead to denial of service (DoS) conditions if an attacker performs an attack against the backdoor vulnerability.

150. The primary key is used to uniquely identify records in a database. By adding additional variables to the primary key, two items with the same identifier can be differentiated. This is often used to prevent inference attacks. Which of the following is best described by this scenario?
    A. Polymorphism
    B. Polyalphabetic
    C. Polyvariabolic
    D. Polyinstantiation

151. A database that uses pre-defined groupings of data that can only be accessed based upon a user's authorization level uses which of the following access control models or concepts?
    A. Role-based access control (RBAC)
    B. Database view control
    C. Mandatory access control (MAC)
    D. Nondiscretionary access control (NDAC)

152. Which of the following database attacks describes an attack where the perpetrator uses information gained through authorized activity to reach conclusions relating to unauthorized data?
    A. Unauthorized access attack
    B. Bypass attack
    C. Structured Query Language (SQL) attack
    D. Inference attack

153. One of the most significant differences between the software development lifecycle (SDLC) and the system lifecycle (SLC) is that the SDLC does not include which of the following phases?
    A. Post-development operation and maintenance
    B. Startup/requirements
    C. Development/construction
    D. Operational testing

154. How can polyinstantiation be used to protect a sensitive database?
    A. It confirms that all sensitive data within the system conforms to integrity checking.
    B. It prevents low-level users from inferring the existence of higher level data.
    C. It ensures that all security mechanisms within the database management system are working together to enforce the security policy.
    D. It ensures that two processes trying to access the same element will randomize the access to ensure integrity.

155. Why does compiled code pose more of a security risk than interpreted code?
    A. Because compilers are not as trusted as interpreters
    B. Because malicious code embedded into compiled code is hard to detect
    C. Because browsers can execute interpreted code as part of their functionality
    D. Because most web applications cannot process compiled code using legacy programming languages

156. Which framework allows organizations to evaluate their software process based on quality of its associated development and maintenance process using a 5-level scale?
    A. The IDEAL model
    B. The Total Quality Model (TQM)
    C. The Software Capability Maturity Model (SW-CMM)
    D. The Agile model

157. The security of an application is most effective and economical in which of the following?
    A. The application is optimized prior to adding security.
    B. The system is purchased from an official certified vendor.
    C. The system is customized to meet the specific security threats known.
    D. The application is designed originally to provide the necessary security based on requirements.

158. Building security into the application begins at
    A. The development phase
    B. The project initiation phase
    C. The management buy-in phase
    D. The functional design phase

159. Which of the following is MOST likely to cause long-term damage?
    A. Black box, white hat tester
    B. Black box, black hat tester
    C. White box, white hat tester
    D. White box, black hat tester

160. Why is inference from a database an important security problem to address?
    A. Statistics may be deduced from having access to records.
    B. Granular access rules may be difficult to implement in database environments.
    C. Private information may be deduced from aggregate data.
    D. Multiple database queries using analysis tools cannot be prevented.

161. What is the name of a malicious program that has the ability to infect both program files and boot sectors?
    A. Multipartite
    B. Polymorphic
    C. Stealth
    D. Companion

162. Which of the following best characterizes a buffer overflow attack?
    A. Multiple processes use the same buffer.
    B. Data stored in a buffer is corrupted by the malicious program.
    C. A program fails to check the buffer size limits properly.
    D. A program is maliciously forced to create multiple buffers.