CISSP®

Certified Information
Systems Security Professional

CISSP Training Course Assessment

(CISSP Exam Outline 2015 Rev1)

1. Which of these terms is **MOST** closely related to confidentiality?

A. Reliability
B. Need-to-know
C. Auditability
D. Trustworthiness

2. Building security into the application begins at _____

A. development.
B. project initiation.
C. functional design.
D. management buy-in.

3. Which of these is the **MOST** important factor when considering the alignment between releasing a product and making it secure?

A. Service level agreements
B. Customer satisfaction
C. Policy
D. Profit

4. Which statement is **MOST** accurate in the majority of organizational structures?

A. The Security Officer is responsible for ensuring that recommendations to executive management are full, accurate, and complete
B. The Security Officer accepts the risk of system failures
C. The Security Officer reports to the Privacy Officer
D. The Security Officer is responsible for protection of business information assets

5. Governance involves _____

A. the regulations that affect a company within a state or country.
B. the risk management processes and procedures within a company.
C. the organization structure that includes standards, procedures, and policies.
D. the organizational chart that describes who reports to whom as defined for a company.

6. Which of these Intellectual Property Law concepts is **NOT** a part of Contract Law?

A. Commercial software
B. Shareware
C. Public domain
D. Freeware

7. In order to determine whether encrypted messages can be sent between any two particular countries, which resource should be consulted?

A. World Intellectual Property Office (WIPO)
B. International Traffic in Arms Reductions (ITAR) Agreements
C. Organization for Economic Cooperation and Development (OECD)
D. Wassenaar Arrangement

8. Which of these is one of the Organization for Economic Cooperation and Development (OECD) guidelines on privacy?

A. Personal data should be relevant to the purpose for which they are to be used
B. Personal data might need to be protected by reasonable security safeguards as necessary
C. The use of personal data does not need to be disclosed at any time
D. There are no limits on the amount of personal data or the type of personal data that is collected

9. Which statement best describes the differences in the access control vulnerabilities known as skimming and spoofing?

A. Skimming occurs when an actor is able to capture the magnetic stripe on a card (e.g., credit card or employee badge)
B. Spoofing is using someone else's identity to get into a computer system, which skimming means that you use a radio signal detector to pick up someone's identity for later use
C. Spoofing is easiest to do with MAC addresses on computer systems; skimming is getting a fake IP address from an unattended computer
D. Both these hacks are tricks to get the MAC address of someone's computer

10. Which of the following definitions is correct?

A. RTO (Recovery Time Objective) is the amount of time it will take to recover all critical systems at an alternate site
B. RPO (Recovery Point Objective) is a measure of tolerable data loss
C. End of disaster is when all systems are recovered at the alternate site
D. End of disaster declaration occurs when the Security Manager determines that the activation was a false alarm

11. What is essential to get from an employee or contractor when they leave an organization?

A. A Non-disclosure agreement
B. Their passwords
C. His or Her badge
D. Any clothing items with the company logo

12. In risk analysis calculations, which of these statements is correct?

A. When exposure factor (EF) is unknown, it should be assumed to be zero
B. Annual Rate of Occurrence (ARO) increases whenever Single Loss Expectancy (SLE) is greater than zero
C. ALE (Annual Loss Expectancy) equals Asset Value (AV) times EF times ARO
D. ALE equals Asset Value (AV) times (EF) times SLE

Scenario (Questions 13-14)

Senior management decides to buy a new secure application development platform and passes a mandate that all new development must take place using this platform They spent a significant amount of money on acquisition and training Post implementation, the developers reported that most systems do not have enough hard disk space to install the application or save output files, nor do most of them have enough RAM to run the application at an acceptable pace

13. To prevent these problems from happening again the company needs _____

A. appropriate change and configuration management policies.
B. an incident response policy.
C. a baseline analysis of all existing hardware deployed in the development department.
D. a procedure for application acquisition that includes testing on machines that conform to company standards.

14. To correct the current problem, senior management needs _____

A. a policy that states the minimum hardware configuration for new purchases.
B. to allocate budget for necessary hardware upgrades.
C. a baseline analysis of all existing software.
D. a new set of software acquisition guidelines.

15. Which of these 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

16. Which of these is **NOT** an example of social engineering?

A. Session hijacking
B. Shoulder surfing
C. Tailgating
D. Baiting

17. Which of these statements is **MOST** likely to trigger a policy change?

A. Lack of compliance by staff
B. Large number of approved exceptions
C. Policy is short
D. Policy contains metrics

18. The purpose of an information classification system is to _____

A. comply with governmental regulations.
B. give data the appropriate level of protection.
C. enforce the need to know concept.
D. ensure that only those people with proper clearances can gain access to data.

19. Which of the following is the **MOST** accurate statement with respect to categorization?

A. A system with a higher categorization than it needs is an acceptable error
B. A system with a lower categorization than it needs is an acceptable error
C. Categorization is part of a company's overall risk management strategy
D. Categorization is simply another word for classification

20. Which of the following is most often missing from classification policies, standards, and procedures?

A. Penalties for unauthorized disclosure
B. Methods for keeping the data secure
C. Ways to determine which level (eg, secret, confidential) to apply to a data item
D. Declassification of standards and procedures

Scenario (Questions 21-23)

A sales database table contains the following items:

Buyer's name	Buyer's address	Buyer's phone number	Buyer credit card number
Item purchased	Date of purchase	Item quantity	Item Price
…..	……	……	……

Please answer the following questions related to that database:

21. What is the **BEST** way to make sure that data items are only available to those with authorized need to know?

A. Rule Based Access Control
B. Role Based Access Control
C. Mandatory Access Control
D. Content Based Access Control

22. PCI-DSS contracts provide for large penalty payments when stored credit card data is abused. However, the card information must be saved in order to process refunds What is the **BEST** way to solve this problem?

A. Encrypt the database using the data owner's private key
B. Encrypt the credit card numbers using a shared symmetric key
C. Tokenize the credit card numbers and limit access to the translation routines
D. Ask the customers to supply the credit card information they used when requesting a refund, but do not save the numbers

23. A medical database contains records of device sales, such as canes, walkers, braces, etand many sales are done via in-home visits. Recognizing that these items are covered under HIPAA, PIPEDA, and other international equivelants, what should be done to protect the company?

A. All data must be encrypted
B. Encryption is not required and due to the overhead of key management, is not warranted
C. Encryption of Patient Identification Information (PII) alone is required, and each sales person must have a unique key
D. Whole disk encryption is not required, but is the easiest and safest solution

24. What is the difference between the information owner and the data custodian?

A. There is no difference, the terms are used interchangeably
B. The information owner classifies the data, the data custodian creates, uses, and eventually destroys it
C. The data custodian classifies the data, the information owner creates, uses, and eventually destroys it
D. The data owner creates, classifies, uses, and eventually destroys the data The data custodian stores it, backs it up, restores it on demand, and otherwise protects its availability

25. Which of these is **NOT** part of Data Life Cycle Control?

A. Specification and modeling
B. Use and audit
C. Archiving and backup
D. Decommissioning and disposal

26. Data storage in the cloud is increasingly popular. What is the **BEST** way to deal with data remanence for the data?

A. Destroy the key
B. Create a strong Service Level Agreement (SLA)
C. Audit the cloud provider
D. Overwrite the data with nonsense bytes

27. What is the **BEST** way to delete data on a solid state drive?

A. Use the manufacturer's crypto-erase function
B. Use the manufacturer's built-in sanitization commands
C. Use multiple overwrite passes that contain enough data to fill the disk
D. Physically destroy the disk

28. If there is no law or regulation dictating the answer, how long should a company retain data?

A. Management may set any retention policy it wishes
B. Management should refer to the ISO standards on record retention and treat them as a maximum
C. Management should refer to the ISO standards on record retention and treat them as a minimum
D. Management should follow industry standard practices

29. The **MOST** important reason to adopt a cyber-security framework is _____

A. it is required by law.
B. it will identify the gap between current state and desired state.
C. it will assess progress as a company moves toward the desired state.
D. it will help lower the overall risk profile of the organization.

30. Loss of a thumb drive can disclose confidential data. Which of the following is the **BEST** way to protect against that loss?

A. File encryption software
B. Media encryption software
C. Self encrypting drives
D. In transit encrypting technologies

31. The EU courts support "the right to be forgotten". The court's jurisdiction applies unless which of these conditions are met?

A. The data is stored outside the EU, the person is an EU citizen or resident, but the data are available inside the EU
B. The data are stored outside the EU, the person is an EU citizen or resident, but the data are unavailable inside the EU
C. The data is stored outside the EU, the person is not an EU citizen or resident, and the data are unavailable inside the EU
D. The data is stored inside the EU, the person is not an EU citizen or resident, and the data are unavailable inside the EU

32. The capability models are all about maturing business processes The **MOST** significant step is the transition from reactive to proactive This happens on the migration from _____

A. Step 1 to Step 2.
B. Step 2 to Step 3.
C. Step 3 to Step 4.
D. Step 4 to Step 5.

33. Which of these is **NOT** a common method of achieving memory protection?

A. Segmentation
B. Paging
C. Reference monitor
D. Keying

34. Which of these is **NOT** an advantage of an Enterprise Security Architecture (ESA)?

A. It provides a monolithic solution
B. It presents a long-term, strategic view of the system
C. It unifies security controls
D. It leverages existing technology investments

35. Which of these is a confidentiality model?

A. Biba
B. Graham-Denning
C. Brewer-Nash
D. Clark-Wilson

36. In lattice models, the STAR property refers to _____

A. reading only.
B. writing only.
C. reading and writing.
D. invocation.

37. Which of these security models is the combination of two other models?

A. Lipner
B. Clark-Wilson
C. Brewer-Nash
D. Biba

38. The main evaluation model in use today is _____

A. The Rainbow Series.
B. TCSEC (Trusted Computer System Evaluation Criteria).
C. ITSEC (Information Technology System Evaluation Criteria).
D. Common Criteria.

39. PCI-DSS is mandated via _____

A. law.
B. regulation.
C. contract.
D. ISO Standard.

40. A CPU must be able to support two states, which are _____

A. privilege and problem.
B. supervisor and problem.
C. Ring 2 and Ring 1.
D. supervisor and error.

41. Which of the following methods of hiding data files is considered to be the most dangerous kind of malware?

A. Digital Rights Management
B. Steganography
C. Alternate Data Streams
D. Rootkits

42. Which of the following **BEST** describes the differences in a thin client solution vs a diskless workstation solution?

A. Storage is on external media such as a thumb drive when using a diskless workstation, but in the cloud when using a thin client
B. Storage is on a central computer when using a diskless workstation, but in the cloud when using a thin client
C. Thin clients do processing on the station itself, but diskless workstations do it on a central computer
D. Diskless workstations do processing on the station itself, but thin clients do it on a central computer

43. What is the **MOST IMPORTANT** benefit of storing passwords as hashed values?

A. Because hashed passwords re harder to decrypt than encrypted passwords
B. Because for a given word, generating a password hash is faster than encrypting it
C. Because if you able to find a word that hashed to a stored password hash value, you have only found one password; not all of them
D. Because encription is illiegal in some countries so storing as hashes enables logins to be possible internationally

44. Examining a patient's records and noticing bills for visits to a General Practitioner, a Gastroenterologist, and an Oncologist would suggest that the patient has stomach or colon cancer. This conclusion is an example of _____

A. metadata.
B. inference.
C. data warehousing.
D. polyinstantiation.

45. Which statement is **NOT** correct?

A. "Aggregation" is a conclusion based on substantial facts
B. "Data Mining" is discovering information by uncovering otherwise hidden relationships among data items
C. "Instantiation" is the creation of a new database by the DBA (Database Administrator)
D. "Metadata" is data about the data

46. Which statement about grid computing is **FALSE**?

A. Grid computers can have different operating systems
B. Idle resources on a desktop can be made part of a grid
C. Grid nodes can be geographically dispersed
D. Grid computers are also known as computing clusters

47. In cloud computing, the responsibility for effective controls and countermeasures _____

A. remains with the original data owner, but also becomes the responsibility of the cloud provider.
B. shifts to the cloud provider.
C. transfers entirely to the cloud provider.
D. are the same as they were before moving to the cloud.

48. A digital signature does **NOT** _____

A. provide non-repudiation of origin.
B. provide proof of integrity.
C. provide proof of delivery.
D. use asymmetric keys.

49. In a hybrid protocol such as SSL/TLS, the session key is encrypted with the _____

A. sender's private key.
B. sender's public key.
C. receiver's private key.
D. receiver's public key.

50. In SSL/TLS, the session key is _____

A. based on the previous session key.
B. a random number generated by the server.
C. a random number generated by the client.
D. exchanged via out-of-band communications.

51. Which of the entries on this list happens before the others when establishing a SSL/TLS session?

A. Validate that the certificate has not expired
B. Validate that the name on the certificate matches the domain name on the website
C. Check the CRL (Certificate Revocation List)
D. Exchange certificates

52. Given that a cryptanalyst has several samples of plaintext and ciphertext to work with, which of these techniques is most likely to reveal the key in the shortest amount of time?

A. Known plaintext
B. Chosen plaintext
C. Chosen ciphertext
D. Brute force

53. Which of these is a step in creating a digital signature?

A. Encrypt the message with receiver's public key
B. Encrypt the message with sender's public key
C. Encrypt the hash with receiver's public key
D. Encrypt the hash with sender's private key

54. Which of the following is a transposition cipher?

A. Caesar cipher
B. Vigenere square
C. Spartan scytale
D. Enigma machine

55. Often the acronym IAAA is used to describe the four phases of access control, in the order in which they are normally done. Which statement matches both the definitions and sequence of the IAAA terms?

A. Integrity, Authorization, Auditing, and Accounting
B. Identity, Authentication, Authorization, and Auditing
C. Integrity, Authorization, Authentication, and Auditing
D. Identity, Accounting, Authorization, and Auditing

56. Which of these deals with international copyright agreements?

A. ISO 27000
B. The Wassenaar Arrangement
C. The Montreal Protocol
D. WIPO

57. Closed-circuit camera feeds and recordings are commonly used as all of these **EXCEPT** for which of the following?

A. A deterrent control
B. A detective control
C. A corrective control
D. A preventive control

58. A compensating control is _____

A. a control put in place when another control is suspended or disabled.
B. a control put in place to overcome the shortcomings in another control.
C. a control put in place that automatically continues to protect the system when the primary control fails.
D. a control that compensates for law enforcement's or management's lack of technical skills.

59. Which of the following is **NOT** a component of CPTED (Crime Prevention Through Environmental Design)?

A. Access control
B. Guards
C. Surveillance
D. Territoriality

60. Which of these types of glass is **LEAST** able to withstand wide temperature variations?

A. Plate glass
B. Tempered glass
C. Acrylic glass
D. Polycarbonate glass

61. Which of these is most dangerous when a wiring closet catches fire?

A. Power outage
B. Internet data outage
C. Telephone outage
D. Noxious fumes

62. Which of the following is **NOT TRUE** of the database access language known as ODBC?

A. ODBC is only used by Microsoft desktops to access database systems
B. ODBC is the dominant means of standardized data access
C. Using ODBC, the data from a successful query is returned in cleartext form
D. With ODBC, calling applications must be checked to ensure they do not allow data aggregation

63. Routers chat among themselves in order to learn about networks not directly connected to them. This information is stored in routing tables and is used by the _____

A. Data Link layer.
B. Network layer.
C. Transport layer.
D. Session layer.

64. Which of the following is **NOT** an SDLC phase?

A. Functional Requirements Definition
B. Certification and Accreditation
C. Systems Replacement
D. Systems Design and Specification

65. The two **BEST** alternatives choices for key exchange available to a telecommuter using Transport Mode IPSEC are _____

A. Certificate-based or PSK (Pre-Shared Key).
B. Certificate-based or Diffie-Hellman Key Exchange (DH).
C. ISAKMP (IPsec Security Association Key Management Protocol) or DH (Diffie-Hellman Key Exchange).
D. PSK (Pre-Shared Key) or ISAKMP (IPsec Security Association Key Management Protocol).

66. In a TCP connection, which station sets the FIN bit to "on"?

A. The client
B. The server
C. Whichever station initiated the connection
D. Whichever station wants to terminate the connection

67. Attacking Supervisory Control And Data Acquisition (SCADA) systems via a virus or worm _____

A. is easy; because there's no built-in security.
B. is difficult; they use DNP3 which is not compatible with IPv4.
C. is of moderate difficulty; it requires human assistance - but social engineering is easy.
D. is impossible; SCADA systems are stand-alone devices not connected to the internet.

68. Which of these is **NOT** a feature of MPLS (Multi Protocol Label Switching)?

A. Traffic engineering
B. Better router performance
C. Built-in encryption
D. Built-in tunneling

69. Which of the following wireless solutions is **BEST** used for small group networking?

A. WiMax
B. Bluetooth
C. Cellular
D. Wireless Lan

70. What is the difference between an amplifier and a repeater?

A. None, they're one and the same
B. An amplifier boosts noise and signal, a repeater just boosts signal
C. An amplifier boosts noise and signal, a repeater makes a new original signal
D. An amplifier allows for longer cable runs without need for a repeater

71. Which of these is **NOT** part of the RFC 1918 private address pool?

A. 10.0.0.0 to 10.255.255.255
B. 169.254.0.0 to 169.254.255.255
C. 172.16.00 to 172.31.255.255
D. 192.168.0.0 to 192.168.255.255

72. A branch office and its headquarters both use addresses from the RFC 1918 pools. In order to set up an IPSEC link between them, they would need to use _____

A. Tunnel Mode IPSEC.
B. IPSec with NAT.
C. Transport Mode IPSEC.
D. Natural Mode IPSEC.

73. Wireless 80211 LANs primarily use _____

A. Polling.
B. CSMA/CD.
C. CSMA/CA.
D. Deterministic Token Passing Rings.

74. When comparing cable modems to DSL service for the home user, which of the following is the **GREATEST** benefit of cable modems?

A. Higher data rates than DSL
B. "Always on" encryption
C. Greater availability than DSL
D. Lower cost than DSL

75. SDN (Software Defined Networking) has three layers Which of these is **NOT** one of them?

A. Application
B. Control
C. Communications
D. Infrastructure

76. A PVLAN is a Private VLAN There are three types of nodes in PVLANs Which is **NOT** one of them?

A. Promiscuous: can talk to any node in the vlan
B. Isolated: can only talk to a promiscuous nodes
C. Community: can talk to others in the community and any promiscuous node
D. Controlled: can talk to others on an approved list and any promiscuous node

77. Enumeration is also known as _____

A. exploiting known weaknesses in an organization's system.
B. finding all of an organization's systems that are up and running.
C. determining the open ports on systems that are up and running.
D. running vulnerability scans on specific ports on organizational systems.

78. Which of these attacks is **LEAST** likely to be effective on modern network devices?

A. Syn flood
B. IP Address Spoofing
C. Ping of Death
D. Smurf Attack

79. Modern database systems have various integrity forms. Which statement **BEST** describes these forms?

A. A database system must understand the semantics of the data; else processing errors will happen
B. The entity integrity model forces each tuple to have a unique and non-null value primary key
C. The referential integrity model allows foreign keys to be null values
D. To achieve data integrity, database systems hash each table, twice, one for the entire table, and then the second time for each record

80. Which of the following is **MOST** likely to successfully prevent unauthorized access?

A. An access control policy
B. An incident response plan
C. A visitor log
D. An RFID-embedded badge

81. Which of these is done by an operating system?

A. Discretionary Access Control
B. Database Access Control
C. Content-Sensitive Access Control
D. Context-Sensitive Access Control

82. "Clearance" is a concept found only in _____

A. DAC (Discretionary Access Control).
B. N-DAC (Non-Discretionary Access Control).
C. MAC (Mandatory Access Control).
D. RBAC (Role-Based Access Control).

83. Who or what defines the classifications of corporate data?

A. The Security Administrator
B. The System Administrator
C. The Data/Information Owner
D. The Security Policy

84. Which of these following is the **BEST** way to prevent unauthorized access through an employee entrance?

A. Policy
B. Waist height turnstile
C. Training
D. Mantrap

85. A physical access control technique that requires two keys to be turned simultaneously to enter or activate a system is called _____

A. Dual control.
B. Double entry.
C. Mutual exclusion.
D. Two-factor.

86. In a discretionary access control environment, need-to-know is a part of _____

A. classification.
B. clearance.
C. categorization.
D. certification.

87. In database models, which of the following is true of the use of foreign and primary keys to search a database table?

A. A table is fastest to search using its primary key
B. A table can always be searched using its foreign key
C. Because foreign keys are so important, every table must have a foreign key
D. A table cannot be searched using its foreign key

88. Which statement **BEST** describes database models?

A. The transactional persistence model used a single indexed table
B. The network model was designed to be most efficient in an internet environment
C. The relational model was designed to use small tables related to one another to facilitate processing of large amounts of data
D. The network model came first, followed by the hierarchical model and then the relational model

89. Which statement about Kerberos is **TRUE**?

A. It only works with Windows clients and servers
B. It works with all or nearly all Intranet-based applications
C. It is a single point of failure in its default configuration
D. It requires 2-factor authentication methods

90. IDaaS (IDentity as a Service) is growing in popularity Its use is essential in which of the following?

A. Single sign-on authentication
B. Client-server authentication
C. Cloud authentication
D. Federated authentication

91. Copyright protects _____

A. a symbol that represents an idea.
B. a proprietary process or procedure.
C. the expression of an idea.
D. the idea itself.

92. Which of these keys will the sender never use?

A. Receiver's Public
B. Receiver's Private
C. Sender's Public
D. Sender's Private

93. The Identity and Access Management lifecycle has three steps Which of the following is **NOT** among them?

A. Provisioning: Applying appropriate rights to users for files/folders
B. Authentication: Examining rights before each access attempt
C. Review: Periodic monitoring of existing rights for continued need
D. Revocation: Removal of rights when no longer needed or warranted

94. Which of the following **BEST** describes software development methods?

A. First, there was the spiral method, then there was the Waterfall method
B. To develop secure software, non-iterative methods are favored over iterative methods
C. CASE methods provide running code quicker than RAD methods
D. Component methods are built to design all software from the ground up

95. Windows Event Manager automatically maintains several log files Which of the following is **NOT** among them?

A. System
B. Application
C. Host
D. Security

96. Common Operating System log file entries contain all of the following **EXCEPT**?

A. System startup and shutdown times
B. The number of hits the Web Server took in the last day
C. User password change attempts
D. Failed user login attempts

97. When considering a service provider's security controls, which is **LEAST** important to an auditor?

A. Confidentiality
B. Integrity
C. Availability
D. Privacy

98. An Incident Scene is _____

A. the location where the crime was committed.
B. the location where the evidence might be found.
C. the location described in the search warrant.
D. the location where the computer was used or stored.

99. Scientific Working Group for Digital Evidence (SWGDE) principles include all of the following **EXCEPT** _____

A. a named individual is responsible for any actions taken on the evidence while in his possession.
B. seized digital evidence cannot be changed without making it inadmissible.
C. all forensic and procedural best practices must be observed.
D. the person accessing the evidence must be trained for that purpose.

100. Which of the following **BEST** describes the differences in software certification and accreditation activities?

A. Accreditation occurs at the source code level, while certification occurs at the executable code level
B. Certification means you can commence a development project, accreditation means that you can dispose of the software project
C. Certification precedes accreditation
D. Accreditation means you have managements okay to go into production, certification means you have chosen the software development language

Scenario (Question 101-104)

You're the Incident Investigations manager. The head auditor approaches you in confidence saying that the total monies in the organization's bank accounts is significantly less than that shown in the books and records of the business. You launch an investigation, answer the following questions based upon these facts.

101. Your company has consolidated log files via a Security Information Event Management (SIEM) system. Which of these steps should be done first?

A. Ask HR to get updated permission from all financial service employees to inspect their personal bank accounts
B. Ask the system administrators to freeze all financial transactions
C. Arrange for a forensic image of the SIEM server log database
D. Contact management for permission to begin the investigation

102. The log files are, of course, quite large. You run an inquiry to extract records of users who have logged in outside of business hours and put them into a separate file for further examination. This is called _____

A. clipping.
B. filtering.
C. subset examinations.
D. the road to inadmissibility.

103. Your investigation has identified a clear suspect. To confirm your beliefs, you add additional logging to cover every action that person takes. In many countries, the evidence that is collected will be _____

A. admissible under the silver platter doctrine.
B. admissible because your company owns the machines on which the log files reside.
C. inadmissible because you had no search warrant.
D. inadmissible since it was not captured in the ordinary course of business.

104. Due to the fact that the amount of money embezzled was great, you decide to contact law enforcement, at which point they take over the case. One of the investigating officers asks you to do additional logging because they do not have the skill set to do it themselves. Why would this data be admissable?

A. This data is admissible under the plain view doctrine
B. This data is admissible under the silver platter doctrine
C. This data is admissible as a hearsay exception
D. This data is admissible only if law enforcement has a valid search warrant for the data

105. Deep-packet inspection is done by a _____

A. DLP system.
B. Stateful firewall.
C. NIPS system.
D. HIPS system.

106. In today's world there is many ways to hide files Which of these would be **LEAST** effective for data in transit?

A. Covert channels
B. Hidden HTML tags
C. Steganographically modified images
D. Cross Site Scripting

107. Configuration Management systems track changes to several categories of products. Which of these is **LEAST** likely to be subject to Configuration Management tracking?

A. Physical assets, including laptops, tablets, cell phones
B. Cloud Assets, including public and private clouds
C. Workplace Assets, including offices, desks, filing cabinets
D. Virtual assets, including SAN/NAS, SDN (Storage Area Networks/Network Attached Storage, Software Defined Networks)

108. Separation of duties should be implemented _____

A. in all areas.
B. in all areas that could be compromised by a disgruntled employee.
C. in all areas where the risk outweighs the cost.
D. in all areas where it is mandated by law or regulation.

109. The data owner is responsible is **NOT** responsible for _____

A. classification of the data.
B. determining need-to-know.
C. identifying data that has become obsolete.
D. understanding the replacement cost of the data.

110. Which of the following is the **LEAST** essential component of a Service Level Agreement?

A. Termination of the agreement procedures
B. Description of items subject to Non-Disclosure
C. Fines or penalties for non-compliance
D. Arbitration clause

111. The **BEST** definition of data remanence is _____

A. deleted data on disks that haves not yet been overwritten.
B. data remaining after erasure.
C. data on cloud provider's storage systems after deletion by the data owner.
D. data that haves been declared obsolete but have not yet been destroyed.

112. While there are several incident response frameworks, they tend to agree on three common components. Which of these is **NOT** one of those framework components?

A. Creation of a response capability
B. Activating the team
C. Incident handling and response
D. Recovery and feedback

113. What is the difference between an incident and an event?

A. No difference, they're the same
B. An event is something that can be measured, an incident is an event that can cause harm
C. An incident is something that can be measured, an event is an incident that can cause harm
D. An event will trigger an investigation, an incident will trigger litigation

114. Which of these statements details the **MAXIMUM** capabilities of a Network-Layer Firewall?

A. Network layer firewalls are stateless
B. Network layer firewalls can examine source and destination IP addresses
C. Network layer firewalls examine source and destination IP addresses and ports
D. Network layer firewalls can inspect protocols and detect/block inappropriate activity

115. It's been a busy week with several vendors releasing patches to several vulnerabilities. You need to prioritize your work. Which patch would you deploy **LAST**?

A. Vulnerability #1 can give escalated privileges to the attacker
B. Vulnerability #2 is easy to deploy; the attacker can script it
C. Vulnerability #3 requires physical access to the server to exploit, but gives the attacker full control
D. Vulnerability #4 is a data diddler – it can destroy the integrity of SQL databases

116. Which of these Business Continuity Planning statements is **TRUE**?

A. During recovery, least critical functions are addressed first
B. Recovery can be delayed until the arrival of the salvage and recovery team to complete its work
C. "Recovery" is what we do on the way out; "restoration" is what we do upon returning to the original (or a new, permanent) site
D. A vendor hot site is suitable for long-term outages

117. As an employee of an investment bank, you have just completed programming on a highly profitable automated stock trading program. You decide to copy it onto a writable CD and then use the program at home for your friends and family, but do not charge anyone any fees. Which of the follow statements apply?

A. The employer owns the copyright since it is a work for hire, but you may use it if you don't charge anyone for it, under fair use principles
B. The employer owns the copyright since it is a work for hire so you may not use it under any circumstances without permission
C. As author, you own the copyright and may use it any way you wish
D. You and your employer share the copyright and you may use it if you don't charge anyone for it

118. The badge reader at the employee entrance failed, so a guard was posted to examine IDs visually This is an example of a _____

A. corrective control.
B. physical control.
C. detective control .
D. compensating control.

119. The USA is moving to EMV (Europay, Mastercard and Visa) credit cards which have a chip What is the **MAIN** security advantage of these chip-based credit cards?

A. Losses are borne by the consumer, rather than the banks and merchants
B. They are less expensive to produce and replace
C. They have a certificate in them created by the issuing bank which cannot be forged, unlike the magnetic strip that has been in use for decades
D. They enable payment techniques such as ApplePay and Google Wallet

120. Which statement is **LEAST** accurate? Fire doors _____

A. should open out.
B. should close automatically.
C. should be solid, not hollow.
D. should be metal.

121. Which of these intrusion sensors is always active?

A. Microwave sensor
B. Acoustic sensor
C. Vibration sensor
D. Infrared sensor

122. A hardened hinge is _____

A. a steel hinge laminated with titanium.
B. a steel cap on the hinge to prevent hinge removal.
C. a dead bolt lock that has a key or lever on one side and is not visible on the other side of the door.
D. a dead bolt lock that has a key on both sides of the door.

123. What feature of a fireproof safe actually makes them fireproof?

A. They are made of metal, which does not burn
B. They are airtight, thus no oxygen equals no fire
C. There are fire suppression chemicals "painted" on the inside walls
D. They are so thick the heat cannot penetrate

124. Which of the following is part of the System Life Cycle (SLC) but **NOT** part of the Software Development Life Cycle (SDLC)?

A. Documentation
B. Transition to Production
C. Maintenance
D. BCP (Business Continuity Planning) Integration

125. Of the dozen or so things that functional design documents would normally include, which is **LEAST** likely to be required?

A. User acceptance criteria
B. Functions that require special privileges
C. Functions that require separation of duties or dual control
D. Restart and recovery procedures