Test Code 2009v1 Booklet Number 300103

CBK® Review Seminar

Educational Item

Sample Test

For the use of Official CBK Review Seminar Attendees Only

1. Which one of the following is the **MOST** effective method for reducing security vulnerabilities associated with building entrances?

   (A) Minimize the number of entrances
   (B) Use solid metal doors and frames
   (C) Brightly illuminate the entrances
   (D) Install tamperproof hinges and glass

2. Why is projection lighting mounted at the same height as the barbed wire topping of a fence?

   (A) It makes it easier to observe an intruder climbing over the fence.
   (B) It increases the field of view for those observing the scene.
   (C) It lowers the height and cost of observation towers.
   (D) It blinds the approaching intruder's view of the scene.

3. International Organization for Standardization (ISO) standard 27002 provides guidance for vendor compliance by outlining

   (A) guidelines and practices of security controls.
   (B) financial soundness and business viability metrics.
   (C) standard best practice for procurement policy.
   (D) contract agreement writing standards.

4. Which of the following is the **MAIN** advantage of having an application gateway?

   (A) To perform change control procedures for applications
   (B) To provide a means for applications to move into production
   (C) To log and control incoming and outgoing application traffic
   (D) To audit and approve changes to applications

5. Which of the following backup processing alternatives describes a computing facility with telecommunications equipment, some systems, but minimal data?

   (A) Company-owned hot site
   (B) Commercial hot site
   (C) Cold site
   (D) Warm site

6. Important documents that have been soaked in water during fire suppression efforts should be restored by

   (A) document recovery specialists.
   (B) Human Resources personnel.
   (C) document library personnel.
   (D) fire department specialists.

7. In a discretionary mode, who has delegation authority to grant access to information?

(A) User
(B) Security officer
(C) Group leader
(D) Owner

8. Which of the following is an industry specific standard that **PRIMARILY** deals with privacy matters?

(A) Control Objectives for Information and Related Technology (COBIT)
(B) European Union Principles
(C) International Organization for Standardization (ISO) 9001:2000
(D) The Wassenaar Agreement

9. What is the purpose of the Encapsulating Security Payload (ESP) in the Internet Protocol (IP) Security Architecture for Internet Protocol Security (IPSec)?

(A) To provide non-repudiation and confidentiality for IP transmissions
(B) To provide integrity and confidentiality for IP transmissions
(C) To provide integrity and authentication for IP transmissions
(D) To provide key management and key distribution for IP transmissions

10. The best practice to prevent logging clutter in application security is to

(A) log an exception when the exception is wrapped with another exception and propagate.
(B) catch and log exceptions at every level in the software.
(C) catch and log exceptions only at points at which exceptions are actually handled.
(D) disable debug level logging in a production environment.

11. What physical characteristics does a retinal scan biometric device measure?

(A) The amount of light reaching the retina
(B) The amount of light reflected by the retina
(C) The size, curvature, and shape of the retina
(D) The pattern of blood vessels on the retina

12. Which of the following defines the intent of a system security policy?

(A) A description of the settings that will provide the highest level of security
(B) A brief high-level statement defining what is and is not permitted in the operation of the system
(C) A definition of those items that must be denied on the system
(D) A listing of tools and applications that will be used to protect the system

13. To support legacy applications that rely on risky protocols (e.g., plain text passwords), which one of the following can be implemented to mitigate the risks on a corporate network?

(A) Implement strong, centrally-generated passwords to control use of the vulnerable applications
(B) Implement a Virtual Private Network (VPN) with controls on workstations joining the VPN
(C) Use physical access controls to ensure that only authorized, trained users have access to workstations
(D) Ensure audit logging is enabled on all hosts and applications with frequent log reviews

14. What is the recommended frequency that a system recovery plan be tested in a stable data processing environment?

(A) Once to validate the plan
(B) When applications are modified
(C) Prior to all audits
(D) Quarterly or semiannually

QUESTIONS 15–16 REFER TO THE FOLLOWING INFORMATION

ABZ Organization is constructing a new secure facility and has elected to install a two-tier access control system, which will consist of proximity badges and biometric devices. The system security professional is tasked with acquiring the access control systems. The only requirements are to keep cost as low as possible and minimize system down time.

15. While evaluating the effectiveness of several new devices, the security professional should expect that a biometric device becomes more sensitive when

(A) both the False Acceptance Rate (FAR) and False Rejection Rate (FRR) increase.
(B) the FAR increases while the FRR decreases.
(C) the FAR decreases while the FRR increases.
(D) both the FAR and FRR decrease.

16. The point where the False Acceptance Rate (FAR) and False Rejection Rate (FRR) is balanced is known as the

(A) Crossover Error Rate (CER).
(B) Crossover Acceptance Rate (CAR).
(C) Equal Crossover Rate (EQR).
(D) Equal Acceptance Rate (EAR).

17. When the results of process execution depend on the behavior of other processes on the system, the process may be vulnerable to

(A) shared memory corruption.
(B) a poorly designed locking strategy.
(C) poor data validation.
(D) a race condition.

18. What type of networking model can be deployed for small, inexpensive, and less secure networking?

(A) Wide Area Network (WAN)
(B) Metropolitan Area Network (MAN)
(C) Campus Area Network (CAN)
(D) Peer-to-Peer Network (P2P)

19. Which of the following is the **BEST** reason for using an automated risk analysis methodology?

(A) Automated methodologies generally require minimal training and knowledge of risk analysis.
(B) Most software tools have user interfaces that are easy to use and require little or no computer experience.
(C) Minimal information gathering is required due to the amount of information built into the software tool.
(D) Much of the data gathered during the review can be reused, greatly reducing the time required to perform a subsequent analysis.

20. Which of the following information system evaluation methods is process oriented rather than assurance oriented?

(A) International Organization for Standardization (ISO) 15408
(B) ISO 27002
(C) Systems Security Engineering Capability Maturity Model (SSE-CMM)
(D) Information Technology Security Evaluation Criteria (ITSEC)

21. Initial and ongoing authentication can be used as mitigation against which of the following network attacks?

(A) Spoofing
(B) Tampering
(C) Side channel
(D) Traffic analysis

22. What is one advantage of content-dependent access control of information?

(A) It prevents data locking.
(B) It limits the user's individual address space.
(C) It provides highly granular control.
(D) It confines access to authorized users of the system.

23. What is the **GREATEST** vulnerability of relying solely on proximity cards for access to a secure facility?

(A) A lost or stolen card may allow an unauthorized person to gain access.
(B) A proximity card is too easy to duplicate or forge.
(C) A proximity card does not record time of departure.
(D) An electrical power failure may deny access to all users.

24. What is one issue **NOT** addressed by the Bell-LaPadula model?

(A) Information flow control
(B) Security levels
(C) Need to Know
(D) Access modes

25. Which of the following is **TRUE** for an effective Incident Response Plan?

(A) Conduct a Business Impact Analysis (BIA) prior to developing the plan.
(B) The plan should be part of a Disaster Recovery Plan (DRP).
(C) Establish a leader who has a thorough understanding of the plan.
(D) The plan should be developed by an outside consulting agency.

26. An organizational information security strategy is incomplete without

(A) recommendations for salary improvement of security professionals.
(B) addressing privacy and health care requirements of employees.
(C) alignment with organizational audit and marketing plans.
(D) incorporating input from organizational privacy and safety professionals.

27. Which one of the following is an example of electronic piggybacking?

(A) Attaching to a communications line and injecting data
(B) Abruptly terminating a dial-up or direct-connect session
(C) Following an authorized user into the computer room
(D) Recording and playing back computer transactions

28. Computer generated evidence is **NOT** considered reliable because it is

(A) stored on volatile media.
(B) too complex for jurors to understand.
(C) seldom comprehensive enough to validate.
(D) too difficult to detect electronic tampering.

29. Which one of the following conditions is **NOT** necessary for a long dictionary attack to succeed?

(A) The attacker must have access to the target system.
(B) The attacker must have read access to the password file.
(C) The attacker must have write access to the password file.
(D) The attacker must know the password encryption mechanism and key variable.

30. Wired Equivalent Privacy (WEP) uses which of the following ciphers?

(A) Rivest-Shamir-Adleman (RSA)
(B) Triple Data Encryption Standard (3DES)
(C) Advanced Encryption Standard (AES)
(D) Rivest Cipher 4 (RC4)

31. Which one of the following is the **BEST** defense against worms?

(A) Differentiating systems along the lines exploited by the attack
(B) Placing limits on sharing, writing, and executing programs
(C) Keeping data objects small, simple, and obvious as to their intent
(D) Limiting connectivity by means of well-managed access controls

32. The **MAIN** goal of implementing change management processes in an organization is to

(A) ensure that the entire environment is safe and free of problems and errors.
(B) help prepare for documentation for the auditors.
(C) help provide the statistics of changes to upper management for cost-benefit analysis.
(D) provide feedback to the Information Technology (IT) support staff to improve their technical skills.

33. The organizational information security plan can

(A) assure protection of organizational data and information.
(B) select the technology solutions to enhance organizational security effectiveness.
(C) identify potential risks to organizational employee behavior.
(D) align organizational data protection schemes to business goals.

34. What type of subsystem is an application program that operates outside the operating system and carries out functions for a group of users, maintains some common data for all users in the group, and protects the data from improper access by users in the group?

(A) Prevented subsystem
(B) Protected subsystem
(C) File subsystem
(D) Directory subsystem

35. Which one of the following describes a reference monitor?

(A) Access control concept that refers to an abstract machine that mediates all accesses to objects by subjects
(B) Audit concept that refers to the monitoring and recording of all accesses to objects by subjects
(C) Identification concept that refers to the comparison of material supplied by a user with its reference profile
(D) Network control concept that distributes the authorization of subject accesses to objects

36. Which one of the following describes a covert timing channel?

(A) Modulated to carry an unintended information signal that can only be detected by special, sensitive receivers
(B) Used by a supervisor to monitor the productivity of a user without their knowledge
(C) Provides the timing trigger to activate a malicious program disguised as a legitimate function
(D) Allows one process to signal information to another by modulating its own use of system resources

37. Which one of the following does **NOT** describe an information integrity model?

(A) Clark-Wilson
(B) Bell-LaPadula
(C) Biba
(D) Sutherland

38. The purpose of the Internet Protocol Security (IPSec) Authentication Header (AH) is to provide

(A) Proof of delivery.
(B) Encryption of a payload.
(C) Validation of the sender.
(D) Validation of the recipient.

39. In which order are successful business continuity planning project process phases accomplished?

(A) Plan development, testing, Business Impact Analysis (BIA), risk analysis, and maintenance
(B) Requirement analysis, design, implementation, testing, and maintenance
(C) Plan design, requirement analysis, plan testing, implementation, and maintenance
(D) Requirement analysis, recovery strategy selection, user training, and maintenance

40. What technology interleaves data frames from multiple conversations into a single data stream for transmission?

(A) Time-Division Multiplexing (TDM)
(B) Real-time Transport Protocol (RTP)
(C) Synchronous Data Link Control (SDLC)
(D) Wired Equivalent Privacy 2 (WEP2)

41. An active content module that attempts to monopolize and exploit system resources is called a

(A) Macro virus.
(B) Hostile applet.
(C) Plug-in worm.
(D) Cookie.

42. One example of a security countermeasure against Structured Query Language (SQL) injection attacks is

(A) To deploy an Intrusion Detection System (IDS).
(B) To encrypt communications using Secure Sockets Layer (SSL).
(C) Anti-virus deployment.
(D) User input validation.

43. Patch management

(A) can only be performed by automated systems.
(B) is a vendor responsibility.
(C) requires accurate asset information.
(D) is only necessary for desktop computers.

44. Which one of the following is **NOT** a valid X.509 V.3 certificate field?

(A) Subject's public key information
(B) Subject's X.500 name
(C) Issuer's unique identifier
(D) Subject's digital signature

45. Which one of the following represents an addition to a message digest (MD) algorithm to increase its cryptographic strength?

(A) Internet Security Association and Key Management Protocol (ISAKMP)/Oakley
(B) Keyed-Hash Message Authentication Code (HMAC)
(C) Triple Data Encryption Standard (3DES)
(D) Message Digest 5 (MD5)

46. The three goals of integrity models are preventing unauthorized users from making modifications to data or programs, preventing authorized users from making improper or unauthorized modifications, and

(A) maintaining a current and complete audit record of all transactions.
(B) maintaining internal and external consistency of data and programs.
(C) assuring that all modifications are tracked to the responsible party.
(D) assuring data and programs are readily available to the intended user.

47. Why does fiber optic communication technology have a significant security advantage over other transmission technology?

(A) Higher data rates can be transmitted.
(B) Interception of data traffic is more difficult.
(C) Traffic analysis is prevented by multiplexing.
(D) Single and double-bit errors are correctable.

48. What determines the correct classification of data in a Mandatory Access Control (MAC) environment?

(A) The analysis of the users in conjunction with the audit department
(B) The assessment by the information security department
(C) The user's evaluation of a particular information element
(D) The requirements of the organization's published security policy

49. Log file review

(A) should be performed only after a Return on Investment (ROI) calculation.
(B) can help identify attack precursors.
(C) requires a high degree of technical skill.
(D) is only necessary for servers.

50. An effective countermeasure against Trojan horse malware is

(A) a key logger.
(B) a cryptologically strong password.
(C) a Host-based Intrusion Prevention System (HIPS).
(D) an Intrusion Detection System (IDS) in the network perimeter.

51. Why is the investigation of computer crime involving malicious damage especially challenging?

(A) Information stored in a computer is intangible evidence.
(B) Evidence may be destroyed in an attempt to restore the system.
(C) Isolating criminal activity in a detailed audit log is difficult.
(D) Reports resulting from common user error often obscure the actual violation.

52. In what way can web applets pose a security threat?

(A) Their transport can interrupt the secure distribution of World Wide Web pages over the Internet by removing Secure Sockets Layer (SSL) and Secure HyperText Transfer Protocol (S-HTTP).
(B) Client execution environment may not provide the ability to limit system access that an applet could have on a client system.
(C) Executables from the Internet may attempt an unintentional attack when they are downloaded on a client system because of bad programming.
(D) Client execution environment will check the bytecode at runtime or provide other safety mechanisms for program isolation from the client system.

53. Which one of the following is concerned with the frequency, length, and origin-destination patterns of the communications between systems?

(A) Masking analysis
(B) Protocol analysis
(C) Traffic analysis
(D) Pattern analysis

54. Which of the following is **NOT** a protection feature associated with Secure Sockets Layer (SSL)?

(A) Certificate-based authentication of web client
(B) Certificate-based authentication of web server
(C) Data confidentiality between client and web server
(D) Data confidentiality between two web servers

55. When disposing of classified data, file wipe programs exist that actually overwrite media that can be used on all media types **EXCEPT**

(A) flash drives.
(B) hard drives.
(C) tape drives.
(D) optical drives.

56. An Information Technology (IT) department has just been notified they will be audited in six weeks. How should they prepare?

(A) Reviewing the system documentation will be enough for a successful audit
(B) Notify staff the week before the audit will be performed
(C) No additional work is needed if a continuous compliance program is in place
(D) Implement a continuous compliance program right away

57. What is considered an industry standard for Internet Protocol Security (IPSec) remote access Virtual Private Networks (VPN) key exchange?

(A) Internet Key Exchange (IKE) Extended Authentication
(B) Internet Security Association and Key Management Protocol (ISAKMP)
(C) Transport Layer Security (TLS)
(D) Interior Gateway Routing Protocol (IGRP)

58. Why can surge suppressors that protect stand-alone computers and peripherals cause damage to computers and peripherals on a network?

(A) Stand-alone surge protectors are used only to filter electricity to the computers plugged into it.
(B) Only stand-alone surge suppressors signal a warning so that orderly shutdown can take place.
(C) Stand-alone surge suppressors divert the high surge voltage to the ground where it can enter the network communications lines.
(D) Stand-alone surge suppressors could overload the electrical circuits during a surge and result in a fire.

59. In the event of a disaster, in what order should services be recovered?

(A) Executive functions first
(B) Highest to lowest business impact
(C) Lowest to highest business impact
(D) Decreasing complexity of restoration

60. Verifying vendor compliance with their active security policies is typically provided through

(A) indemnification clauses.
(B) unqualified vendor management reports.
(C) good faith agreements.
(D) audit and standards compliance reporting.

61. What is the **MOST** critical factor to the success of enterprise security?

(A) Ability to effectively monitor the enterprise
(B) Budget available for security department
(C) Senior management support
(D) Complete security awareness plans

62. Which one of the following is used to provide authentication and confidentiality for e-mail messages?

(A) Digital signature
(B) Digital certificate
(C) Authentication Header (AH)
(D) Message digest (MD)

63. The **MAIN** reason for validating a vendor's Information Technology (IT) security policies and procedures is to verify the

(A) use of approved operating systems and specific computer hardware.
(B) vendor is not a liability to the company's technology operations.
(C) vendor is financially stable and viable.
(D) vendor has implemented a corporate strategy and vision statement.

64. Which one of the following is the **FIRST** step in auditing source code?

(A) Validate whether the implementation meets the design
(B) Matching as-built to as-designed
(C) Identify the internal Application Programming Interface (API) for getting input
(D) Analyze to determine whether there is a vulnerability

65. When establishing a process to track and analyze violations, which one of the following is often used to keep the quantity of data to manageable levels?

(A) Quantity baseline
(B) Maximum log size
(C) Circular logging
(D) Clipping levels

66. Patch management processes are

(A) standard for every organization.
(B) unique for every organization.
(C) effective only in large organizations.
(D) built around automated deployment systems.

67. Which one of the following individuals has **PRIMARY** responsibility for determining the classification level of information?

(A) Security manager
(B) User
(C) Owner
(D) Auditor

68. When basic standards for software development are implemented within an organization and are in common use (defined, established, and documented), the organization has reached what level of the Capability Maturity Model Integration (CMMI) for software engineering?

(A) Level 1
(B) Level 2
(C) Level 3
(D) Level 4

69. When a communication link is subject to monitoring, what advantage does end-to-end encryption have over link encryption?

(A) Cleartext is only available to the sending and receiving processes.
(B) Routing information is included in the message transmission protocol.
(C) Routing information is encrypted by the originator.
(D) Each message has a unique encryption key.

70. Computer security is the responsibility of

(A) everyone in the organization.
(B) corporate management.
(C) the corporate security staff.
(D) everyone with computer access.

71. What two factors should a backup program track to ensure the serviceability of backup tape media?

(A) The initial usage date of the media and the number of uses
(B) The physical characteristics and rotation cycle of the media
(C) The manufacturer and model number of the tape media
(D) The frequency of usage and magnetic composition

72. What is the **PRIMARY** objective for implementing a security awareness program?

(A) To reduce the cost associated with security tools
(B) To ensure users are aware of security policies and their responsibilities
(C) To reduce the risk of social engineering
(D) To obtain the support of users when investigating security breaches

73. Requests for adding or modifying functional requirements during software development can **BEST** be managed by using

(A) quality management processes.
(B) change management policies.
(C) management oversight standards.
(D) risk management plans.

74. When considering the Heating, Ventilation, and Air Conditioning (HVAC) requirements for a data processing center, why should an information security architect be concerned with the effect of humidity on data availability?

(A) Low humidity may cause condensation to occur, which could lead to data loss through a short circuit.
(B) High humidity may lead to high electrostatic buildup, which could lead to data loss through static discharge.
(C) High humidity may cause condensation to occur, which could lead to data loss through a short circuit.
(D) Low humidity may lead to high electrostatic buildup, which could lead to data loss through condensation.

75. Employee involuntary termination processing should include

(A) a list of all passwords used by the individual.
(B) a report on outstanding projects.
(C) the surrender of any company identification.
(D) the signing of a Non-Disclosure Agreement (NDA).

76. In e-mail security, both Secure Multipurpose Internet Mail Extensions (S/MIME) and Pretty Good Privacy (PGP) use Diffie-Hellman cipher. What is the purpose of using Diffie-Hellman?

(A) Key agreement or negotiation
(B) Digital signature
(C) Encrypting e-mail messages
(D) Creating a Message Authentication Code (MAC)

77. What is one disadvantage of content-dependent access control of information?

(A) It increases processing overhead.
(B) It requires additional password entry.
(C) It exposes the system to data locking.
(D) It limits the user's individual address space.

78. Why is it important that system owners categorize their information and systems in conjunction with their initial Certification and Accreditation (C&A) efforts?

(A) To determine what level of protection is required and what controls are needed to protect the system
(B) To determine the budget that is required to complete the initial certification assessment
(C) To develop a better project plan and method for allowing changes to be made to the system
(D) To determine whether their system is compatible with legacy systems in their inventory

79. The **MOST** dangerous consequence of a buffer overflow vulnerability is

(A) Denial of Service (DoS).
(B) arbitrary code execution.
(C) disclosure of confidential information.
(D) damage to the organizational brand.

80. Comparing the starting and ending locations of partitions on a disk, as reported by the partition table, is an example of

(A) a consistency check.
(B) an integrity check.
(C) a file system check.
(D) an atomic check.

81. An Internet worm that causes several computer systems to become unresponsive is seeking to reduce which of the following?

(A) Confidentiality
(B) Integrity
(C) Availability
(D) Denial of Service (DoS)

82. What is the company benefit, in terms of risk, for people taking a vacation of a specified minimum length?

(A) Reduces stress levels, thereby lowering insurance claims
(B) Improves morale, thereby decreasing errors
(C) Increases potential for discovering frauds
(D) Reduces dependence on critical individuals

83. Using a System Development Life Cycle (SDLC) methodology in a software development project should

(A) improve the quality of the software product.
(B) include an exact schedule for the project.
(C) increase the number of software vulnerabilities.
(D) decrease the complexity of the software code.

84. The International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) standard 27002 documents which body of knowledge?

(A) Information security management
(B) Personally identifiable health information data management
(C) Credit card handling processes
(D) Software development best practices

85. Many common vulnerabilities such as buffer overflows, Structured Query Language (SQL) injection, and command injections, can be traced to failure to

(A) install the latest vendor patches.
(B) maintain a hardened server configuration.
(C) validate user input.
(D) abide by organizational security policies.

86. What is the **PRIMARY** benefit of capturing all network traffic during an attack, as opposed to only capturing alerts?

(A) Attacks can be stopped before they occur.
(B) Attack captures can be easily compressed.
(C) Attacks using proxies can be easily traced.
(D) Attacks can be repeated later in test environments for analysis.

87. Which one of the following is the **MOST** crucial link in the computer security chain?

(A) Access controls
(B) People
(C) Management
(D) Awareness programs

88. During a routine investigation of violation reports, a technician discovers a memorandum written to a competitor containing sensitive information about the technician's company. Based on the $(ISC)^2$ Code of Ethics, what is the **FIRST** action the technician should take?

(A) Delete the memorandum to ensure no one else will see it
(B) Contact the author of the memorandum to let them know of the discovery
(C) Immediately inform the company's management of the technician's findings and the potential risk
(D) Launch a training program outlining the need for protection of intellectual property

89. When dealing with intellectual property rights for software between nations, it is important to consider

(A) information concerning the overall foreign trade agreements between the two nations.
(B) the governing law in the agreements between the two nations.
(C) foreign corrupt trading practices in the agreement between the two nations.
(D) information about the specific product liabilities that the software has.

90. What is the **MAIN** purpose of periodically testing the Incident Response Plan?

(A) To identify flaws in the plan and make it effective over time by updating it
(B) To satisfy auditors as the test reports generated are required for compliance
(C) To help the system administrators to identify any weaknesses present in their applications in advance
(D) To help prevent the occurrence of security incidents in the future

91. A critical step in the Business Impact Analysis (BIA) is to

(A) document application vulnerabilities.
(B) create a vendor contact list.
(C) identify acceptable recovery times.
(D) determine if a warm or hot site will be used.

92. Which of the following is the **MOST** important information to consider when writing a security policy?

(A) The impact on the organization's ability to achieve its goals.
(B) The acceptance by members of the IT department.
(C) The effect it could have on organizational morale.
(D) The degree to which it may affect the Business Continuity Plan (BCP).

93. Which of the following is the **LEAST** important information to record when logging a security violation?

(A) User's name
(B) UserID
(C) Type of violation
(D) Date and time of the violation

94. During the **INITIAL** stages of software development, a development team should analyze the vulnerabilities that could be encountered by the application produced. The method of analysis is termed

(A) audit analysis.
(B) threat modeling.
(C) cost benefit analysis.
(D) Software Development Life Cycle (SDLC).

95. How can a user of digital signatures ensure non-repudiation of delivery of the correct message?

(A) Sender encrypts the message with the recipient's public key and signs it with their own private key.
(B) Sender computes a digest of the message and sends it to a trusted third party who signs it and stores it for later reference.
(C) Sender signs the message and sends it to the recipient and requests "return receipt" of the e-mail.
(D) Sender gets a digitally signed acknowledgement from the recipient containing a copy or digest of the message.

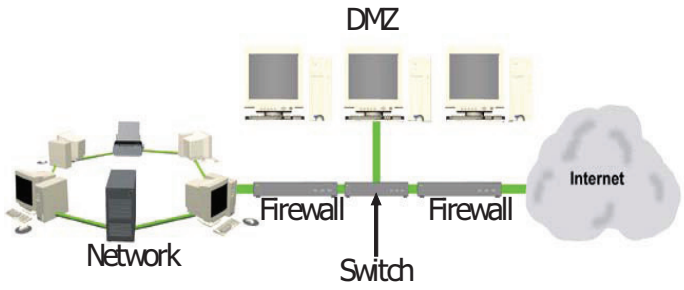
96. Cryptoperiod refers to the

(A) length of time a particular cryptographic key may be used.
(B) length of time that keys can be generated before the series begins to repeat.
(C) number of encrypted messages before the ciphertext repeats.
(D) number of decrypted messages before the plaintext repeats.

97. As the Chief Information Security Officer (CISO) for an organization, which of the following is of **LEAST** concern during an incident response?

(A) The affected system Recovery Time Objective (RTO) because that is a Business Impact Analysis issue and is irrelevant during an incident response.
(B) The affected system Recovery Point Objective (RPO) because that only deals with how long a system can go between backups.
(C) Alerting Law Enforcement because they may take over the investigation and reduce workload on the organization.
(D) Monitoring the situation to assess the effectiveness of the press briefing at controlling news reports that may disclose sensitive information.

98. Referring to the following diagram, which of the following statements is most correct:



(A) Place the enterprise mail server in the DMZ area because a mail relay would not provide adequate mail service.
(B) Place a router between the Internet and the first firewall to provide appropriate warning that the firewall is under attack.
(C) VPN connections from a VPN concentrator should terminate at the firewall closest to the network to minimize traffic in the DMZ area.
(D) A protocol based network Intrusion Detection System (IDS) could be placed in the DMZ area.

99. In order to reduce the costs and complexity of providing fault tolerant processor services, a certain number of the most recent transactions are allowed to be lost during the recovery. The magnitude of this loss is specified in the

(A) Recovery Point Objective (RPO).
(B) Recovery Time Objective (RTO).
(C) Return to Access Objective
(D) Annualized Loss Expectancy (ALE).

100. Feeding fake information into a phishing site with the intent to make the phisher's haul less valuable is referred to as

(A) reverse phishing.
(B) Denial of Service (DoS).
(C) takedown.
(D) dilution.

101. Which of the following is **MOST** true about Management's overarching security policy.

(A) It details the organization's security plan.
(B) It directly reflects management's commitment to security.
(C) It should be published so it can be read.
(D) Copies should be controlled for easy of updating, accountability purposes, auditing, and to demonstrate management's commitment to security

102. All of the following are basic components of a security policy **EXCEPT** the

(A) Definition of the issue being addressed and relevant terms.
(B) Statement of roles and responsibilities.
(C) Statement of applicability and compliance requirements.
(D) Statement of performance characteristics and requirements.

103. Which of the following provides for an effective security program?

(A) An hierarchical definition of security policies, standards, and procedures
(B) The identification, assessment, and mitigation of vulnerabilities
(C) A definition of program modules and procedures for data structures
(D) The identification of organizational, procedural, and administrative weaknesses

.

104. Which one of the following risk analysis terms characterizes the absence or weakness of a risk-reducing safeguard?

(A) Threat
(B) Probability
(C) Vulnerability
(D) Loss expectancy

105. When conducting a risk assessment, which one of the following is **NOT** an acceptable social engineering practice?

(A) Shoulder surfing
(B) Misrepresentation
(C) Asking the CEO to email his private key to the assessor.
(D) Dumpster diving

106. Removing unnecessary processes, segregating inter-process communications, and reducing executing privileges to increase system security is commonly called

(A) Hardening.
(B) Segmenting.
(C) Aggregating.
(D) Kerneling.

107. What type of key distribution system allows two parties to establish a secure session without exchanging any secret key?

(A) Key exchange, but it is processor intensive.
(B) Symmetric Key Cryptography because of its speed.
(C) Session key, but only if it uses an asymmetric key.
(D) Key negotiation using Diffie-Hellman

108. The network topology that provides the **MOST** security and the least risk is:

(A) Symmetric networks because the increased amount of redundancy reduces the possibility of an integrity error occurring without being caught.
(B) Symmetric Key Cryptography because of its speed.
(C) Bus because all users are on the same LAN segment.
(D) Ring if it is dedicated with no external connections

109. Which of the following is **LEAST** important when selecting a security control?

(A) Cost of the control compared to the level of security it provides.
(B) Evaluated Assurance Level (EAL) under Common Criteria.
(C) Value of the asset being protected.
(D) The Protection Profile if it does not reflect the environment for which the organization will employ the control.

110. Which of the following could **BEST** be utilized to validate the continued need for access to system resources?

(A) Periodically review and recertify privileged users
(B) Periodically review audit and access logs
(C) Periodically review processes that grant access
(D) Periodically review data classifications by management

111. Non-binding statements on how to achieve compliance with protective standards are called:

(A) Policies if signed by the Chief Information Officer (CIO).
(B) Standards, but only if issued by an International Organization.
(C) Guidelines if they provide "Best Practices."
(D) Procedures if they are properly written.

112. You are the Chief Information Security Officer for the United Nations. Understanding the International challenges will be difficult. However, which of the following will have the **LEAST** impact on your decision-making during risk analysis?

(A) Cost/benefit analysis
(B) Deploying safeguards
(C) Auditing
(D) Selecting products from different International vendors.

113. Which risk management methodology uses the exposure factor multiplied by the asset value to determine its outcome?

(A) Annualized Loss Expectancy
(B) Single Loss Expectancy
(C) Annualized Rate of Occurrence
(D) Information Security Risk Management

114. What is a **PRIMARY** reason for designing the security kernel to be as small as possible?

(A) The operating system cannot be easily penetrated by users.
(B) Changes to the kernel are not required as frequently.
(C) Due to its compactness, the kernel is easier to formally verify.
(D) System performance and execution are enhanced as the kernel is faster

115. What should be the size of a Trusted Computer Base?

(A) Small - in order to permit it to be implemented in all critical system components without using excessive resources
(B) Small - in order to facilitate the detailed analysis necessary to prove that it meets design requirements
(C) Large - in order to accommodate the implementation of future updates without incurring the time and expense of recertification
(D) Large - in order to enable it to protect the potentially large number of resources in a typical commercial system environment

116. Which one of the following refers to a series of characters used to verify a user's identity?

(A) Token serial number
(B) UserID
(C) Password
(D) Security ticket

117. Which of the following MUST be true before the least privilege principle applies?

(A) The individual must have a need to know.
(B) The object's label must be updated with the subject's clearance level.
(C) The object's label must grant the subject access to the object.
(D) The individual must be assigned to a leadership position in the organization.

118. A large number of approved waivers to an organization's policy may indicate:

(A) that the policy is too general.
(B) that that the policy is being enforced.
(C) that the policy is inappropriate for the organization or situation.
(D) that the waiver process is not properly processing the waivers.

119. IPSEC (IP Security), S-HTTP (Secure HTTP) and SSL (Secure Socket Layer) are examples of ?

(A) Secure Multi-purpose Internet Mail Extensions (S/MIME).
(B) Secure Internet protocols.
(C) Internet transaction protocols.
(D) Application protocol interfaces.

120. Which one of the following can be used to increase the authentication strength of an access control system?

(A) Multi-party
(B) Two factor
(C) Mandatory
(D) Discretionary

121. What is the **BEST** method of storing user passwords for a system?

(A) Password-protected file
(B) File restricted to one individual
(C) One-way encrypted hash
(D) Two-way encrypted cipher

122. CISSPs may be faced with an ethical conflict between their company's policies and the $(ISC)^2$ Code of Ethics. According to the $(ISC)^2$ Code of Ethics, in which order of priority should ethical conflicts be resolved?

(A) Duty to principals, profession, public safety, and individuals
(B) Duty to public safety, principals, individuals, and profession
(C) Duty to profession, public safety, individuals, and principals
(D) Duty to public safety, profession, individuals, and principals

123. Key elements of an information security program include

(A) Disaster recovery and business continuity planning, definition of access control requirements, and human resources policies.
(B) Business impact, threat and vulnerability analysis, delivery of an information security awareness program, and physical security of key installations.
(C) Security policy implementation, assignment of roles and responsibilities, and information asset classification.
(D) Senior management organizational structure, message distribution standards, and procedures for the operation of security management systems.

124. Which of the following statements is true about traffic passing from the DMZ interface to the inside interface?

(A) Traffic is allowed access by default.
(B) Traffic is blocked by default
(C) Traffic passes if the access control lists are established between the inside and the DMZ.
(D) Traffic passes if the inside security level is higher than the DMZ's interface's level.

125. Which one of the following evidence collection methods is **MOST** likely to be acceptable in a court case?

(A) Providing a full system backup inventory
(B) Creating a file-level archive of all files
(C) Providing a bit-level image of the hard drive
(D) Copying all files accessed at the time of the incident