CISSP CBK Review Baseline Exam

1. A corporation is considering a best authentication method for access control, which of the following method has the best authentication strength? (Access Control Domain)

    A. Multi-party

    B. Two factor

    C. Mandatory

    D. Discretionary

2. A security engineer is evaluating methods to store user passwords in an information system. What may be the best method for storing user passwords and meeting the confidentiality security objective? (Cryptography Domain)

    A. Password-protected file

    B. File restricted to one individual

    C. One-way encrypted file

    D. Two-way encrypted file

3. What is the minimum and customary practice that constitutes "responsible protection of information assets that affects a community or societal norm"? (Information Security & Risk Management Domain)

    A. Due diligence

    B. Risk mitigation

    C. Asset protection

    D. Due care

4. A timely review of system access records would be an example of what type of basic security function? (Operations Security Domain)

    A. Avoidance

    B. Deterrence

    C. Prevention

    D. Detection

5. What type of access control is implemented where a database administrator can grant "Update" privilege in a database to specific users or group? (Application Security Domain)

    A. Supplemental

    B. Discretionary

C. Mandatory

D. System

6. What is the purpose of biometrics in access control? (Access Control Domain)

A. Certification

B. Authorization

C. Authentication

D. Confirmation

7. A practicing CISSP may face an ethical conflict between his/her company's interests 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? (Legal, Regulations, Compliance, and Investigations Domain)

A. Duty to principles, profession, public safety, and individuals.

B. Duty to public safety, principles, individuals, and profession.

C. Duty to profession, public safety, individuals, and principles.

D. Duty to public safety, profession, individuals, and principles.

8. Company X is planning to implement rule based access control mechanism for controlling access to its information assets. What type of access control is this usually related to? (Access Control Domain)

A. Discretionary Access Control

B. Task-initiated Access Control

C. Subject-dependent Access Control

D. Token-oriented Access Control

9. What security implementation principle is used for granting users only the rights that are necessary for them to perform their work? (Information Security & Risk Management Domain)

A. Discretionary Access

B. Least Privilege

C. Mandatory Access

D. Separation of Duties

10. As an information systems security manager (ISSM), how would you explain the purpose a system security policy? (Information Security & Risk Management Domain)

    A. A definition of the particular settings that have been determined to provide optimum security

    B. A set of brief, high-level statements that defines what is and is not permitted during the operation of the system

    C. A definition of those items that must be excluded on the system

    D. A listing of tools and applications that will be used to protect the system

11. In addition to ensure changes to the computer system taking place in an identifiable and controlled manner; configuration management provides assurance that changes… (Application Security Domain)

    A. to application software cannot bypass system security features.

    B. do not adversely affect implementation of the security policy.

    C. to the operating system are always subjected to independent validation and verification.

    D. in technical documentation maintain an accurate description of the Trusted Computer Base.

12. In addition to performing cryptographic operation, what is another reason for using asymmetric key cryptography? (Cryptography Domain)

    A. It is used for key management.

    B. It is used for key storage.

    C. It is used for key generation.

    D. It is used for key recovery.

13. Under what circumstance might a Certification Authority (CA) revokes a certificate? (Cryptography Domain)

    A. The certificate owner has not utilized the certificate for an extended period.

    B. The certificate owner public key has been compromised.

    C. The certificate owner' private key has been compromised.

    D. The certificate owner has upgraded his/her web browser.

14. In the Rivest-Shamir-Adleman (RSA) algorithm, a modulus is derived by… (Cryptography Domain)

A. calculating the product of two large prime numbers.

B. calculating the square of large prime numbers and then adding the smaller prime number.

C. calculating the quotient of the larger prime number divided by the smaller prime number.

D. raising the larger prime number to the power of the smaller prime number.

15. What type of crypto-analytical attack where an adversary has least amount of information to work with? (Cryptography Domain)

A. Known plain text

B. Cipher text only

C. Plain text only

D. Chosen cipher text

16. Company X is building a data center, what may be the most effective method for reducing security risks associated with building entrances? (Physical and Environmental Security Domain)

A. Minimize the number of entrances

B. Use solid metal doors and frames

C. Brightly illuminate the entrances

D. Install tamperproof hinges and glass

17. When disposing magnetic storage media, all of the following methods ensure that data is unreadable except… (Security Architecture and Design Domain)

A. writing random data over the old file.

B. physical alteration of media.

C. degaussing the disk or tape.

D. removing the volume header information.

18. Prior to installation of an intrusion prevention system (IPS), a network engineer usually place packet sniffers on the network, what is the purpose for using a packet sniffer? (Telecommunications and Network Security Domain)

A. It tracks network connections.

B. It monitors network traffic.

C. It scans network segments for cabling faults.

D. It detects illegal packets on the network.

19. In mandatory access control, what determines the assignment of data classifications? (Information Security & Risk Management Domain)

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. A security classification policy / guideline

20. Granularity defines the level of detail to which… (Application Security Domain)

A. a trusted system can authenticate users.

B. imperfections of a trusted system can be measured.

C. an access control system can be adjusted.

D. packets can be filtered.

21. An advantage of asymmetric key cryptography is that… (Cryptography Domain)

A. it is relatively easy to distribute keys.

B. both keys are the same.

C. it can be easily implemented in hardware.

D. its execution is very fast.

22. What is the proper way to dispose confidential computer printouts? (Physical and Environmental Security Domain)

A. Have them collected and destroyed by janitorial staff

B. Place them with other printouts for collection by a document removal service

C. Store them securely until removed and destroyed by authorized personnel

D. Place them in a recycling bin for pickup and removal

23. Which of the following is a reasonable response from an intrusion detection system (IDS) when it detects Internet Protocol (IP) packets where the source address is the same as the destination address? (Telecommunications & Network Security Domain)

(A) Allow the packet to be processed by the network and record the event

(B) Record selected information about the item and delete the packet

(C) Resolve the destination address and process the packet

(D) Translate the source address arid resend the packet

24. As a security manager, how would you explain the primary goal of a security awareness program to senior management? (Information Security & Risk Management Domain)

(A) Provide a vehicle for communicating security procedures

(B) Provide a clear understanding of potential risk and exposure

(C) Provide a forum for disclosing exposure and risk analysis

(D) Provide a forum to communicate user responsibilities

25. Which of the following refers to a series of characters used to verify a user's identity? (Access Control Domain)

(A) Token serial number

(B) UserID

(C) Password

(D) Security ticket

26. Which of the following is not a valid X.509 V.3 certificate field? (Cryptography Domain)

(A) Subject's public key information

(B) Subject's X.500 name

(C) Issuer's unique identifier

(D) Subject's digital signature

27. Security should first become involved in what stage of application development life cycle? (Application Security Domain)

(A) Prior to the implementation.

(B) Prior to user acceptance testing.

(C) During unit testing.

(D) During requirements development.

28. Which of the following evidence collection method is most acceptable in a court case? (Legal, Regulations, Compliance, and Investigations Domain)

(A) A full system backup inventory.

(B) A file-level archive of all files.

(C) A mirrored image of the hard drive.

(D) A copy of files accessed at the time of the incident.

29. When engaging an external contractor for a software development project, source code escrow can be used to protect against… (Operations Security Domain)

(A) system data loss.

(B) vendor bankruptcy.

(C) copyright violation.

(D) legal liability.

30. All of the followings are goals for change control management process except ensuring the changes are… (Application Security Domain)

(A) authorized.

(B) effective.

(C) documented.

(D) correct.

31. What type of access control where the security clearance of a subject must match the security classification of an object? (Access Control Domain)

(A) Mandatory

(B) Discretionary

(C) Relational

(D) Administrative

32. Which of the following connection-oriented protocol is an OSI Transport Layer protocol? (Telecommunications & Network Security Domain)

(A) Transmission Control Protocol (TCP)

(B) Internet Control Message Protocol (ICMP)

(C) Used Defined Protocol (UDP)

(D) Layer 2 Transmission Protocol (L2TP)

33. Which of the following fire suppression system suppresses a Class C fire without harming the earth's ozone? (Physical and Environmental Security Domain)

(A) Water

(B) Soda acid

(C) FM-200

(D) Halon

34. When a communication link is subjected to monitoring, what is the advantage for using an end-to-end encryption solution over link encryption solution? (Telecommunications & Network Security Domain)

A. Cleartext is only available to the sending and receiving entities.

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.

35. What classic cipher uses simple substitution algorithm? (Cryptography Domain)

A. Rivest, Shamir, Adleman (RSA)

B. Data Encryption Standard (DES)

C. Caesar Cipher

D. Blowfish

36. An information security program should include the following elements: (Information Security & Risk Management Domain)

A. Disaster recovery and business continuity planning, and 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.

37. What are the objectives of emergency actions taken at the beginning stage of a disaster? Preventing injuries, loss of life, and … (Business Continuity & Disaster Recovery Planning)

A. determining damage.

B. protecting evidence.

C. relocating operations.

D. mitigating damage.

38. When handling electronic evidence, what is the implementation principle for chain of custody that documents the evidence life cycle? (Legal, Regulations, Compliance, and Investigations Domain)

A. Must be signed by the judge.

B. Must be signed by the originator.

C. Ensures that the evidence will be admissible.

D. Must account for everyone who had access to the evidence.

39. Security of an automated information system is most effective and economical if the system is… (Security Architecture & Design Domain)

A. optimized prior to addition of security.

B. customized to meet the specific security threat.

C. subjected to intense security testing.

D. designed originally to meet the information protection needs.

40. It is important that information about an ongoing computer crime investigation be… (Legal, Regulations, Compliance, and Investigations Domain)

A. destroyed as soon after trial as possible.

B. reviewed by upper management before being released.

C. replicated to a backup system to ensure availability.

D. limited to as few people as possible.

41. After signing out a laptop computer from the company loaner pool, you discovered there is a memorandum stored in the loaner laptop written to a competitor containing sensitive information about a new product your company is about to release. What is the ethical action you should take? (Legal, Regulations, Compliance, and Investigations Domain)

A. Delete the memorandum from the laptop to ensure no one else will see it.

B. Contact the author of the memorandum to let him/her know the memorandum was on the laptop.

C. Immediately inform your company's management of your findings and its potential ramifications.

D. Inform the security awareness trainers that data disclosure prevention in a mobile computing environment needs to be added to their classes.

42. What is the purpose of a firewall? (Telecommunications & Network Security Domain)

A. To protect networks from each other.

B. To prevent data traffic from going out of the network.

C. Block SNA traffic.

D. Monitor network traffic.

43. Which of the following is the least important information to record when logging a security violation? (Legal, Regulations, Compliance, and Investigations Domain)

A. User's name

B. User id.

C. Type of violation

D. Date and time of the violation

44. Which of the following device might be used to commit telecommunications fraud using the "shoulder surfing" technique? (Physical and Environmental Security Domain)

A. Magnetic stripe copier.

B. Tone generator.

C. Tone recorder.

D. Video recorder.

45. Spoofing can be defined as… (Application Security Domain)

A. eavesdropping on communications between persons or processes.

B. a person or process emulating another person or process.

C. a hostile or unexpected entity concealed within another entity.

D. the testing of all possibilities to obtain information.

46. Which of the following is a feature of a hot site? (Business Continuity & Disaster Recovery Planning Domain)

A. Relocation of equipment during critical times.

B. Basic facilities such as interface connections and communications.

C. Fully equipped with external interfaces and communications.

D. Partially equipped for resumption of operations in a short period of time.

47. Which of the following shall be used to achieve non-repudiation of delivery? (Telecommunications & Network Security Domain)

A. Sender encrypts the message with the recipients 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 (TTP) who signs it and stores it for later reference.

C. Sender sends the message to a TTP who signs it together with a time stamp and sends it on to the recipient.

D. Sender gets a digitally signed acknowledgment from the recipient containing a copy or digest of the message.

48. The deliberate planting of apparent flaws in a system for the purpose of detecting attempted penetrations or confusing an intruder about which flaws to exploit is called… (Legal, Regulations, Compliance, and Investigations Domain)

A. alteration.

B. re-direction.

C. cracking.

D. enticement.

49. What is the trusted registry that guarantees the authenticity of client and server public keys? (Cryptography Domain)

A. Public key notary.

B. Certification authority.

C. Key distribution center.

D. Key revocation certificate.

50. The concept that all accesses must be mediated, protected from unauthorized modification, and verifiable as correct is implemented through what? (Security Architecture & Design Domain)

A. A secure model.

B. A reference monitoring.

C. A security kernel.

D. A trusted computing base.

51. Programmed procedure that ensures valid transactions are processed accurately and only once in the current timescale, are referred to as… (Application Security Domain)

A. data installation controls.

B. application controls.

C. operation controls.

D. physical controls.

52. Eavesdropping is what type of attack? (Operations Security Domain)

A. Active

B. Passive

C. Aggressive

D. Masquerading

53. For what reason would a network administrator leverage the promiscuous mode on a network interface? (Telecommunications & Network Security Domain)

A. To screen out all network errors that affect network statistical information.

B. To monitor the network to gain a complete statistical picture of activity.

C. To monitor only unauthorized activity and use.

D. To capture only unauthorized internal/external use.

54. Which of the following is an example of hyperlink spoofing? (Applications Security Domain)

A. Compromising a web server Domain Name Service reference

B. Connecting the user to a different web server

C. Executing Hypertext Transport Protocol Secure GET commands

D. Starting the user's browser on a secured page

55. During a disaster, how does a closed-circuit television (CCTV) help management and security to minimize loss? (Physical and Environmental Security Domain)

A. It helps the management to direct resources to the hardest hit area.

B. It records instances of looting and other criminal activities.

C. It documents shortcomings of plans and procedures.

D. It captures the exposure of assets to physical risk.

56. What is the first step in establishing a disaster recovery plan (DRP)? (Business Continuity & Disaster Recovery Domain)

A. Demonstrate adherence to a standard disaster recovery process.

B. Agree on the goals and objectives of the plan.

C. Identify applications to be run during a disaster.

D. Determine the site to be used during a disaster.

57. The guiding principle of ethics is to do nothing… (Legal, Regulations, Compliance, and Investigations Domain)

A. illegal.

B. harmful.

C. untruthful.

D. untrusting.

58. Which of the following distinguishes misuse detection from intrusion detection? (Telecommunications & Network Security Domain)

A. The perpetrator has no valid accounts on any of the systems in the network.

B. It uses statistical measures to detect unusual behavior.

C. The perpetrator has at least one valid account on one of the systems in the network.

D. It uses a collection of known attacks to detect intrusion.

59. A goal of cryptanalysis is to… (Cryptography Domain)

A. forge coded signals that will be accepted as authentic.

B. ensure that the key has no repeating segments.

C. reduce the system overhead for cryptographic functions.

D. determine the number of encryption permutations required.

60. Which of the following is not identified by a business impact analysis (BIA)? (Business Continuity & Disaster Recovery Domain)

A. Analyzing the threats associated with each functional area

B. Determining risks associated with threats

C. Identifying major functional areas of information

D. Determining team members associated with disaster planning

61. The three primary methods for authenticating a user to a system or network are… (Access Control Domain)

A. passwords, tokens, and biometrics.

B. authorization, identification, and tokens.

C. passwords, encryption, and identification.

D. identification, encryption, and authorization.

62. Pretty Good Privacy (PGP) provides… (Cryptography Domain)

A. confidentiality, integrity, and authenticity.

B. integrity, availability, and authentication.

C. availability, authentication, and non-repudiation.

D. authorization, non-repudiation, and confidentiality.

63. Which of the following can be identified when exceptions occur using operations security detective controls? (Operations Security Domain)

A. Unauthorized people seeing printed confidential reports

B. Unauthorized people destroying confidential reports

C. Authorized operations people performing unauthorized functions

D. Authorized operations people not responding to important console messages

64. When downloading software from Internet, why do vendors publish MD5 hash values when they provide software to customers? (Cryptography Domain)

A. Recipients can verify the software's integrity after downloading.

B. Recipients can confirm the authenticity of the site from which they are downloading the patch.

C. Recipients can request future updates to the software by using the assigned hash value.

D. Recipients need the hash value to successfully activate the new software.

65. The three principal schemes that provide a framework for managing access control are… (Access Control Domain)

A. Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role Based Access Control (RBAC).

B. Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Layer Based Access Protocol (LBAP).

C. Mandatory Access Control (MAC), Layer Based Access Protocol (LBAP), and Target Based Access Protocol (TBAP).

D. Role Based Access Control (RBAC), Layer Based Access Protocol (LBAP), and Target Based Access Protocol (TBAP).

66. From a legal perspective, which of the following rules must be addressed when investigating a computer crime? (Legal, Regulations, Compliance, and Investigations Domain)

A. Search and seizure

B. Data protection

C. Engagement

D. Evidence

67. Before powering off a computer system, the computer crime investigator should record the contents of the monitor and… (Legal, Regulations, Compliance, and Investigations Domain)

A. save the contents of the spooler queue.

B. dump the memory contents to a disk.

C. backup the hard drive.

D. collect the owner's boot up disks.

68. The growth of Internet e-mail has contributed to the widespread propagation of which of the following? (Application Security Domain)

A. Macro Viruses

B. Boot Sector Viruses

C. Attack Applets

D. Malicious Cookies

69. Which of the following transaction processing properties ensures once a transaction completes successfully (commits), the updates survive even if there is a system failure? (Application Security Domain)

A. Atomicity.

B. Consistency.

C. Isolation.

D. Durability.

70. Which of the following is the best-known example of a symmetric key cipher system? (Cryptography Domain)

A. Data Encryption Standard (DES).

B. Rivest Shamir Adelman (RSA).

C. ElGamel (ElG).

D. Message Digest 5 (MD5).

71. Which of the following equates to annualized loss expectancy (ALE) ? (Information Security & Risk Management Domain)

A. Gross loss expectancy multiplied by loss frequency.

B. Asset value multiplied by loss expectancy.

C. Total cost of loss plus actual replacement value.

D. Single loss expectancy multiplied by annualized rate of occurrence.

72. Which of the following describes the step prior to an encrypted session using Data Encryption Standard (DES)? (Cryptography Domain)

A. Key clustering

B. Key compression

C. Key signing

D. Key exchange

73. The security planning process must define: how security will be managed, who will be responsible, and… (Business Continuity & Disaster Recovery Domain)

A. what practices are reasonable and prudent for the enterprise.

B. who will work in the security department.

C. what impact security will have on the intrinsic value of data.

D. how security measures will be tested for effectiveness.

74. A security policy provides a way to… (Information Security & Risk Management Domain)

A. establish a cost model for security activities.

B. allow management to define system recovery requirements.

C. identify and clarify security goals and objectives.

D. enable management to define system access rules.

75. Another name for a Virtual Private Network (VPN) is a… (Telecommunications & Network Security Domain)

A. tunnel.

B. firewall proxy.

C. named-pipe.

D. domain.

76. What security feature does a digital signature provide? (Cryptography Domain)

A. It provides the ability to encrypt an individual's confidential data.

B. It ensures an individual's privacy.

C. It identifies the source and verifies the integrity of data.

D. It provides a framework for law and procedures.

77. Monitoring of electromagnetic pulse emanations from personal computers (PCs) and cathode ray televisions (CRTs) provides a hacker with what significant advantage? (Physical and Environmental Security Domain)

A. Defeat the TEMPEST safeguards

B. Bypass the system security application

C. Gain system information without trespassing

D. Undetectable active monitoring

78. Computer security is generally considered to be the responsibility of… (Information Security & Risk Management Domain)

A. everyone in the organization.

B. corporate management.

C. the corporate security staff.

D. everyone with computer access.

79. A set of step-by-step instructions used to satisfy control requirements is called … (Information Security & Risk Management Domain)

A. policy.
B. standard.
C. guideline.
D. procedure.

80. The practice of embedding a message in a document, image, video or sound recording so that its very existence is hidden is called… (Cryptography Domain)

A. anonymity.
B. steganography.
C. shielding.
D. data diddling.

81. Which of the following can assist in preventing denial of service attacks? (Telecommunications & Network Security Domain)

A. Employ a strong password policy.
B. Configure the router to check all outgoing traffic.
C. Ensure the encryption is 128 bits.
D. Validate digital signatures on all incoming packets.

82. What characteristic of Digital Encryption Standard (DES) used in Electronic Code Book (ECB) mode makes it unsuitable for long messages? (Cryptography Domain)

A. Block fragmentation causes message cipher instability.
B. Weak keys will produce symmetrical message holes.
C. Each message block produces a single cipher text block.
D. Repeated message blocks produce repeated cipher text blocks.

83. Separation of duties should be… (Information Security & Risk Management Domain)

A. enforced in all organizational areas.
B. cost justified for the potential of loss.
C. enforced in the program testing phase of application development.
D. determined by the availability of trained staff.

84. Which of the following is an advantage of the Rivest, Shamir, Adelman (RSA) public key system over the Digital Signature Algorithm (DSA)? (Cryptography Domain)

    A. It uses the secure hash algorithm to condense a message before signing.

    B. It can be used for encryption.

    C. It cannot be compromised through substitution.

    D. It uses the function of escrowed encryption.

85. What common attack can be used against a system that stores one-way encrypted passwords if a copy of the password file can be obtained? (Cryptography Domain)

    A. Birthday attack

    B. Dictionary attack

    C. Plaintext attack

    D. Smurf attack

86. When securing Internet connections, which of the following should be used to protect internal routing and labeling schemes? (Telecommunications & Network Security Domain)

    A. Virtual Private Networks (VPN)

    B. Layer 2 Tunneling Protocol (L2TP)

    C. Domain Name Systems (DNS)

    D. Network Address Translation (NAT)

87. When establishing a violation tracking and analysis process, which of the following parameter is used to keep the quantity of data to manageable levels? (Operations Security Domain)

    A. Quantity baseline

    B. Maximum log size

    C. Circular logging

    D. Clipping levels

88. The Initial phase of the system development life cycle would normally include… (Security Architecture & Design Domain)

    A. cost-benefit analysis.

    B. system design review.

    C. executive project approval.

D. project status summary.

89. Which of the following security model is used for enforcing data confidentiality only? (Security Architecture & Design Domain)

A. Clark-Wilson.

B. Bell-LaPadula.

C. Biba.

D. Brewer-Nash.

90. The accounting branch of a large organization requires an application to process expense vouchers. Each voucher must be input by one of many accounting clerks, verified by the clerk's applicable supervisor then reconciled by an auditor before the reimbursement check is produced. What access control technique should be built into the application to meet the information protection needs? (Access Control Domain)

A. Mandatory Access Control (MAC)

B. Password Security

C. Role-based Access Control (RBAC)

D. Terminal Access Controller Access System (TACACS)

91. What security implementation principle recommends division of responsibilities so that one person cannot commit an undetected fraud? (Information Security & Risk Management Domain)

A. Separation of duties.

B. Collusion.

C. Need to know.

D. Least privilege.

92. Which type of communication should an investigator use so the hacker is not aware of an ongoing investigation? (Application Security Domain)

A. PGP authenticated mail.

B. Digitally signed e-mail.

C. Shared directory documents.

D. Out-of-band messaging.

93. Looting of computing assets in a data center after Hurricane Katrina is considered as what type of physical security threat? (Physical and Environmental Security Domain)

A. Natural/environmental threat.

B. Man made threat.

C. Politically motivated threat.

D. Insider threat.

94. What technique can be used to defeat a callback security system? (Telecommunications & Network Security Domain)

A. War dialer.

B. Call forwarding.

C. Secure Modem.

D. Direct inward dial calling.

95. Why does fiber optic communication technology have a significant security advantage over other transmission technology? (Telecommunications & Network Security Domain)

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.

96. Trusted computing base (TCB) is comprised of what combination of system components? (Security Architecture and Design Domain)

1. Hardware.
2. Firmware.
3. Software.

A. 1 and 3.

B. 2 and 3.

C. 1 and 2.

D. All of the above.

97. When verifying security controls in a system design, the security specialist should ensure that the… (Operations Security Domain)

A. final system design has security administrator approval.

B. auditing procedures have been defined.

C. vulnerability assessment has been conducted.

D. impact assessment has been approved.

98. Which of the following protocol is commonly used to verify dial-up connections between hosts? (Telecommunications & Network Security Domain)

A. Unix-to-Unix Communication Protocol (UTJCP)

B. Challenge Handshake Authentication Protocol (CHAP)

C. Point-to-Point Tunneling Protocol (PPTP)

D. Simple Key management for Internet Protocol (SKIP)

99. What type of cryptographic attack enables an attacker to discover the cryptographic key by selecting a series of plaintext and corresponding ciphertext? (Cryptography Domain)

A. Purchase-key attack

B. Chosen plaintext attack

C. Known plaintext attack

D. Chosen-key attack

100. Which statement below most accurately reflects the goal of risk mitigation? (Information Security & Risk Management Domain)

A. Defining the acceptable level of risk the organization can tolerate, then reduce risk to that level.

B. Analyzing and removing all vulnerabilities and threats to security within the organization.

C. Defining the acceptable level of risk the organization can tolerate, and assigning any costs associated with loss or disruption to a third party such as an insurance carrier.

D. Analyzing the effects of a business disruption and preparing the company's response.