# Chapter7:

**Item number 68**

Chapter 7: Physical and Environmental Security

Section: Removing Data from Drives

Item type: Multiple Choice

Question: Which of the following does not destroy the data on a hard drive?

Options:

1. Disk wiping
2. Data destruction
3. Formatting
4. Degaussing

Answer: C

Explanation: Formatting deletes the operating system and the addressing table from a disk, but it does not delete the actual data. The data can be restored with data recovery software.

**Item number 69**

Chapter 7: Physical and Environmental Security

Section: Removing Data from Drives

Item type: Multiple Choice

Question: Which of the following can permanently remove data from a drive?

Options:

1. Deleting and formatting
2. Deleting and disk wiping
3. Formatting and degaussing
4. Disk wiping and degaussing

Answer: D

Explanation: The two methods to permanently remove data from a drive are disk wiping and degaussing. Deleting removes only the operating systems reference to a file and formatting deletes the MBR and operating system without actually deleting the data.

**Item number 70**

Chapter 7: Physical and Environmental Security

Section: What About Disposal?

Item type: Multiple Choice

Question: Which of the following statements best describes hidden files?

Options:

1. Temporary storage of web documents, such as HTML pages and downloads
2. Files that the operating system by design does not display
3. A temporary holding area for files being created
4. Files that authorized users can view and access

Answer: B

Explanation: Hidden files are files that the operating system does not display.

**Item number 71**

Chapter 7: Physical and Environmental Security

Section: Removing Data from Drives

Item type: Multiple Choice

Question: Which of the following statements about formatting is not true?

Options:

1. Formatting deletes the master boot record.
2. Formatting permanently deletes the files on a disk.
3. Formatting deletes the operating system address table.
4. All the above are true.

Answer: B

Explanation: Formatting does not permanently delete the data on a disk, only the master boot record and the system address table. Files can be recovered with data recovery software.

**Item number 72**

Chapter 7: Physical and Environmental Security

Section: What About Disposal?

Item type: Multiple Choice

Question: Which of the following statements best describes metadata?

Options:

1. Information about websites visited
2. Files that the operating system by design does not display
3. Details about a file that describe or identify it
4. Temporary storage area for web documents

Answer: C

Explanation: Metadata is data about data and contains details about a file that describe or identify it such as author’s name, dates and times, and subjects.

**Item number 73**

Chapter 7: Physical and Environmental Security

Section: What About Disposal?

Item type: Multiple Choice

Question: Which of the following statements best describes a cookie?

Options:

1. Information about web sites visited
2. Files that the operating system by design does not display
3. Details about a file that describe or identify it
4. Temporary storage area for web documents

Answer: A

Explanation: Cookies store information about visited web site such as site references and login status.

**Item number 74**

Chapter 7: Physical and Environmental Security

Section: What About Disposal?

Item type: Multiple Choice

Question: Which of the following is a temporary storage for web documents such as HTML pages and downloads?

Options:

1. Data cache
2. Metadata
3. Web cache
4. Cookies

Answer: C

Explanation: Web cache is a temporary storage area for web documents such as web pages and downloads.

**Item number 75**

Chapter 7: Physical and Environmental Security

Section: What About Disposal?

Item type: Multiple Choice

Question: Which of the following is an example of a browser-based data?

Options:

1. Cookies
2. Form history
3. Search bar history
4. All the above

Answer: D

Explanation: Browser-based data includes browsing history, download history, form history, search bar history, and cookies.

**Item number 76**

Chapter 7: Physical and Environmental Security

Section: What About Disposal?

Item type: Multiple Choice

Question: Cookies and search items entered into search engines are examples of which of the following?

Options:

1. Metadata
2. Browser-based data
3. Temporary files
4. Web cache

Answer: B

Explanation: Cookies and search terms entered in a search engine are examples of browser-based data. Other browser-based data includes browsing history, download history, and form history.

**Item number 77**

Chapter 7: Physical and Environmental Security

Section: How Dangerous is Fire?

Item type: Multiple Choice

Question: Class C fire extinguishers are best suited for which of the following fires?

Options:

1. Computer equipment fires
2. Fires in document storage areas
3. Fires with liquids and gases
4. Fires involving metals

Answer: A

Explanation: Class C fire extinguishers are used for electrical equipment fires. Class A fire extinguishers are used for paper fire, class B fire extinguishers are used for flammable liquids and gases, and Class D fire extinguishers are used for metals.

**Item number 78**

Chapter 7: Physical and Environmental Security

Section: How Dangerous is Fire?

Item type: Multiple Choice

Question: Class A fire extinguishers are best suited for which of the following?

Options:

1. Computer equipment fires
2. Fires in document storage areas
3. Fires with liquids and gases
4. Fires involving metals

Answer: B

Explanation: Class A fire extinguishers are used for paper fires. Class C fire extinguishers are used for electrical equipment fires, Class B are used for flammable liquids and gases, and Class D are used for metals.

**Item number 79**

Chapter 7: Physical and Environmental Security

Section: Energy Consumption

Item type: Multiple Choice

Question: Which of the following is recommended to reduce energy consumption?

Options:

1. Turning off peripherals when not in use
2. Turning off monitors when not in use
3. Turing off computer when not in use
4. All the above

Answer: D

Explanation: According to the Cornell University turning-off peripherals, monitors and computers when not in use can reduce daily power consumption by up to 88 percent.

**Item number 80**

Chapter 7: Physical and Environmental Security

Section: How Dangerous Is fire?

Item type: Multiple Choice

Question: Which of the following is the first line of defense in case of fires?

Options:

1. Fire detection controls
2. Fire prevention controls
3. Fire containments controls
4. Fire suppression controls

Answer: B

Explanation: The first line of defense in case of fires is active and passive fire prevention controls.

**Item number 81**

Chapter 7: Physical and Environmental Security

Section: How Dangerous Is fire?

Item type: Multiple Choice

Question: Which of the following is an example of a fire prevention control?

Options:

1. Fire containment equipment
2. Fire extinguishers
3. Fire suppressors
4. Adhering to building and construction codes

Answer: D

Explanation: Fire prevention controls are the first line for defense and include adhering to building and construction codes, using flame resistant materials, proper handling and storage of flammable materials, and hazard inspections and assessments.

**Item number 82**

Chapter 8: Communications and Operations Security

Section: Are There Different Types of Malware?

Item type: Multiple Choice

Question: Which of the following best describes the difference between a virus and a worm?

Options:

1. A virus is malicious software that requires a host file to spread itself, whereas a worm is malicious software that does not require a host file to spread itself.
2. A worm is a malicious software that requires a host file to spread itself, whereas a virus is malicious software that does not require a host file to spread itself.
3. A virus is malicious software that attaches itself to executable files, whereas a worm is malicious software that attaches itself to an image file.
4. There is not difference between a virus and a worm.

Answer: A

Explanation: Both viruses and worms are malicious software, but a virus requires a host file to spread whereas a worm can spread from machine to machine without a host file.

**Item number 83**

Chapter 8: Communications and Operations Security

Section: How Is Malware Controlled?

Item type: Multiple Choice

Question: Which of the following is an example of a malware prevention control?

Options:

1. Real-time firewall detection of suspicious file downloads
2. Review and analysis of log files
3. User awareness to recognize and report suspicious activity
4. Not allowing users to have administrative rights on their workstations

Answer: D

Explanation: Not allowing users to have admin rights on their workstations is an example of a malware prevention control because most malware requires administrative access to install on a machine. The remaining choices are examples of detection controls.

**Item number 84**

Chapter 8: Communications and Operations Security

Section: Are There Different Types of Malware?

Item type: Multiple Choice

Question: Which of the following statements best describes a Trojan?

Options:

1. Malicious software that hides into the lower levels of the operating system and opens a backdoor
2. Malicious software that records every key stroke and mouse movement
3. Malicious software that disguises itself as a legitimate program
4. Malicious software that takes the computer data hostage to extort money

Answer: C

Explanation: Trojans are malicious software that disguises themselves as legitimate programs. Ransomware is a type of malware that encrypts the data on a drive unless the owner pays a requested amount of money. A keylogger is malicious software that records every key stroke and mouse movement. A rootkit is malicious software that hides in the lower levels of the operating system with privileged access permissions and opens a backdoor on a system.

**Item number 85**

Chapter 8: Communications and Operations Security

Section: Are There Different Types of Malware?

Item type: Multiple Choice

Question: Which of the following statements about Trojans is true?

Options:

1. Trojans reproduce by infecting other files.
2. Trojans need user interaction to spread.
3. Trojans self-replicate.
4. Trojans are legitimate programs that enhance user experience.

Answer: B

Explanation: Trojans are malicious software that cannot reproduce by infecting other files and cannot self-replicate but need user interaction to spread.

**Item number 86**

Chapter 8: Communications and Operations Security

Section: Data Replication

Item type: Multiple Choice

Question: Which of the following statements best describes data duplication?

Options:

1. The process of copying data to another drive weekly
2. The process of copying data to a second location that is available for immediate use
3. The process of copying and storing data that could be restored to its original location
4. The process of copying data to the cloud

Answer: B

Explanation: Data replication is the process of copying data to a second location with the data available for immediate use without the need of restoring it.

**Item number 87**

Chapter 8: Communications and Operations Security

Section: Data Replication

Item type: Multiple Choice

Question: Which of the following statements about data backup is not true?

Options:

1. Backups can be stored in the cloud.
2. Backups can be conducted once a week.
3. Backups do not have to be restored as long as they are stored in the cloud.
4. Backups can be stored to a tape.

Answer: C

Explanation: Data backup is the process of copying and storing data that needs to be restored before it can be used. Backups can be stored on tape, other drives, and in the cloud.

**Item number 88**

Chapter 8: Communications and Operations Security

Section: What Is Antivirus Software?

Item type: Multiple Choice

Question: Which of the following statements about antivirus software is not true?

Options:

1. Antivirus software uses signature-based recognition and behavior-based recognition to detect malware.
2. Antivirus software can detect various types of malware.
3. Antivirus software is 100 percent effective against malware intrusions.
4. Antivirus software can detect, contain, or eliminate malware.

Answer: C

Explanation: Antivirus software can be used to detect, contain, or eliminate malware and can use signature-based or behavior-based recognition, but it is not 100 percent effective. The antivirus software can detect only the malware it knows about.

**Item number 89**

Chapter 8: Communications and Operations Security

Section: Understanding Embedded Malware

Item type: Multiple Choice

Question: Which of the following malware takes advantage of a security vulnerability on the same day that the vulnerability becomes known to the public?

Options:

1. Ransomware
2. Screen scraper
3. Zero-day exploit
4. Bot

Answer: C

Explanation: A zero-day exploit takes advantage of a vulnerability that was released on the same day. Ransomware is a type of malware that encrypts the data on a drive unless the owner pays a requested amount of money. A screen scraper makes a copy of the user’s screen. A bot is a snippet of code commonly used by an attacker to automate tasks and carry out a denial-of-service attack.

**Item number 90**

Chapter 8: Communications and Operations Security

Section: Are There Different Types of Malware?

Item type: Multiple Choice

Question: Which of the following is a snippet of code designed to automate tasks and often used by attackers to carry out a denial-of-service attacks?

Options:

1. Ransomware
2. Screen scraper
3. Zero-day exploit
4. Bot

Answer: D

Explanation: A bot is a snippet of code commonly used by an attacker to automate tasks and carry out a denial-of-service attack. Ransomware is a type of malware that encrypts the data on a drive unless the owner pays a requested amount of money. A screen scraper makes a copy of the user’s screen. A zero-day exploit takes advantage of a vulnerability that was released on the same day.

**Item number 91**

Chapter 8: Communications and Operations Security

Section: Are There Different Types of Malware?

Item type: Multiple Choice

Question: Which of the following is an example of a Trojan that is designed to capture login information to financial websites?

Options:

1. Melissa
2. Zeus
3. Slammer
4. Sapphire

Answer: B

Explanation: Zeus is a Trojan designed to capture banking information and financial login credentials.

**Item number 92**

Chapter 8: Communications and Operations Security

Section: Are There Different Types of Malware?

Item type: Multiple Choice

Question: Which of the following is a worm that infects Microsoft SQL server and Microsoft SQL desktop engine?

Options:

1. Zeus
2. SpyEye
3. Slammer
4. Melissa

Answer: C

Explanation: The Slammer worm is the fastest spreading worm. It infects a Microsoft SQL server and Microsoft SQL desktop engine by exploring an unpatched buffer overflow.

**Item number 93**

Chapter 8: Communications and Operations Security

Section: Are There Different Types of Malware?

Item type: Multiple Choice

Question: Which of the following viruses was distributed as an e-mail attachment and used Microsoft Outlook to e-mail itself to the first 50 contacts in the user address book?

Options:

1. Zeus
2. SpyEye
3. Slammer
4. Melissa

Answer: D

Explanation: The Melissa virus is distributed as an e-mail attachments and when on a system with Microsoft Outlook emailed itself to the first 50 contacts in the user’s address book.

**Item number 94**

Chapter 8: Communications and Operations Security

Section: Activity Monitoring and Log Analysis

Item type: Multiple Choice

Question: Which of the following best describes the trend analysis log analysis technique?

Options:

1. Comparing log data to known bad activity
2. Comparing log data to known good activity
3. Identifying activity over time that in isolation might appear normal
4. Tying individual entries together based on related information

Answer: C

Explanation: Trend analysis involves identifying activity over time that might appear normal otherwise. Signature analysis compares log data to known bad activity. Correlation analysis involves tying individual entries based on related information.

**Item number 95**

Chapter 8: Communications and Operations Security

Section: Activity Monitoring and Log Analysis

Item type: Multiple Choice

Question: Which of the following log analysis techniques compares the log entries against a set of known bad activity?

Options:

1. Trend analysis
2. Signature analysis
3. Correlation analysis
4. Sequencing analysis

Answer: B

Explanation: Signature analysis compares log data to known bad activity. Trend analysis involves identifying activity over time that might appear normal otherwise. Correlation analysis involves tying individual entries based on related information. Sequencing analysis examines activity based on patterns.

**Item number 96**

Chapter 8: Communications and Operations Security

Section: Activity Monitoring and Log Analysis

Item type: Multiple Choice

Question: Which of the following log analysis techniques examines activity based on patterns?

Options:

1. Trend analysis
2. Signature analysis
3. Correlation analysis
4. Sequencing analysis

Answer: D

Explanation: Sequencing analysis examines activity based on patterns. Signature analysis compares log data to known bad activity. Trend analysis involves identifying activity overtime that might appear normal otherwise. Correlation analysis involves tying individual entries together based on related information.

**Item number 97**

Chapter 8: Communications and Operations Security

Section: Activity Monitoring and Log Analysis

Item type: Multiple Choice

Question: Which of the following statements best describes the correlation log analysis technique?

Options:

1. Comparing log data to known bad activity
2. Comparing log data to known good activity
3. Identifying activity over time that in isolation might appear normal
4. Tying individual entries together based on related information

Answer: D

Explanation: Correlation analysis involves tying individual entries together based on related information. Signature analysis compares log data to known bad activity. Trend analysis involves identifying activity over time that might appear normal otherwise.

**Item number 98**

Chapter 9: Access Control Management

Section: How Is Identity Verified?

Item type: Multiple Choice

Question: Using a smart card and a one-time passcode is an example of which of the following authentication methods?

Options:

1. Single-factor authentication
2. Multifactor authentication
3. Multilayer authentication
4. Cognitive password authentication

Answer: C

Explanation: Smart cards and one-time passcodes are examples of something you have authenticated and represent a single factor, so they are an example of a multilayer authentication.

**Item number 99**

Chapter 9: Access Control Management

Section: How Is Identity Verified?

Item type: Multiple Choice

Question: Which of the following is not an example of something you know authentication?

Options:

1. Cognitive password
2. PIN
3. One-time passcode
4. Password

Answer: C

Explanation: A one-time passcode is an example of something you have authenticated.

**Item number 100**

Chapter 9: Access Control Management

Section: How Is Identity Verified?

Item type: Multiple Choice

Question: Which of the following is the most commonly used single-factor authentication method?

Options:

1. PINs
2. Passwords
3. Smart cards
4. Retina scans

Answer: B

Explanation: Passwords are the most commonly used single factor authentication method.

**Item number 101**

Chapter 9: Access Control Management

Section: What Is Authorization?

Item type: Multiple Choice

Question: Which of the following is a type of access control that is defined by a policy and cannot be changed by the information owner?

Options:

1. Mandatory access control
2. Discretionary access control
3. Role-based access control
4. Rule-based access control

Answer: A

Explanation: A mandatory access control is defined by a policy and cannot be changed by the information owner. It is a model commonly used in government and military systems.

**Item number 102**

Chapter 9: Access Control Management

Section: What Is Authorization?

Item type: Multiple Choice

Question: Which of the following is an access control that is based on a specific job roles or functions?

Options:

1. Mandatory access control
2. Discretionary access control
3. Role-based access control
4. Rule-based access control

Answer: C

Explanation: Role-based access control is based on specific job roles or functions.

**Item number 103**

Chapter 9: Access Control Management

Section: How Is Identity Verified?

Item type: Multiple Choice

Question: Providing your mother’s maiden name as verification is an example of which of the following?

Options:

1. One-time passcode
2. Cognitive password
3. Multilayer authentication
4. Multifactor authentication

Answer: B

Explanation: A cognitive password is a type of knowledge-based authentication that is used as a verification mechanism to verify user identity. A mother’s maiden name is a common example of a cognitive password.

**Item number 104**

Chapter 9: Access Control Management

Section: Inherence: Something You Are

Item type: Multiple Choice

Question: Which of the following is an example of an inherence authentication?

Options:

1. Smart card
2. Fingerprint scan
3. One-time passcode
4. Cognitive password

Answer: B

Explanation: Inherence authentication includes using biometrics to identify humans based on distinctive, measurable characteristics such as fingerprint scans and retina scans.

**Item number 105**

Chapter 9: Access Control Management

Section: What Is Authorization?

Item type: Multiple Choice

Question: Which of the following are mandatory access controls embedded in object and subject properties?

Options:

1. Object capabilities
2. Security labels
3. Access control lists
4. Whitelists

Answer: B

Explanation: Security labels are mandatory access controls embedded in object and subject properties. They are one of the three primary authorization models.

**Item number 106**

Chapter 9: Access Control Management

Section: What Is Authorization?

Item type: Multiple Choice

Question: Which of the following statements best describes object capability?

Options:

1. Mandatory access controls embedded in object and subject properties
2. Used to determine access based on a combination of specific criteria
3. Used programmatically and based on a combination of an unforgettable reference and an operational message
4. The process of assigning authenticated subjects permission to carry out a specific task

Answer: C

Explanation: Object capability is used programmatically and based on a combination of an unforgettable reference and an operational message.

**Item number 107**

Chapter 9: Access Control Management

Section: Infrastructure Access Controls

Item type: Multiple Choice

Question: Which of the following is a segment of the internal network that requires a high degree of protection?

Options:

1. Enclave network
2. Trusted network
3. DMZ
4. Guest network

Answer: A

Explanation: An enclave network is a segment of the internal network that requires a high degree of protection.

**Item number 108**

Chapter 9: Access Control Management

Section: Infrastructure Access Controls

Item type: Multiple Choice

Question: The Internet is an example of which of the following networks?

Options:

1. Enclave network
2. Untrusted network
3. DMZ
4. Guest network

Answer: B

Explanation: An untrusted network is one outside of your control. The Internet is an example of an untrusted network.

**Item number 109**

Chapter 9: Access Control Management

Section: What Is Layered Border Security?

Item type: Multiple Choice

Question: Which of the following best describes the purpose of a firewall?

Options:

1. Passive devices that analyze network traffic to detect unauthorized access
2. Active devices that sit inline with traffic and can respond to intrusions by disabling the connection, dropping the packet, or deleting the malicious content
3. A software or hardware device that can filter incoming or outgoing traffic based on specific rules
4. A device that monitors the characteristics of a single host and the events occurring on that host

Answer: C

Explanation: A firewall is a software or a hardware device that can filter incoming or outgoing traffic based on certain criteria.

**Item number 110**

Chapter 9: Access Control Management

Section: What Is Layered Border Security?

Item type: Multiple Choice

Question: Which of the following best describes an intrusion prevention system?

Options:

1. Passive devices that analyze network traffic to detect unauthorized access
2. Active devices that sit inline with traffic and can respond to intrusions by disabling the connection, dropping the packet, or deleting the malicious content
3. A software or hardware device that can filter incoming or outgoing traffic based on specific rules
4. A device that monitors the characteristics of a single host and the events occurring on that host

Answer: B

Explanation: An Intrusion prevention system (IPS) is an active device that monitors traffic and can respond to intrusions.

**Item number 111**

Chapter 10: Information Systems Acquisition, Development, and Maintenance

Section: What Is PKI?

Item type: Multiple Choice

Question: Which of the following is used to associate a public key with an identity?

Options:

1. Encryption
2. Digital hash
3. Digital certificate
4. Digital signature

Answer: C

Explanation: A digital certificate is used to associate a public key with an identity. The certificates contain the public key and are digitally signed.

**Item number 112**

Chapter 10: Information Systems Acquisition, Development, and Maintenance

Section: Asymmetric Key

Item type: Multiple Choice

Question: Which of the following statements about asymmetric key cryptography is true?

Options:

1. Asymmetric key cryptography uses one shared key.
2. Asymmetric key cryptography is also called private key cryptography.
3. Asymmetric key cryptography uses two keys called public keys.
4. Asymmetric key cryptography is also called public key cryptography.

Answer: D

Explanation: Asymmetric key cryptography is also called public key cryptography, and it uses two keys that are mathematically related called public and private key.

**Item number 113**

Chapter 10: Information Systems Acquisition, Development, and Maintenance

Section: What Is PKI?

Item type: Multiple Choice

Question: Which of the following issues and maintains digital certificates?

Options:

1. Registration Authority
2. Certification Authority
3. Public Key Infrastructure
4. Client nodes

Answer: B

Explanation: The Certification Authority is responsible for issuing and maintaining digital certificates.

**Item number 114**

Chapter 10: Information Systems Acquisition, Development, and Maintenance

Section: Disposal Phase

Item type: Multiple Choice

Question: Which of the following tasks is part of the disposal phase of the SDLC?

Options:

1. Authorization
2. Conducting risk assessment
3. Archiving information and sanitization of media
4. Adding hardware and software

Answer: C

Explanation: Archiving information and sanitization of media is part of the disposal phase of the SDLC. Authorization is part of the implementation phase; risk assessment is part of the development phase; and identification of compliance requirements is part of the initiation phase.

**Item number 115**

Chapter 10: Information Systems Acquisition, Development, and Maintenance

Section: Initiation phase

Item type: Multiple Choice

Question: Identification of compliance requirements is done during which of the following phases of the SDLC?

Options:

1. Initiation
2. Development
3. Implementation
4. Operational

Answer: A

Explanation: Identification of compliance requirements is done during the first, initiation phase of the SDLC.

**Item number 116**

Chapter 10: Information Systems Acquisition, Development, and Maintenance

Section: What Is Injection?

Item type: Multiple Choice

Question: Which of the following is the most common web application vulnerability?

Options:

1. Failure to validate output
2. Failure to validate input
3. Dynamic data validation
4. Static data validation

Answer: B

Explanation: The most common web application vulnerability is the failure to validate input. Not validating input can lead to SQL injection and other injection attacks.

**Item number 117**

Chapter 10: Information Systems Acquisition, Development, and Maintenance

Section: Symmetric Keys

Item type: Multiple Choice

Question: Symmetric key cryptography uses which of the following?

Options:

1. One public key
2. One shared key
3. Two public keys
4. One public and one private key

Answer: B

Explanation: Symmetric key cryptography uses one shared key that has to be shared in advance.

**Item number 118**

Chapter 10: Information Systems Acquisition, Development, and Maintenance

Section: Symmetric Keys

Item type: Multiple Choice

Question: Which of the following is the most well-known symmetric algorithm?

Options:

1. AES
2. RSA
3. DES
4. IPsec

Answer: C

Explanation: DES is the most well-known symmetric algorithm.

**Item number 119**

Chapter 10: Information Systems Acquisition, Development, and Maintenance

Section: Symmetric keys

Item type: Multiple Choice

Question: Which of the following statements about symmetric key cryptography is not true?

Options:

1. Symmetric key cryptography uses one shared key.
2. Symmetric algorithms can provide confidentiality.
3. Symmetric algorithms can provide nonrepudiation and authenticity.
4. Symmetric key cryptography uses a single secret key.

Answer: C

Explanation: Symmetric algorithms cannot provide nonrepudiation and authenticity because the keys are shared.

**Item number 120**

Chapter 10: Information Systems Acquisition, Development, and Maintenance

Section: What Is PKI?

Item type: Multiple Choice

Question: Which of the following are components of PKI?

Options:

1. Certification Authority
2. Registration Authority
3. Client nodes
4. All the above

Answer: D

Explanation: PKI is a framework of services used to create, manage, distribute, and revoke public keys. Components of PKI include Certification Authority, Registration Authority, client nodes, and digital certificates.

**Item number 121**

Chapter 11: Information Security Incident Management

Section: How Are Incidents Reported?

Item type: Multiple Choice

Question: Which of the following statements is not true?

Options:

1. Employees should report all actual incidents.
2. Employees should report all suspected incidents.
3. Employees should assign a severity level when reporting incidents.
4. Employees should not be penalized if they report a perceived incident that ends up being a false positive.

Answer: C

Explanation: Employees should be encouraged to report all incidents, actual and perceived, even if the reported incident ends up being a false positive. Employees should not assign a severity level because they might not properly assess the incident and determine its severity.

**Item number 122**

Chapter 11: Information Security Incident Management

Section: Incident Severity Levels

Item type: Multiple Choice

Question: Which of the following is an example of a Level 2 incident?

Options:

1. Malware detected on multiple systems
2. User’s excessive use of bandwidth and resources
3. Compromise of any company web site or company presence
4. Compromise or suspected compromise of protected customer information

Answer: A

Explanation: Malware detected on multiple systems is a Level 2 incident. Compromising company web presence and web sites and compromise of protected customer information are examples of Level 1 incident. User’s excessive use of resources is an example of a Level 3 incident.

**Item number 123**

Chapter 11: Information Security Incident Management

Section: Incident Severity Levels

Item type: Multiple Choice

Question: Which of the following is an example of a Level 1 incident?

Options:

1. Inappropriate access to legally protected or proprietary information
2. Malware detected on multiple systems
3. User access to content or sites restricted by policy
4. Denial-of-service attack

Answer: D

Explanation: A denial-of-service attack is an example of a Level 1 incident. Inappropriate access to legally protected or proprietary information and malware detected on multiple systems are an example of a Level 2 incident. User access to content restricted by policy is an example of Level 3 incident.

**Item number 124**

Chapter 11: Information Security Incident Management

Section: Incident Severity Levels

Item type: Multiple Choice

Question: Which of the following is an example of a Level 3 incident?

Options:

1. Malware detected on multiple systems
2. User’s excessive use of bandwidth and resources
3. Compromise of any company web site or company presence
4. Compromise or suspected compromise of protected customer information

Answer: B

Explanation: User’s excessive use of resources is an example of a Level 3 incident. Malware detected on multiple systems is a Level 2 incident. Compromising company web presence and web sites and compromise of protected customer information are examples of Level 1 incident.

**Item number 125**

Chapter 11: Information Security Incident Management

Section: How Are Incidents Reported?

Item type: Multiple Choice

Question: Who must be notified of Level 3 incidents?

Options:

1. Chief executive officer
2. Chief operating officer
3. Chief information security officer
4. Legal council

Answer: C

Explanation: The chief information security officer must be notified about all Level 3 incidents.

**Item number 126**

Chapter 11: Information Security Incident Management

Section: Data Breach Notification Requirements

Item type: Multiple Choice

Question: Which of the following regulations address the protection of personally identifiable information?

Options:

1. HITECH
2. FISMA
3. GLBA
4. All the above

Answer: D

Explanation: Many federal regulations such as HITECH, GLBA, FISMA, and FERPA address the protection of personally identifiable information.

**Item number 127**

Chapter 11: Information Security Incident Management

Section: HIPAA/HITECH Personal Healthcare Information (PHI)

Item type: Multiple Choice

Question: Within what time frame does the HITECH Act require covered entities to notifying affected individuals of a data breach of personal healthcare information?

Options:

1. 1 week
2. 30 days
3. 40 five
4. 60 days

Answer: D

Explanation: The HITECH Act requires covered entities to notify affected individual within 60 days of the discovery of any breach of personal healthcare information.

**Item number 128**

Chapter 11: Information Security Incident Management

Section: State Breach Notification Laws

Item type: Multiple Choice

Question: Which of the following states does not have security breach law?

Options:

1. Alabama
2. Texas
3. California
4. Massachusetts

Answer: A

Explanation: Alabama, Kentucky, New Mexico, and South Dakota are states that do not have security breach laws.

**Item number 129**

Chapter 11: Information Security Incident Management

Section: What Is an Incident Response Program?

Item type: Multiple Choice

Question: Which of the following best describes the purpose of the detection and investigation portion of the incident response plan?

Options:

1. To describe the steps that need to be taken to prevent the incident from spreading
2. To establish processes and knowledge base to accurately detect and assess precursors and indicators
3. To describe incident declaration and notification
4. To describe the steps to eliminate the components of the incident

Answer: B

Explanation: The detection and investigation portion of the incident response plan includes the processes and knowledge base to accurately detect and assess precursors and indications of an incident.

**Item number 130**

Chapter 11: Information Security Incident Management

Section: Incident Severity Level

Item type: Multiple Choice

Question: A denial-of-service attack is considered which of the following?

Options:

1. Level 1 incident
2. Level 2 incident
3. Level 3 incident
4. Internal incident

Answer: A

Explanation: A denial-of-service attack is considered a Level 1 incident.

**Item number 131**

Chapter 12: Business Continuity Management

Section: Why Is Testing Important?

Item type: Multiple Choice

Question: Which of the following testing exercises are discussion-based only and don’t involve deploying equipment or other resources

Options:

1. Functional exercises
2. Full scale testing
3. Tabletop exercise
4. Plan audits

Answer: C

Explanation: Tabletop exercises are only discussion-based and do not involve deploying equipment and other resources. Structures review and simulations are the two types of tabletop exercises.

**Item number 132**

Chapter 12: Business Continuity Management

Section: Relocation Strategies

Item type: Multiple Choice

Question: Which of the following best describes a warm site?

Options:

1. A backup facility that has power and HVAC but no equipment
2. A self-contained unit that has hardware, software, and peripherals
3. A fully operational location that is ready for immediate move in and contains all data
4. An operational location that contains all equipment but data must be restored

Answer: D

Explanation: A warm site contains all necessary equipment, but data must be restored for the company to continue operations.

**Item number 133**

Chapter 12: Business Continuity Management

Section: Relocation Strategies

Item type: Multiple Choice

Question: Which of the following best describes a mobile site?

Options:

1. A backup facility that has power and HVAC but no equipment.
2. A self-contained unit that has hardware, software, and peripherals.
3. A fully operational location that is ready for immediate move in and contains all data.
4. An operational location that contains all equipment, but data must be restored.

Answer: B

Explanation: A mobile site is a self-contained unit that has hardware, peripherals, and software, but data must be restored.

**Item number 134**

Chapter 12: Business Continuity Management

Section: What Is a Business Impact Assessment?

Item type: Multiple Choice

Question: Which of the following is the total length of time an essential business function can be unavailable without causing significant harm to the organization?

Options:

1. Maximum tolerable downtime
2. Maximum tolerable uptime
3. Recovery time objective
4. Recovery point objective

Answer: A

Explanation: The maximum tolerable downtime (MTD) is the total length of time an essential business function can be unavailable without causing significant harm to the organization.

**Item number 135**

Chapter 12: Business Continuity Management

Section: What Is a Business Impact Assessment?

Item type: Multiple Choice

Question: Which of the following represents the acceptable data loss?

Options:

1. Maximum tolerable downtime
2. Maximum tolerable uptime
3. Recovery time objective
4. Recovery point objective

Answer: D

Explanation: The recovery point objective (RTO) is the point of time prior to the system disruption that data can be recovered.

**Item number 136**

Chapter 12: Business Continuity Management

Section: The Business Continuity Plan

Item type: Multiple Choice

Question: Which of the following plans focuses on the initial response and includes plan activation, notification, evacuation, and communication?

Options:

1. Response plans
2. Contingency plans
3. Recovery plans
4. Resumption plans

Answer: A

Explanation: Response plans focus on initial response and include elements such as plan activation, evacuation procedures, notification procedures, communication, and security. Resumption plans guide the organization back to normalcy. Contingency plans focus on immediate, near-term, and short-term alternative workforce and business processes. Recovery plans focus on recovery of information systems and facilities.

**Item number 137**

Chapter 12: Business Continuity Management

Section: The Business Continuity Plan

Item type: Multiple Choice

Question: Which of the following business continuity plans focus on the immediate and near-term alternative workplace and business processes?

Options:

1. Response plans
2. Contingency plans
3. Recovery plans
4. Resumption plans

Answer: B

Explanation: Contingency plans focus on immediate, near-term, and short-term alternate workforce and business processes. Response plans focus on initial response and include elements such as plan activation, evacuation procedures, notification procedures, communication, and security. Resumption plans guide the organization back to normalcy. Recovery plans focus on recovery of information systems and facilities.

**Item number 138**

Chapter 12: Business Continuity Management

Section: The Resumption Phase

Item type: Multiple Choice

Question: Which of the following is the official notification that the organization is no longer operating in an emergency or disaster mode?

Options:

1. Validation
2. Activation
3. Deactivation
4. Resumption

Answer: C

Explanation: Deactivation is the official notification that an organization is no longer in emergency or disaster mode.

**Item number 139**

Chapter 12: Business Continuity Management

Section: Plan Testing and Maintenance

Item type: Multiple Choice

Question: Which of the following statements best describes functional exercises?

Options:

1. Testing conducted at the enterprise level with a full simulation of a disaster with suspending all operations
2. Scenario-driven exercises but limited in scope to simulate a failure of a critical business function
3. A discussion-based exercise that does not involve deploying equipment or other resources
4. A systematic walkthrough of the procedures to determine disaster readiness

Answer: B

Explanation: Functional exercises are scenario-driven but limited in scope. Full-scale testing simulates a real disaster. Tabletop simulations are discussion-based and structured reviews are a procedure walkthroughs.

**Item number 140**

Chapter 12: Business Continuity Management

Section: Plan Testing and Maintenance

Item type: Multiple Choice

Question: Which of the following best describes full-scale testing?

Options:

1. Testing conducted at the enterprise level with a full simulation of a disaster with suspending all operations
2. Scenario-driven exercises but limited in scope to simulate a failure of a critical business function
3. A discussion-based exercise that does not involve deploying equipment or other resources
4. A systematic walkthrough of the procedures to determine disaster readiness

Answer: A

Explanation: Full-scale testing simulates a real disaster. Functional exercises are scenario-driven but limited in scope. Tabletop simulations are discussion-based and structured reviews are procedure walkthroughs.

**Item number 141**

Chapter 13: Regulatory Compliance for Financial Institutions

Section: What Is a Federal Institution?

Item type: Multiple Choice

Question: Which of the following agencies regulates financial institutions not covered by other agencies?

Options:

1. Federal Trade Commission (FTC)
2. Commodity Futures Trading Commission (CFTC)
3. National Credit Union Administration (NCUA)
4. Federal Deposit Insurance Corporation (FDIC)

Answer: A

Explanation: The FTC regulates institutions not covered by other agencies. The National Credit Union Administration is responsible for regulating federally chartered credit unions. CFTC regulates futures and option markets. FDIC regulates state-chartered banks.

**Item number 142**

Chapter 13: Regulatory Compliance for Financial Institutions

Section: What Is a Federal Institution?

Item type: Multiple Choice

Question: Which of the following agencies regulates state-chartered banks?

Options:

1. Federal Trade Commission (FTC)
2. Commodity Futures Trading Commission (CFTC)
3. National Credit Union Administration (NCUA)
4. Federal Deposit Insurance Corporation (FDIC)

Answer: D

Explanation: The FDIC regulates state-chartered banks. The National Credit Union Administration is responsible for regulating federally chartered credit unions. The FTC regulates institutions not covered by other agencies. CFTC regulates futures and option markets.

**Item number 143**

Chapter 13: Regulatory Compliance for Financial Institutions

Section: What Is a Federal Institution?

Item type: Multiple Choice

Question: The Federal Reserve Board is responsible for regulating which of the following?

Options:

1. Bank holding companies and member banks of the Federal Reserve System
2. National banks, federal saving associations, and federal branches of foreign banks
3. Federally charted credit unions
4. State-chartered banks

Answer: A

Explanation: The Federal Reserve Board (FRB) regulates banks holding companies and member banks of the Federal Reserve System. The OCC regulates national banks, federal saving associations, and federal branches of foreign banks. The National Credit Union Administration is responsible for regulating federally chartered credit unions. FDIC regulates state-chartered banks.

**Item number 144**

Chapter 13: Regulatory Compliance for Financial Institutions

Section: Assess Risk

Item type: Multiple Choice

Question: Which of the following statements best describes operational risk?

Options:

1. The risk arising from adverse business decisions
2. The risk arising from negative public opinion
3. The risk arising from problems with service or product delivery
4. The risk of loss resulting from inadequate or failed internal processes, people, or systems

Answer: D

Explanation: The risk of loss resulting from inadequate or failed internal processes, people, or systems is operational risk. Transactional risk is the risk arising from problems with service or product delivery. The risk arising from adverse business decisions is strategic risk. The risk arising from negative public opinion is reputational risk.

**Item number 145**

Chapter 13: Regulatory Compliance for Financial Institutions

Section: Assess Risk

Item type: Multiple Choice

Question: Which of the following statements best describes reputational risk?

Options:

1. The risk arising from adverse business decisions
2. The risk arising from negative public opinion
3. The risk arising from problems with service or product delivery
4. The risk of loss resulting from inadequate or failed internal processes, people, or systems

Answer: B

Explanation: The risk arising from negative public opinion is reputational risk. Transactional risk is the risk arising from problems with service or product delivery. The risk arising from adverse business decisions is strategic risk. The risk of loss resulting from inadequate or failed internal processes, people, or systems is operational risk.

**Item number 146**

Chapter 13: Regulatory Compliance for Financial Institutions

Section: Testing

Item type: Multiple Choice

Question: Which of the following best describes an assessment?

Options:

1. Evidenced-based examination that compares current practices against a specific internal or external criteria
2. A focused privileged inspection to determine condition, locate weakness or vulnerabilities, and identity corrective actions
3. Testing controls by performing vulnerability assessment tests that simulate real attacks
4. Configuring the System and Security logs on each system to record and audit activities

Answer: B

Explanation: A focused privileged inspection to determine condition, locate weakness or vulnerabilities, and identity corrective actions is an assessment. An audit is an evidenced-based examination that compares current practices against a specific internal or external criteria and testing controls by performing vulnerability assessment tests that simulate real attacks is an assurance.

**Item number 147**

Chapter 13: Regulatory Compliance for Financial Institutions

Section: Testing

Item type: Multiple Choice

Question: Which of the following testing measures how well controls and safeguards work by subjecting the system to an attack?

Options:

1. Testing
2. Audit
3. Assurance
4. Assessment

Answer: C

Explanation: Testing controls by performing vulnerability assessment tests that simulate real attacks is an assurance. An audit is an evidenced-based examination that compares current practices against specific internal or external criteria. A focused privileged inspection to determine condition, locate weakness or vulnerabilities, and identity corrective actions is an assessment.

**Item number 148**

Chapter 13: Regulatory Compliance for Financial Institutions

Section: Testing

Item type: Multiple Choice

Question: Which of the following is an evidence-based examination that compares current practices against internal or external criteria?

Options:

1. Testing
2. Audit
3. Assurance
4. Assessment

Answer: B

Explanation: An audit is an evidenced-based examination that compares current practices against specific internal or external criteria. Testing controls by performing vulnerability assessment tests that simulate real attacks is an assurance. A focused privileged inspection to determine condition, locate weakness or vulnerabilities, and identity corrective actions is an assessment.

**Item number 149**

Chapter 13: Regulatory Compliance for Financial Institutions

Section: The Federal Trade Commission (FTC) Safeguards Act

Item type: Multiple Choice

Question: What is the FTC implementation of the GBLA?

Options:

1. Interagency guidelines
2. Guidelines for Safeguarding Member Information
3. Safeguards Act
4. Banks Holding Company Act

Answer: C

Explanation: The FTC implementation of the GLBA is the Safeguards Act. The Interagency Guidelines apply to banks, and the Guidelines for Safeguarding Member Information apply to credit unions.

**Item number 150**

Chapter 13: Regulatory Compliance for Financial Institutions

Section: The Gramm-Leach-Bliley Act

Item type: Multiple Choice

Question: What is the term used to describe names, addresses, and phone numbers when linked to bank and credit card account information?

Options:

1. Private information
2. Nonpublic personal information
3. Nonpublic private information
4. Personal information

Answer: B

Explanation: Names, addresses, and phone numbers linked to bank and credit card number are considered nonpublic personal information (NPPI).

**Item number 151**

Chapter 13: Regulatory Compliance for Financial Institutions

Section: Assess Risk

Item type: Multiple Choice

Question: Financial institutions must address which of the following threats at a minimum?

Options:

1. Denial-of-service attacks
2. Unauthorized access
3. Unauthorized data modification
4. System infiltration
5. Malware
6. Destruction of data or systems
7. All the above

Answer: G

Explanation: At minimum financial institutions must address the following threats: denial-of-service attacks, unauthorized access, unauthorized data modification, system infiltration, malware, and destruction of data or systems.

**Item number 152**

Chapter 14: Regulatory Compliance for the Healthcare Sector

Section: The HIPAA Security Rule

Item type: Multiple Choice

Question: Which of the following statements best describes a healthcare provider?

Options:

1. A person or organization that provides patient or medical services
2. An entity that provides payment for medical services
3. An entity that processes nonstandard health information it receives from another entity
4. A person or entity that creates, receives, maintains, transmits, accesses, or has the potential to access ePHI

Answer: A

Explanation: A person or organization that provides patient or medical services is considered a healthcare provider. A health plan is an entity that provides payment for medical services. A healthcare clearinghouse is an entity that processes nonstandard health information it receives from another entity. A business associate is a person or entity that creates, receives, maintains, transmits, accesses, or has the potential to access ePHI.

**Item number 153**

Chapter 14: Regulatory Compliance for the Healthcare Sector

Section: The HIPAA Security Rule

Item type: Multiple Choice

Question: Which of the following statements best describes a healthcare clearing house?

Options:

1. A person or organization that provides patient or medical services
2. An entity that provides payment for medical services
3. An entity that processes nonstandard health information it receives from another entity
4. A person or entity that creates, receives, maintains, transmits, accesses, or has the potential to access ePHI

Answer: C

Explanation: A healthcare clearinghouse is an entity that processes nonstandard health information it receives from another entity. A health plan is an entity that provides payment for medical services. A person or organization that provides patient or medical services is considered a healthcare provider. A business associate is a person or entity that creates, receives, maintains, transmits, accesses, or has the potential to access ePHI.

**Item number 154**

Chapter 14: Regulatory Compliance for the Healthcare Sector

Section: How Is the HIPAA Security Rule Organized?

Item type: Multiple Choice

Question: Which of the following best describes HIPAA administrative safeguards?

Options:

1. Retention, availability, and update requirements related to supporting documentation
2. The use of technical security measures to protect ePHI data
3. Standards for business associate contracts and other arrangement
4. Documented policies and procedures for managing day-to-day operations and access to ePHI

Answer: D

Explanation: Administrative safeguards include documented policies and procedures for managing day-to-day operations and access to ePHI. Organizational requirements include standards for business associate contracts and other arrangements. Documentation requirements include retention, availability, and update requirements related to supporting documentation. Technical safeguards address the use of technical security measures to protect ePHI data.

**Item number 155**

Chapter 14: Regulatory Compliance for the Healthcare Sector

Section: What Are Technical Safeguards?

Item type: Multiple Choice

Question: Which of the following is the goal of an audit controls standard?

Options:

1. Implementing technical controls that protect ePHI from improper alteration or destruction
2. Restrict access to ePHI only to users and processes that have been specifically authorized
3. Implementing of hardware, software, and mechanisms that record and examine activity in information systems that contain ePHI
4. Verification that a person or process seeking to access ePHI is the one claimed

Answer: C

Explanation: The goal of the access control standard is to restrict access to ePHI only to users and processes that have been specifically authorized. The goal of the integrity controls standard is to implement technical controls that protect ePHI from improper alteration or destruction. The goal of the audit controls standard is to implement hardware, software, and mechanisms that record and examine activity in information systems that contain ePHI. The goal of a person or entity authentication standard is to verify that a person or process seeking to access ePHI is the one claimed.

**Item number 156**

Chapter 14: Regulatory Compliance for the Healthcare Sector

Section: What Are Technical Safeguards?

Item type: Multiple Choice

Question: Which of the following is the goal of integrity control standard?

Options:

1. Implementing technical controls that protect ePHI from improper alteration or destruction
2. Restrict access to ePHI only to users and processes that have been specifically authorized
3. Implementing of hardware, software, and mechanisms that record and examine activity in information systems that contain ePHI
4. Verification that a person or process seeking to access ePHI is the one claimed

Answer: A

Explanation: The goal of the access control standard is to restrict access to ePHI only to users and processes that have been specifically authorized. The goal of the integrity controls standard is to implement technical controls that protect ePHI from improper alteration or destruction. The goal of the audit controls standard is to implement hardware, software, and mechanisms that record and examine activity in information systems that contain ePHI. The goal of a person or entity authentication standard is to verify that a person or process seeking to access ePHI is the one claimed.

**Item number 157**

Chapter 14: Regulatory Compliance for the Healthcare Sector

Section: Breach Notification Requirements

Item type: Multiple Choice

Question: Which of the following statements best describes the HIPAA breach notification rules?

Options:

1. Covered entities are required to notify individuals for any ePHI breach within 60 days after the discovery of the breach.
2. Covered entities are required to notify individuals for breach of unsecured ePHI within 60 days after the discovery of the breach.
3. Covered entities are required to notify individuals for any ePHI breach within 30 days after the discovery of the breach.
4. Covered entities are required to notify individuals for breach of unsecured ePHI within 30 days after the discovery of the breach.

Answer: B

Explanation: Covered entities are required to notify individuals whose unsecured ePHI is breached within 60 days after the discovery of the breach.

**Item number 158**

Chapter 14: Regulatory Compliance for the Healthcare Sector

Section: Breach Notification Requirements

Item type: Multiple Choice

Question: Who should be notified of ePHI breaches?

Options:

1. Department of Justice
2. Local law enforcement
3. Department of Health and Human Services
4. State Attorney

Answer: C

Explanation: The Department of Health and Human Services (DHHS) should be notified by covered entities of all breaches.

**Item number 159**

Chapter 14: Regulatory Compliance for the Healthcare Sector

Section: What Are the Administrative Safeguards?

Item type: Multiple Choice

Question: Security awareness and training and workforce security standards are examples of which of the following?

Options:

1. Administrative safeguards
2. Physical safeguards
3. Technical safeguards
4. Organizational requirements

Answer: A

Explanation: Security Awareness and Training standards and Workforce Security standards are examples of administrative safeguards.

**Item number 160**

Chapter 14: Regulatory Compliance for the Healthcare Sector

Section: What Changed for Business Associates?

Item type: Multiple Choice

Question: Under the HITECH Act criminal violations can be brought against which of the following?

Options:

1. Covered entities
2. Employees
3. Covered entities and employees
4. Anyone who wrongly discloses ePHI

Answer: D

Explanation: Under the HITECH Act criminal violations can be brought against only covered entities and employees, but also anyone who wrongly discloses ePHI.

**Item number 161**

Chapter 14: Regulatory Compliance for the Healthcare Sector

Section: What Are Physical Safeguards?

Item type: Multiple Choice

Question: Which of the following is an example of a HIPAA physical safeguard standard?

Options:

1. Workforce security
2. Workstation use
3. Audit controls
4. Security Incident Response

Answer: B

Explanation: Workstation use is an example of a physical safeguard. Workforce security and a Security Incident Response are administrative standards; audit controls are technical safeguards.

**Item number 162**

Chapter 14: Regulatory Compliance for the Healthcare Sector

Section: What Are Administrative Safeguards?

Item type: Multiple Choice

Question: Which of the following is an example of a HIPAA administrative safeguard standard?

Options:

1. Workforce security
2. Workstation use
3. Audit controls
4. Workstation security

Answer: A

Explanation: Workforce security is an administrative standard. Workstation use and workstation security are examples of physical safeguards. Audit controls are technical safeguards.

**Item number 163**

Chapter 14: Regulatory Compliance for the Healthcare Sector

Section: What Are Technical Safeguards?

Item type: Multiple Choice

Question: Which of the following is an example of a HIPAA technical safeguard standard?

Options:

1. Workforce security
2. Workstation use
3. Audit controls
4. Workstation security

Answer: C

Explanation: An audit controls is a technical safeguard. Workforce security is an administrative standard. Workstation use and workstation security are examples of physical safeguards.

**Item number 164**

Chapter 15: PCI Compliance for Merchants

Section: Protecting Cardholder Data

Item type: Multiple Choice

Question: Which of the following is considered cardholder data?

Options:

1. Service code
2. Full magnetic stripe data
3. Security code
4. PIN

Answer: A

Explanation: Cardholder data includes the primary account number, cardholder name, expiration date, and service code. Sensitive authentication data includes full magnetic stripe data, security codes (CAV, CVC2, CVV2, and CID), and PINs or PIB blocks.

**Item number 165**

Chapter 15: PCI Compliance for Merchants

Section: Protecting Cardholder Data

Item type: Multiple Choice

Question: Which of the following is considered sensitive authentication data?

Options:

1. Full magnetic stripe data
2. Primary account number
3. Expiration date
4. Cardholder name

Answer: A

Explanation: Sensitive authentication data includes full magnetic stripe data, security codes (CAV, CVC2, CVV2, and CID), and PINs or PIB blocks. Cardholder data includes the primary account number, cardholder name, expiration date, and service code.

**Item number 166**

Chapter 15: PCI Compliance for Merchants

Section: Compliance Validation Categories

Item type: Multiple Choice

Question: PCI compliance validation is composed of four levels. Which of the following levels requires conducting an annual onsite evaluation?

Options:

1. Level 1
2. Level 2
3. Level 3
4. Level 4

Answer: A

Explanation: Level 1 merchants are required to pass an annual onsite compliance assessment. Level 2 and Level 3 merchants can complete the self-assessment questionnaire (SAQ); although submission of SAQ is not required. Level 4 merchant’s compliance requirements are determined by the merchant bank.

**Item number 167**

Chapter 15: PCI Compliance for Merchants

Section: Compliance Validation Categories

Item type: Multiple Choice

Question: Which of the following statements best describe PCI DSS compliance assessment?

Options:

1. An annual onsite evaluation of compliance with PCI DSS
2. A self-assessment questionnaire
3. A compliance requirement conducted by the merchant bank
4. A compliance report submitted by the internal security assessor

Answer: A

Explanation: PCI DSS compliance assessment is an annual onsite evaluation of compliance conducted by a qualified security advisor or an internal security advisor.

**Item number 168**

Chapter 15: PCI Compliance for Merchants

Section: Build and Maintain a Secure Network and Systems

Item type: Multiple Choice

Question: Which of the following requirements is part of the Build and maintain a secure network and systems PCI DSS core principle?

Options:

1. Do not use vendor-supplied defaults for system passwords and security parameters.
2. Protect stored card data.
3. Restrict physical access to cardholder data.
4. Track and monitor all access to network resources and cardholder data.

Answer: A

Explanation: The Build and maintain a secure network and systems core principle consists of the following two requirements: Install and maintain a firewall configuration to protect a cardholder data, and do not use vendor-supplied defaults for system passwords and security parameters.

**Item number 169**

Chapter 15: PCI Compliance for Merchants

Section: Protect Cardholder Data

Item type: Multiple Choice

Question: Which of the following requirements is part of the protect cardholder data PCI DSS core principle?

Options:

1. Maintain a policy that addresses information security for all personnel.
2. Develop and maintain secure systems and applications.
3. Restrict physical access to cardholder data.
4. Protect stored card data.

Answer: D

Explanation: The protect cardholder data core principle consists of the following two requirements: Protect stored card data, and encrypt transmission of cardholder data across open, public networks.

**Item number 170**

Chapter 15: PCI Compliance for Merchants

Section: Maintain a Vulnerability Management Program

Item type: Multiple Choice

Question: Which of the following requirements is part of the maintain a vulnerability management program PCI DSS core principle?

Options:

1. Install and maintain firewall configuration to protect cardholder data.
2. Develop and maintain secure systems and applications.
3. Protect all systems against malware and regularly update antivirus software.
4. Encrypt transmission of cardholder data across open, public networks.

Answer: C

Explanation: The maintain a vulnerability management program PCI DSS core principle consists of the following two requirements: Protect all systems against malware and regularly update antivirus software, and develop and maintain secure systems and architecture.

**Item number 171**

Chapter 15: PCI Compliance for Merchants

Section: Protecting Cardholder Data

Item type: Multiple Choice

Question: Which of the following is not an example of cardholder data?

Options:

1. Primary account number
2. PIN number
3. Service code
4. Expiration date

Answer: B

Explanation: Cardholder data includes the primary account number, cardholder name, expiration date, and service code. Sensitive authentication data includes full magnetic stripe data, security codes (CAV, CVC2, CVV2, and CID), and PINs or PIB blocks.

**Item number 172**

Chapter 15: PCI Compliance for Merchants

Section: Protecting Cardholder Data

Item type: Multiple Choice

Question: Which of the following is not considered sensitive authentication data?

Options:

1. Full magnetic stripe data
2. CAV2 code
3. Expiration date
4. CVC2 code

Answer: C

Explanation: Sensitive authentication data includes full magnetic stripe data, security codes (CAV, CVC2, CVV2, and CID), and PINs or PIB blocks. Cardholder data includes the primary account number, cardholder name, expiration date, and service code.

**Item number 173**

Chapter 15: PCI Compliance for Merchants

Section: Implement Strong Access Control Measures

Item type: Multiple Choice

Which of the following requirements is part of the implement strong access control measures PCI DSS core principle?

Options:

1. Restrict access to cardholder data by business need-to know.
2. Develop and maintain secure systems and applications.
3. Protect all systems against malware and regularly update antivirus software.
4. Encrypt transmission of cardholder data across open, public networks.

Answer: A

Explanation: The implement strong access control measures PCI DSS core principle consists of the following three requirements: Restrict access to cardholder data by business need-to know; identify and authenticate access to system components; and restrict physical access to cardholder data.

**Item number 174**

Chapter 14: Regulatory Compliance for Healthcare Sector

Section: The HITECH Act and Omnibus Rule

Item type: Multiple Choice

Question: Which of the following is a change made to HIPAA by the Omnibus Rule?

Options:

1. Expanded the definition of “business associate”
2. Increased penalties for violations to up to $1.5 million
3. Granting authority to State Attorney Generals to enforce HIPAA rules and pursue criminal and civil cases
4. All the above

Answer: D

Explanation: The Omnibus Rule made significant changes in coverage, enforcement, and payment protection by redefining “business associate,” increasing penalties, and allowing for greater enforcement and prosecution of criminal cases.

**Item number 175**

Chapter 14: Regulatory Compliance for Healthcare Sector

Section: Access Control

Item type: Multiple Choice

Question: Which of the following are the two required implementation specifications of the access control standard under HIPAA?

Options:

1. User identification and establishing emergency access procedures
2. Implementing automatic logoff procedures and encrypting/decrypting information at rest
3. User identification and implementing automatic logoff procedures
4. Encrypting/decrypting information at rest and establishing emergency access procedures

Answer: A

Explanation: The access control standard has two required and two addressable implementation specifications. User identification and establishing emergency access procedures are required, and implementing automatic logoff procedures and encrypting/decrypting information at rest are addressable.

**Item number 176**

Chapter 13: Regulatory Compliance for Financial Institutions

Section: The Gramm-Leach-Bliley Act (GLBA)

Item type: Multiple Choice

Question: Which of the following is not considered NPPI?

Options:

1. Social Security number
2. Customer address
3. Credit card account number
4. Credit history

Answer: B

Explanation: Customer address by itself is not considered NPPI unless it is linked to sensitive information such as credit card numbers and Social Security numbers.

**Item number 177**

Chapter 13: Regulatory Compliance for Financial Institutions

Section: What are the Interagency Guidelines?

Item type: Multiple Choice

Question: According to the Interagency Guidelines, who must approve the bank’s written information security program?

Options:

1. chief executive officer
2. chief security officer
3. Board of Directors
4. information owner

Answer: C

Explanation: According to the Interagency Guidelines, the Board of Directors is ultimately responsible for approving the bank’s written information security program and assigning specific responsibilities for its implementation.

**Item number 178**

Chapter 12: Business Continuity Management

Section: Emergency Preparedness

Item type: Multiple Choice

Question: Which of the following is an example of willful damage?

Options:

1. Cybercrime
2. User operator error
3. Hazardous chemical exposure
4. Public health emergency

Answer: A

Explanation: Cybercrime is an example of willful damage. User operator error and hazardous chemical exposure are examples of accidents, and public health emergency is an example of an environmental event.

**Item number 179**

Chapter 12: Business Continuity Management

Section: The Business Continuity Plan

Item type: Multiple Choice

Question: Which of the following business continuity plans guides the organization back to normalcy?

Options:

1. Response plans
2. Contingency plans
3. Recovery plans
4. Resumption plans

Answer: D

Explanation: Resumption plans guide the organization back to normalcy. Contingency plans focus on immediate, near-term, and short-term alternative workforce and business processes. Response plans focus on initial response and include elements such as plan activation, evacuation procedures, notification procedures, communication, and security. Recovery plans focus on recovery of information systems and facilities.

**Item number 180**

Chapter 12: Business Continuity Management

Section: Disaster Response Plans

Item type: Multiple Choice

Question: Which of the following describes evacuations and shelter-in-place procedures for a threat or incident?

Options:

1. Occupant emergency plan (OEP)
2. Business continuity threat assessment
3. Business continuity risk assessment
4. Continuity of operation plan (COOP)

Answer: A

Explanation: The occupant emergency plan (OEP) describes evacuation and shelter-in-place procedures in case of an emergency, incident, or threat. It is maintained by the Human Resource department and is separate from the business continuity plan.

**Item number 181**

Chapter 11: Information Security Incident Management

Section: What Is an Incident?

Item type: Multiple Choice

Question: Which of the following is an example of an intentional unauthorized access or use?

Options:

1. Clicking a link in an e-mail that happens to contain malware
2. Installing a keylogger on a system in an attempt to collect usernames and passwords
3. Flooding a system with ping requests in an attempt to take it down
4. View medical records to satisfy one’s curiosity

Answer: B

Explanation: Installing a keylogger to collect usernames and passwords is an example of an unauthorized access or use. Flooding a system with ping requests is an example of a denial-of-service attack. Viewing medical records for curiosity is an example of inappropriate use.

**Item number 182**

Chapter 11: Information Security Incident Management

Section: What Is an Incident?

Item type: Multiple Choice

Question: Which of the following is an example of a denial-of-service attack?

Options:

1. Clicking a link in an e-mail that happens to contain malware
2. Installing a keylogger on a system in an attempt to collect usernames and passwords
3. Flooding a system with ping requests in an attempt to take it down
4. View medical records to satisfy one’s curiosity

Answer: C

Explanation: Flooding a system with ping requests is an example of a denial-of-service attack. Installing a keylogger to collect usernames and passwords is an example of an unauthorized access or use. Viewing medical records for curiosity is an example of inappropriate use.

**Item number 183**

Chapter 11: Information Security Incident Management

Section: What Is an Incident Response Program?

Item type: Multiple Choice

Question: Which of the following best describes the activities within the detection and investigation portion of the incident response plan?

Options:

1. Incident declaration, internal notification, and activation of an incident response team
2. Steps taken to prevent the incident from spreading
3. Establishing processes and a knowledge base to accurately detect and assess precursors and indicators
4. Elimination of components of the incident

Answer: C

Explanation: The detection and investigation portion of the incident response plan includes establishing processes and a knowledge base to accurately detect and assess precursors and indicators. Incident declaration, internal notification, and activation of an incident response team is part of an initial response. Containment includes the steps taken to prevent the incident from spreading. Eradication and recovery includes the elimination of components of the incident.

**Item number 184**

Chapter 11: Information Security Incident Management

Section: What Is an Incident Response Program?

Item type: Multiple Choice

Question: Which of the following are activities conducted during the initial response portion of the incident response plan?

Options:

1. Incident declaration, internal notification, and activation of an incident response team
2. Steps taken to prevent the incident from spreading
3. Establishing processes and a knowledge base to accurately detect and assess precursors and indicators
4. Elimination of components of the incident

Answer: A

Explanation: Incident declaration, internal notification, and activation of an incident response team is part of initial response. Detection and investigation portion of the incident response plan includes establishing processes and a knowledge base to accurately detect and assess precursors and indicators. Containment includes the steps taken to prevent the incident from spreading. Eradication and recovery includes the elimination of components of the incident.

**Item number 185**

Chapter 11: Information Security Incident Management

Section: Understanding Forensic Analysis

Item type: Multiple Choice

Question: Which of the following are the steps in a digital forensic analysis according to NIST SP 800-87?

Options:

1. Collection, acquisition, security, reporting
2. Collection, examination, analysis, reporting
3. Collection, security, analysis, reporting
4. Collection, analysis, reporting, testifying

Answer: B

Explanation: According NIST Special Publication 800-87, the four steps for performing digital forensic analysis include collection, examination, analysis, and reporting.

**Item number 186**

Chapter 10: Information Systems Acquisition, Development, and Maintenance

Section: Cryptography

Item type: Multiple Choice

Question: Which of the following is the process of creating a numeric value that represents the original text?

Options:

1. Encryption
2. Decryption
3. Hashing
4. Key management

Answer: C

Explanation: Hashing is the process of creating a numeric value that represents the original text. Encryption is the process of converting a plan text to cipher text. Decryption is the process of converting cipher text to plain text. Key management is the process of protecting the encryption keys.

**Item number 187**

Chapter 10: Information Systems Acquisition, Development, and Maintenance

Section: Cryptography

Item type: Multiple Choice

Question: Which of the following provides confidentiality?

Options:

1. Encryption
2. Decryption
3. Hashing
4. Key management

Answer: A

Explanation: Encryption is the process of converting a plan text to cipher text and can provide confidentiality. Hashing is the process of creating a numeric value that represents the original text and can provide integrity. Decryption is the process of converting cipher text to plain text. Key management is the process of protecting the encryption keys.

**Item number 188**

Chapter 10: Information Systems Acquisition, Development, and Maintenance

Section: Asymmetric Keys

Item type: Multiple Choice

Question: Public key cryptography uses which of the following?

Options:

1. A shared key
2. A public key
3. A private key
4. Both a public and a private key

Answer: D

Explanation: Public key cryptography, also called asymmetric key cryptography, uses two keys: a public key and a private key.

**Item number 189**

Chapter 9: Access Control Management

Section: Intrusion Detection Systems and Intrusion Protection Systems

Item type: Multiple Choice

Question: Which of the following examines network traffic to identify threats that generate unusual traffic flow?

Options:

1. Wireless IDS
2. Network-based IDS
3. Host-based IDS
4. Network behavior analysis IDS

Answer: D

Explanation: Network behavior analysis IDSs examine network traffic to identify threats that generate unusual traffic flow. Host-based IDSs monitor a single system. Wireless IDSs monitor wireless traffic. Network-based IDSs monitor network traffic.

**Item number 190**

Chapter 9: Access Control Management

Section: Intrusion Detection Systems and Intrusion Protection Systems

Item type: Multiple Choice

Question: Which of the following is the most dangerous and unwanted IDS decision state?

Options:

1. False positive
2. False negative
3. True positive
4. True negative

Answer: B

Explanation: False negative is the most dangerous and unwanted response because it means that the IDS system did not detect a security issue but instead considered it a normal activity.

**Item number 191**

Chapter 9: Access Control Management

Section: Intrusion Detection Systems and Intrusion Protection Systems

Item type: Multiple Choice

Question: Which of the following is the most wanted IDS decision state?

Options:

1. False positive
2. False negative
3. True positive
4. True negative

Answer: C

Explanation: A true positive is the most wanted decision state because it correctly identifies an issue as such.

**Item number 192**

Chapter 9: Access Control Management

Section: Remote Access Technologies

Item type: Multiple Choice

Question: Which of the following provides a secure tunnel for transmitting data through an insecure network such as the Internet?

Options:

1. Remote access portal
2. Virtual private network
3. Network access control system
4. DMZ

Answer: B

Explanation: A virtual private network provides a secure tunnel for transmitting data through an insecure network such as the Internet. A remote access portal provides access to one or more applications through a single centralized interface. Network access control systems can check if a remote access device meets predefined criteria.

**Item number 193**

Chapter 9: Access Control Management

Section: Remote Access Technologies

Item type: Multiple Choice

Question: Which of the following provides access to one or more applications through a single centralized interface?

Options:

1. Remote access portal
2. Virtual private network
3. Network access control system
4. DMZ

Answer: A

Explanation: A remote access portal provides access to one or more applications through a single centralized interface. A virtual private network provides a secure tunnel for transmitting data through an insecure network such as the Internet. Network access control systems can be used to check if remote access device meets predefined criteria.

**Item number 194**

Chapter 9: Access Control Management

Section: Administrative Account Controls

Item type: Multiple Choice

Question: Which of the following statement best describes segregation of duties?

Options:

1. Two individuals must both complete their half of a specific task.
2. No one individual can control a process from start to finish.
3. Two individuals complete the same task simultaneously.
4. Two individuals complete different tasks at the same time.

Answer: B

Explanation: Segregation of duties requires that no one individual can control a process from start to finish, and dual control requires that two individuals must both complete their half of a specific task.

**Item number 195**

Chapter 9: Access Control Management

Section: Administrative Account Controls

Item type: Multiple Choice

Question: Which of the following statement best describes dual control?

Options:

1. Two individuals must both complete their half of a specific task.
2. No one individual can control a process from start to finish.
3. Two individuals complete the same task simultaneously.
4. Two individuals complete different tasks at the same time.

Answer: A

Explanation: Dual control requires that two individuals must both complete their half of a specific task. Segregation of duties requires that no one individual can control a process from start to finish.

**Item number 196**

Chapter 9: Access Control Management

Section: How Is Identity Verified?

Item type: Multiple Choice

Question: Which of the following is an example of a multifactor authentication?

Options:

1. A password and a PIN
2. A cognitive password and a PIN
3. A fingerprint scan and a retina scan
4. A smart card and a retina scan

Answer: D

Explanation: A multifactor authentication involves using two or more factors.

**Item number 197**

Chapter 9: Access Control Management

Section: How Is Identity Verified?

Item type: Multiple Choice

Question: Which of the following is an example of a multilayer authentication?

Options:

1. A fingerprint scan and a smart card
2. A retina scan and a password
3. A retina scan and a fingerprint scan
4. A password and a smart card

Answer: C

Explanation: A multilayer authentication involves using two or more of the same type of factors.

**Item number 198**

Chapter 9: Access Control Management

Section: Knowledge: Something You Know

Item type: Multiple Choice

Question: A cognitive password is an example of which of the following?

Options:

1. Something you know knowledge-based authentication
2. Something you have authentication
3. Something you are authentication
4. Something you want authentication

Answer: A

Explanation: Passwords, PINs, and cognitive passwords are example of something you know authentication.

**Item number 199**

Chapter 8: Communications and Operations Security

Section: Secure Messaging

Item type: Multiple Choice

Question: Which of the following is the standard protocol for sending e-mail messages?

Options:

1. IPsec
2. SSL
3. SMTP
4. FTP

Answer: C

Explanation: SMPT (Simple Mail Transfer Protocol) is the standard protocol for sending e-mail messages.

**Item number 200**

Chapter 9: Access Control Management

Section: Inherence: Something You Are

Item type: Multiple Choice

Question: Using a fingerprint scan for authentication is an example of which of the following?

Options:

1. Something you know authentication
2. Something you have authentication
3. Something you are authentication
4. Something you want authentication

Answer: C

Explanation: Fingerprint scans are examples of an inherence: something you are authentication.