**Item number 1**

Chapter 1: Understanding Policy

Section: Successful Policy Characteristics

Item type: Multiple Choice

Question: Which of the following elements ensures a policy is enforceable?

Options:

1. Compliance can be measured.
2. Appropriate sanctions are applied when the policy is violated.
3. Appropriate administrative, technical, and physical controls are put in place to support the policy.
4. All the above.

Answer: D

Explanation: Enforceable means that the policy is statutory and the mechanisms for policy enforcement are in place. Policy compliance can be measured and any violations to the policy are treated according to the policy regulations.

**Item number 2**

Chapter 1: Understanding Policy

Section: The Role of Government

Item type: Multiple Choice

Question: FERPA protects which of the following?

Options:

1. Medical records
2. Financial records
3. Personally identifiable information
4. Educational records

Answer: D

Explanation: FERPA protects educational records. GBLA protects customer financial information, and HIPAA deals with patients’ medical records. Some states have legislation that protects personally identifiable information.

**Item number 3**

Chapter 1: Understanding Policy

Section: Information Security Policy

Item type: Multiple Choice

Question: Which of the following is an example of an information asset?

Options:

1. Business plans
2. Employee records
3. Company reputation
4. All the above

Answer: D

Explanation: An information asset is information that an organization uses to conduct business. Examples of information assets include employee information, company information, customers’ information, brand, reputation, and financial documents.

**Item number 4**

Chapter 1: Understanding Policy

Section: Information Security Policy Lifecycle

Item type: Multiple Choice

Question: Policy implementation and enforcement are part of which of the following phases of the policy lifecycle?

Options:

1. Develop
2. Publish
3. Adopt
4. Review

Answer: C

Explanation: The three steps of the policy adoption phase are implement, monitor, and enforce.

**Item number 5**

Chapter 1: Understanding Policy

Section: Information Security Policy Lifecycle

Item type: Multiple Choice

Question: Which of the following is the correct order of the policy lifecycle?

Options:

1. Publish, develop, review, adopt
2. Review, develop, adopt, publish
3. Develop, publish, adopt, review
4. Review, adopt, develop, publish

Answer: C

Explanation: The policy lifecycle starts with policy development, continues with publishing the policy, followed by policy adoption, and ends with policy review.

**Item number 6**

Chapter 1: Understanding Policy

Section: Successful Policy Characteristics

Item type: Multiple Choice

Question: Endorsed is one of the seven policy characteristics. Which of the following statements best describes endorsed?

Options:

1. The policy is supported by management.
2. The policy is accepted by the organization’s employees.
3. The policy is mandatory; compliance is measured; and appropriate sanctions are applied.
4. The policy is regulated by the government.

Answer: A

Explanation: Endorsed means that the policy is supported and championed by management.

**Item number 7**

Chapter 1: Understanding Policy

Section: Policy Review

Item type: Multiple Choice

Question: Which of the following is the outcome of policy review?

Options:

1. Retirement
2. Renewal
3. Reauthorization
4. Both A and B
5. Both A and C
6. Both B and C

Answer: E

Explanation: The outcome of a policy review is either policy retirement or policy reauthorization.

**Item number 8**

Chapter 1: Understanding Policy

Section: Policy Review

Item type: Multiple Choice

Question: How often should policies be reviewed?

Options:

1. Monthly
2. Twice a year
3. Annually
4. Never

Answer: C

Explanation: Policies should be reviewed annually and either retired or reauthorized.

**Item number 9**

Chapter 1: Understanding Policy

Section: Policy Today

Item type: Multiple Choice

Question: Which of the following statements is not true?

Options:

1. Policies should require only what is possible.
2. Policies that are no longer applicable should be retired.
3. All guiding principles and corporate cultures are good.
4. Guiding principles set the tone for a corporate culture.

Answer: C

Explanation: Not all guiding principles and corporate cultures are good. The remaining statements are all true.

**Item number 10**

Chapter 1: Understanding Policy

Section: Information Security Policy Lifecycle

Item type: Multiple Choice

Question: Which of the following is not one of the tasks of the policy development phase?

Options:

1. Approve
2. Write
3. Communicate
4. Authorize

Answer: C

Explanation: To communicate is the first task of the policy publication phase. To approve, write, and authorize are tasks within the policy development phase.

**Item number 11**

Chapter 2: Policy Elements and Style

Section: Policy Hierarchy

Item type: Multiple Choice

Question: Which of the following is not an example of a standard?

Options:

1. Passwords must include at least one special character.
2. Passwords must not include repeating characters.
3. Pass phrases make good passwords.
4. Passwords must not include the user’s name.

Answer: C

Explanation: Pass phrases make good passwords is an example of a guideline, not a standard. The other options are all examples of standards.

**Item number 12**

Chapter 2: Policy Elements and Style

Section: Version Control

Item type: Multiple Choice

Question: Which of the following is an example of a major policy revision?

Options:

1. 3.5
2. 4.0
3. 4.1
4. 5.1

Answer: B

Explanation: Major policy revisions generally advance to the next digit, whereas minor revisions advance as a subsection.

**Item number 13**

Chapter 2: Policy Elements and Style

Section: Version Control

Item type: Multiple Choice

Question: Which of the following would indicate a minor revision?

Options:

1. IV
2. 2.0
3. 2.1
4. 3.0

Answer: C

Explanation: Minor revisions advance as a subsection, whereas major revisions advance to the next digit or letter.

**Item number 14**

Chapter 2: Policy Elements and Style

Section: Introduction

Item type: Multiple Choice

Question: Where is the policy introduction located in a consolidated policy document?

Options:

1. In a separate document
2. Before the version control table
3. After the version control table
4. At the beginning of the document

Answer: C

Explanation: In a consolidated policy document, the introduction follows the version control table. Singular policy introduction is in a separate document.

**Item number 15**

Chapter 2: Policy Elements and Style

Section: Administrative Notations

Item type: Multiple Choice

Question: What is the purpose of the administrative notation section of a policy?

Options:

1. To explain terms, abbreviations, and acronyms used in the policy
2. To refer the reader to additional information
3. To provide the policy version number
4. To provide information about policy exceptions

Answer: B

Explanation: The policy administrative section refers readers to additional information and references them to internal resources such as standards, guidelines, and procedures.

**Item number 16**

Chapter 2: Policy Elements and Style

Section: Policy Definitions

Item type: Multiple Choice

Question: What is the purpose of the policy definition section?

Options:

1. To explain terms, abbreviations, and acronyms used in the policy
2. To refer the reader to additional information
3. To provide the policy version number
4. To provide information about policy exceptions

Answer: A

Explanation: The policy definition section contains a glossary of terms, abbreviations, and acronyms used in the policy documents.

**Item number 17**

Chapter 2: Policy Elements and Style

Section: Policy Hierarchy

Item type: Multiple Choice

Question: Which of the following statement about standards and guidelines is true?

Options:

1. Standards are mandatory, whereas guidelines are not.
2. Guidelines are mandatory, whereas standards are not.
3. Both standards and guidelines are mandatory.
4. Neither standards nor guidelines are mandatory.

Answer: A

Explanation: Standards are mandatory, whereas guidelines are suggestions that can help users conform to a standard and are not mandatory.

**Item number 18**

Chapter 2: Policy Elements and Style

Section: Procedures

Item type: Multiple Choice

Question: Which of the following procedure formats is best suited when there is a decision-making process associated with a task?

Options:

1. Simple step
2. Flowchart
3. Hierarchical
4. Graphic

Answer: B

Explanation: The flowchart procedure format is best suited when there is a decision-making process associated with the task.

**Item number 19**

Chapter 2: Policy Elements and Style

Section: Baselines

Item type: Multiple Choice

Question: Which of the following best describes a baseline?

Options:

1. Specifications for implementation of a policy
2. Instructions on how a policy is carried out
3. Aggregate of implementation standards and security controls
4. Teaching tools that help people conform to a policy

Answer: C

Explanation: A baseline is an aggregate of implementation standards and security controls for a specific category such as mobile device users. Standards are specifications for policy implementation. Procedures are instructions on how a policy is carried out, and guidelines are teaching tools that help users conform to a policy or standard.

**Item number 20**

Chapter 2: Policy Elements and Style

Section: Procedures

Item type: Multiple Choice

Question: Which of the following best describes a procedure?

Options:

1. Specifications for implementation of a policy
2. Instructions on how a policy is carried out
3. Aggregate of implementation standards and security controls
4. Teaching tools that help people conform to a policy

Answer: B

Explanation: Procedures are instructions on how a policy is carried out. A baseline is an aggregate of implementation standards and security controls for a specific category such as mobile device users. Standards are specifications for policy implementation, and guidelines are teaching tools that help users conform to a policy or standard.

**Item number 21**

Chapter 2: Policy Elements and Style

Section: Policy Hierarchy

Item type: Multiple Choice

Question: Which of the following statements about policies and standards is true?

Options:

1. Policies are mandatory, whereas standards are not.
2. Standards are mandatory, whereas policies are not.
3. Both polices and standards are mandatory.
4. Neither policies nor standards are mandatory.

Answer: C

Explanation: Both policies and standards are mandatory. Policies are mandatory statements that present the management’s positions, and standards define actions.

**Item number 22**

Chapter 2: Policy Elements and Style

Section: Policy Hierarchy

Item type: Multiple Choice

Question: Which of the following is the topmost object in the policy hierarchy?

Options:

1. Standards
2. Baselines
3. Guidelines
4. Guiding principles

Answer: D

Explanation: Guiding principles are the topmost object in the policy hierarchy, and policies reflect the guiding principles.

**Item number 23**

Chapter 2: Policy Elements and Style

Section: Plain Language Techniques for Policy Writing

Item type: Multiple Choice

Question: Which of the following is one of the ten plain language techniques for policy writing?

Options:

1. Use passive voice.
2. Use “shall” to indicate requirements.
3. Use long sentences.
4. Limit a paragraph to one subject.

Answer: D

Explanation: Limiting a paragraph to one subject is one of the ten guidelines for policy writing. Other guidelines include using active voice, short sentences, and “must” instead of “shall.”

**Item number 24**

Chapter 2: Policy Elements and Style

Section: Plain Language Techniques for Policy Writing

Item type: Multiple Choice

Question: Which of the following is not one of the plain language techniques for policy writing?

Options:

1. Use active voice.
2. Write short sentences.
3. Use ‘shall’ instead of “must”.
4. Avoid double negatives.

Answer: C

Explanation: According to the ten guidelines, policy writers should use “must” instead of “shall” to indicate requirements.

**Item number 25**

Chapter 2: Policy Elements and Style

Section: Policy Components

Item type: Multiple Choice

Question: What is the purpose of the policy exceptions section?

Options:

1. To define sanctions for violations
2. To convey intent
3. To define exclusions
4. To specify mandatory directives

Answer: C

Explanation: The policy exclusions section defines the policy exclusions. The policy enforcement clause is used to define sanctions for violation. The policy goals and objectives are used to convey intent, and the policy statement specifies mandatory policy directives.

**Item number 26**

Chapter 3: Information Security Framework

Section: What Does the ISO Do?

Item type: Multiple Choice

Question: Which of the following is a network of the national standards institutes of 146 countries?

Options:

1. ISO
2. NIST
3. FIPS
4. IEC

Answer: A

Explanation: ISO is a nongovernment organization of the national standards institutes of 146 countries.

**Item number 27**

Chapter 3: Information Security Framework

Section: Information Security Framework

Item type: Multiple Choice

Question: Which of the following is the official publication series for standards and guidelines adopted under the FIMSA Act?

Options:

1. ITL bulletins
2. FIPS
3. Special Publication 800 series
4. NIST interagency reports

Answer: B

Explanation: FIPS (Federal Information Processing Standards) is the NIST official publication series for standards and guidelines. The SP 800 series report on ITL research, guidelines, and outreach effort. The ITL bulletins discuss a single topic in each issue.

**Item number 28**

Chapter 3: Information Security Framework

Section: In Practice: The “Five A’s” of Information Security

Item type: Multiple Choice

Question: Which of the following traces actions to their source?

Options:

1. Accountability
2. Accounting
3. Assurance
4. Authentication

Answer: A

Explanation: Accountability is the process of tracing actions to their source. Assurance is defined as the processes, policies, and controls used to develop confidence that security measures are working as intended. Authentication is the positive identification of the person or system seeking access to resources, and the logging of access and usage of information resources is accounting.

**Item number 29**

Chapter 3: Information Security Framework

Section: In Practice: The “Five A’s” of Information Security

Item type: Multiple Choice

Question: Which of the following grants users and systems a predetermined level of access?

Options:

1. Accountability
2. Authentication
3. Authorization
4. Assurance

Answer: C

Explanation: Authorization involves granting user and systems a predetermined level of access to information and resources. Accountability is the process of tracing actions to their source. Assurance is defined as the processes, policies, and controls used to develop confidence that security measures are working as intended. Authentication is the positive identification of the person or system seeking access to resources.

**Item number 30**

Chapter 3: Information Security Framework

Section: What is Integrity?

Item type: Multiple Choice

Question: Which of the following is a behavioral control that can be used to safeguard against the loss of integrity?

Options:

1. Rotation of duties
2. Log analysis
3. Code testing
4. Digital signatures

Answer: A

Explanation: Rotation of duties is an example of a behavioral control. Log analysis is a monitoring control, code testing is a process control, and digital signatures are an example of an access control.

**Item number 31**

Chapter 3: Information Security Framework

Section: What is Integrity?

Item type: Multiple Choice

Question: Which of the following is a monitoring control that safeguard against loss of integrity?

Options:

1. File integrity monitoring
2. Separation of duties
3. Encryption
4. Digital signatures

Answer: A

Explanation: File integrity monitoring is a monitoring control that can safeguard the integrity of information. Separation of duties is a behavioral control, and encryption and signatures are access controls.

**Item number 32**

Chapter 3: Information Security Framework

Section: CIA

Item type: Multiple Choice

Question: Which of the following are the three elements of the CIA triad?

Options:

1. Authentication, integrity, confidentiality
2. Availability, integrity, confidentiality
3. Access, integrity, confidentiality
4. Authorization, integrity, confidentiality

Answer: B

Explanation: The three elements of the security triad are availability, integrity, and confidentiality.

**Item number 33**

Chapter 3: Information Security Framework

Section: What is Availability?

Item type: Multiple Choice

Question: What is the computer used in a DDoS attack known as?

Options:

1. Botnet
2. Bot
3. Victim
4. Handler

Answer: B

Explanation: A computer used in a DDoS attach is known as a bot; the compromised computers are known as botnet.

**Item number 34**

Chapter 4: Governance and Risk Management

Section: What Is Meant by Strategic Alignment?

Item type: Multiple Choice

Question: Which of the following is a characteristic of the parallel approach to information security?

Options:

1. Compliance is discretionary.
2. Security is the responsibility of the IT department.
3. Little or no organizational accountability exists.
4. All the above.

Answer: D

Explanation: The parallel approach to information security views the security as a responsibility of the IT department, with no organizational accountability, and no requirements for compliance.

**Item number 35**

Chapter 4: Governance and Risk Management

Section: What is Risk Assessment?

Item type: Multiple Choice

Question: Which of the following is the objective of risk assessment?

Options:

1. Identify the inherent risk.
2. Determine the impact of a threat.
3. Calculate the likelihood of a threat occurrence.
4. All the above.

Answer: D

Explanation: The objective of a risk assessment is to identify any potential threats and the inherent risk based on these threats, followed by determining what impact the threat would have if successful and calculating how likely the threat is to occur.

**Item number 36**

Chapter 4: Governance and Risk Management

Section: Capability Maturity Model (CMM)

Item type: Multiple Choice

Question: At which of the following state of the CMM scale no documented policies and processes exist but the organization is aware they are needed?

Options:

1. Ad-hoc
2. Defined process
3. Optimized
4. Nonexistent

Answer: A

Explanation: At the ad-hoc state there are no documented policies and processes. At the nonexistent state the organization is not aware that it needs policies and processes.

**Item number 37**

Chapter 4: Governance and Risk Management

Section: What Is Risk Assessment?

Item type: Multiple Choice

Question: Which of the following best describes residual risk?

Options:

1. The likelihood of occurrence of a threat
2. The level of risk before security measures are applied
3. The level of risk after security measures are applied
4. The impact of risk if a threat is realized

Answer: C

Explanation: Residual risk is the level of risk after security measures have been applied. The level of risk before security measures are applied is the inherent risk.

**Item number 38**

Chapter 4: Governance and Risk Management

Section: What Is Risk Management?

Item type: Multiple Choice

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

Options:

1. It shifts a portion of the risk responsibility to another organization.
2. It shifts a portion of the risk liability to another organization.
3. It takes steps to eliminate or modify the risk.
4. It shifts the entire risk responsibility to another organization.

Answer: D

Explanation: Risk transfer shifts the entire risk to another organization, whereas risk sharing shifts only a portion of the risk. The goal of risk avoidance is to eliminate or modify the risk.

**Item number 39**

Chapter 4: Governance and Risk Management

Section: Risk Assessment Methodologies

Item type: Multiple Choice

Question: Which of the following risk assessment methodology was developed by CERT?

Options:

1. FAIR
2. OCTAVE
3. RMF
4. CMM

Answer: B

Explanation: OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) was developed at CERT Coordination Center at Carnegie Mellon University.

**Item number 40**

Chapter 4: Governance and Risk Management

Section: What Is Risk Assessment?

Item type: Multiple Choice

Question: Which of the following risks relates to negative public opinion?

Options:

1. Operational risk
2. Strategic risk
3. Financial risk
4. Reputational risk

Answer: D

Explanation: Reputational risk relates to negative public opinion. Operational risk relates to loss from failed or inadequate processes or systems. Financial relates to monetary loss, and strategic relates to adverse business decisions.

**Item number 41**

Chapter 4: Governance and Risk Management

Section: What Is Risk Assessment?

Item type: Multiple Choice

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

Options:

1. Risk that relates to monetary loss
2. Risk that relates to adverse business decisions
3. Risk that relates to a loss from failed or inadequate systems and processes
4. Risk that relates to violation of laws, regulations, or policy

Answer: B

Explanation: Strategic risk relates to adverse business decisions. Operational risk relates to loss from failed or inadequate processes or systems. Financial relates to monetary loss, and regulatory risk relates to violation of laws, regulations, or policy.

**Item number 42**

Chapter 4: Governance and Risk Management

Section: What Is Risk Assessment?

Item type: Multiple Choice

Question: Which of the following is the magnitude of harm?

Options:

1. Risk
2. Threat
3. Impact
4. Vulnerability

Answer: C

Explanation: Impact is the magnitude of harm. Risk is the potential of unfavorable outcome from a give action or inaction. Threat is a natural, environmental, or human event or situation that can have an unwanted effect or cause impact. Vulnerability is a weakness that could be exploited.

**Item number 43**

Chapter 3: Information Security Framework

Section: What Is NIST’s Function?

Item type: Multiple Choice

Question: Which of the following statement best describes NIST?

Options:

1. A regulatory government organization that enforces standards
2. A coalition of 146 countries that creates standards
3. A nonregulatory federal agency that develops and promotes standards
4. A nongovernment organizations that develops and promotes standards

Answer: C

Explanation: NIST is a nonregulatory government organization that develops and promotes standards.

**Item number 44**

Chapter 3: Information Security Framework

Section: In Practice: The “Five A’s” of Information Security

Item type: Multiple Choice

Question: Which of the following best describes accounting?

Options:

1. The logging of access and usage of information resources
2. The configuring of the Security log to record events
3. The process of tracing actions to their source
4. The process of identifying users who seek access to secure information

Answer: A

Explanation: Accounting is the process of logging of access and usage of information resources. Accountability is the process of tracing actions to their source.

**Item number 45**

Chapter 3: Information Security Framework

Section: In Practice: The “Five A’s” of Information Security

Item type: Multiple Choice

Question: Which of the following best describes accountability?

Options:

1. The logging of access and usage of information resources
2. The configuring of the Security log to record events
3. The process of tracing actions to their source
4. The process of identifying users who seek access to secure information

Answer: C

Explanation: Accountability is the process of tracing actions to their source. Accounting is the process of logging of access and usage of information resources.

**Item number 46**

Chapter 3: Information Security Framework

Section: In Practice: The “Five A’s” of Information Security

Item type: Multiple Choice

Question: Which of the following can achieve authentication?

Options:

1. Intrusion detection systems
2. Log files
3. Auditing
4. Tokens

Answer: D

Explanation: Tokens are a form of authentication. Intrusion detection systems and log files are used to achieve accountability, and auditing is used for assurance purposes.

**Item number 47**

Chapter 5: Asset Management

Section: Information Classification

Item type: Multiple Choice

Question: Which of the following statements best describes the Biba security model?

Options:

1. No read up and write up
2. No write up and no write down
3. No read up and no write down
4. No read down and no write up

Answer: D

Explanation: The Biba model objective is to ensure data integrity. The model works on the principle of restricting users to read data at lower than their level and to write data at higher than their security level. This model was designed in the 1970s for the U.S. military.

**Item number 48**

Chapter 5: Asset Management

Section: Information Classification

Item type: Multiple Choice

Question: Which of the following best described the Bell-Lapadula security model?

Options:

1. No read up and read down
2. No write up and no read up
3. No read up and no write down
4. No read down and no write up

Answer: C

Explanation: The Bell-Lapadula model ensures confidentiality and restricts users to read data above their level and to write data below their security level. It was developed in the 1970s for the U.S. military.

**Item number 49**

Chapter 5: Asset Management

Section: Why Is National Security Information Classified Differently?

Item type: Multiple Choice

Question: Which of the following is the heist classification level under the private sector classification system?

Options:

1. Secret
2. Protected
3. Confidential
4. Top secret

Answer: B

Explanation: The highest level under the public classification system is protected. The highest classification level for national security information is top secret.

**Item number 50**

Chapter 5: Asset Management

Section: How Does the Private Sector Classify Data?

Item type: Multiple Choice

Question: Which of the following would most likely be classified as confidential information under the private sector data classification system?

Options:

1. Social Security number
2. List of upcoming trade shows
3. Nonsensitive client or vendor information
4. Laboratory research

Answer: D

Explanation: Confidential information is data that is essential to the organization’s mission and the disclosure would cause significant damage to the organization. Some examples of confidential information include laboratory research, product designs, and employees’ records.

**Item number 51**

Chapter 5: Asset Management

Section: Why Is National Security Information Classified Differently?

Item type: Multiple Choice

Question: Which of the following is not one of the classification levels for national security information?

Options:

1. Secret
2. Protected
3. Confidential
4. Sensitive but Unclassified

Answer: B

Explanation: The classification levels for national security information are top secret, secret, confidential, unclassified, and sensitive but unclassified. Protected is one of the classification levels for private sector data classification.

**Item number 52**

Chapter 5: Asset Management

Section: How Does the Private Sector Classify Data?

Item type: Multiple Choice

Question: Which of the following is not one of the classification levels for private sector information?

Options:

1. Protected
2. Secret
3. Internal use
4. Public

Answer: B

Explanation: The classification levels for private sector information are protected, confidential, internal use, and public. Secret is one of the classification levels for national security information.

**Item number 53**

Chapter 5: Asset Management

Section: Can Information Be Reclassified or Even Declassified?

Item type: Multiple Choice

Question: Which of the following statements describes reclassification?

Options:

1. The process of changing the classification level to a lower level
2. The process of upgrading a classification
3. The process of removing a classification
4. The process of assigning a classification

Answer: B

Explanation: Reclassification is the process of upgrading a classification.

**Item number 54**

Chapter 5: Asset Management

Section: Can Information Be Reclassified or Even Declassified?

Item type: Multiple Choice

Question: Which if the following statements best describes declassification?

Options:

1. The process of downgrading a classification
2. The process of upgrading a classification
3. The process of removing a classification
4. The process of assigning a new classification

Answer: A

Explanation: Declassification is the process of downgrading a classification.

**Item number 55**

Chapter 5: Asset Management

Section: Information Systems Inventory

Item type: Multiple Choice

Question: Which of the following is a hardware identification number that uniquely identifies device?

Options:

1. IP domain name
2. MAC address
3. IPV4 address
4. IPv6 address

Answer: B

Explanation: A MAC address is a unique address assigned to the network card that identifies devices on a network. The MAC address is in a hexadecimal format.

**Item number 56**

Chapter 5: Asset Management

Section: Information Systems Inventory

Item type: Multiple Choice

Question: A MAC address is in which of the following formats?

Options:

1. Decimal
2. Binary
3. Hexadecimal
4. Unicode

Answer: C

Explanation: A MAC address is expressed as six 2-digits hexadecimal numbers.

**Item number 57**

Chapter 6: Human Resources Security

Section: What Does Recruitment Have to Do with Security?

Item type: Multiple Choice

Question: Why shouldn’t information about specific systems be included in a job description?

Options:

1. To make sure candidates know all systems
2. To protect against social engineering and other attacks
3. To get as many candidates as possible
4. To get more knowledgeable candidates

Answer: B

Explanation: Intruders can use information in job posting to collect information about a company and carry out a social engineering or other attacks.

**Item number 58**

Chapter 6: Human Resources Security

Section: What Happens in the Onboarding Phase?

Item type: Multiple Choice

Question: During what step of the employee lifecycle are employees added to the organization’s benefit system?

Options:

1. Recruitment
2. Onboarding
3. User provisioning
4. Orientation

Answer: B

Explanation: During the onboarding phase the new employee is added to the organization’s payroll and benefit systems.

**Item number 59**

Chapter 6: Human Resources Security

Section: What Is User Provisioning?

Item type: Multiple Choice

Question: Which of the following is part of the onboarding phase of the employee lifecycle?

Options:

1. The employee is added to the organization’s payroll.
2. The employee is provided with a username or smart card.
3. A background check is conducted for the employee.
4. The employee expectations of privacy are determined.

Answer: B

Explanation: During the user provisioning phase, user accounts are created and group membership established. Users are also provided with company identification at this phase.

**Item number 60**

Chapter 6: Human Resources Security

Section: Why Is Termination Considered the Most Dangerous Phase?

Item type: Multiple Choice

Question: Which of the following steps of the employee lifecycle is considered the most dangerous?

Options:

1. Onboarding
2. Recruitment
3. Termination
4. User provisioning

Answer: C

Explanation: Employee termination is considered the most dangerous phase of the employee lifecycle because in case of unfriendly termination the employee might decide to take steps to harm the company or sell sensitive information to a competitor.

**Item number 61**

Chapter 6: Human Resources Security

Section: The Importance of Security Education and Training

Item type: Multiple Choice

Question: Which of the following best describes the purpose of security awareness?

Options:

1. To teach skills that would allow a person to perform a certain function
2. To focus attention on security
3. To integrate all the security skills and competencies into a common body of knowledge
4. To involve management in the process

Answer: B

Explanation: Security awareness is not the same as security training, and its goal is to focus attention of security.

**Item number 62**

Chapter 6: Human Resources Security

Section: What Is the SETA Model?

Item type: Multiple Choice

Question: According to SETA model what is the time frame for security training?

Options:

1. Short-term
2. Long-term
3. Intermediate
4. Upon hiring

Answer: C

Explanation: According to the SETA model, the impact time frame for security training is intermediate.

**Item number 63**

Chapter 6: Human Resources Security

Section: The Importance of Security Education and Training

Item type: Multiple Choice

Question: Which of the following best describes the purpose of security training?

Options:

1. To teach skills that would allow a person to perform a certain function
2. To focus attention on security
3. To integrate all the security skills and competencies into a common body of knowledge
4. To involve management in the process

Answer: A

Explanation: The goal of security training is to teach skills that would allow a person to perform a certain task.

**Item number 64**

Chapter 6: Human Resources Security

Section: The Importance of Security Education and Training

Item type: Multiple Choice

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

Options:

1. The purpose of security awareness is to focus attention on security.
2. Awareness is training.
3. Security awareness programs are designed to remind users of appropriate behaviors.
4. A posted reminding users not to write their password down is an example of an awareness program.

Answer: B

Explanation: Security awareness is not training. The goal of awareness is to remind users of appropriate behaviors and to focus attention on security.

**Item number 65**

Chapter 6: Human Resources Security

Section: The Employee Lifecycle

Item type: Multiple Choice

Question: During what phase of the employee lifecycle user accounts are disabled?

Options:

1. Career development
2. Termination
3. User provisioning
4. Onboarding

Answer: B

Explanation: During the termination phase the employee leaves the organization and her user accounts are disabled and access permissions revoked.

**Item number 66**

Chapter 6: Human Resources Security

Section: Components of an Acceptable Use Agreement

Item type: Multiple Choice

Question: Which of the following sections of the Acceptable Use Agreement dictates how information must be stored, transmitted, and communicated?

Options:

1. Introduction
2. Data classification
3. Applicable policy statements
4. Handling standards

Answer: D

Explanation: The Handling standards section of the agreement specifies how information should be stored, transmitted, accessed, communicated, retained, and destroyed.

**Item number 67**

Chapter 6: Human Resources Security

Section: What Is the SETA Model?

Item type: Multiple Choice

Question: Which of the following regulations explicitly specifies the topics that should be covered in a security awareness training?

Options:

1. FACTA
2. HIPAA
3. FCRA
4. DPPA

Answer: B

Explanation: HIPAA Section 164.308(a)(5) requires that a security awareness program should include the following four standards: security reminders, protection from malicious software, log-in monitoring, and password management.