Chapter1

Which of the following elements ensures a policy is enforceable?

A. Compliance can be measured.
B. Appropriate sanctions are applied when the policy is violated.
C. Appropriate administrative, technical, and physical controls are put in place to support the policy.
D. All the above.

FERPA protects which of the following?

A. Medical records
B. Financial records
C. Personally identifiable information
D. Educational records

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

A. Business plans
B. Employee records
C. Company reputation
D. All the above

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

A. Develop
B. Publish
C. Adopt
D. Review

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

A. Publish, develop, review, adopt
B. Review, develop, adopt, publish
C. Develop, publish, adopt, review
D. Review, adopt, develop, publish

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

A. The policy is supported by management.
B. The policy is accepted by the organization’s employees.
C. The policy is mandatory; compliance is measured; and appropriate sanctions are applied.
D. The policy is regulated by the government.

Which of the following is the outcome of policy review?

A. Retirement
B. Renewal
C. Reauthorization
D. Both A and B
E. Both A and C
F. Both B and C

How often should policies be reviewed?

A. Monthly
B. Twice a year
C. Annually
D. Never

Which of the following statements is not true?

A. Policies should require only what is possible.
B. Policies that are no longer applicable should be retired.
C. All guiding principles and corporate cultures are good.
D. Guiding principles set the tone for a corporate culture.

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

A. Approve
B. Write
C. Communicate
D. Authorize

Chapter2

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

A. Passwords must include at least one special character.
B. Passwords must not include repeating characters.
C. Pass phrases make good passwords.
D. Passwords must not include the user’s name.

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

A. 3.5
B. 4.0
C. 4.1
D. 5.1

Which of the following would indicate a minor revision?

A. IV
B. 2.0
C. 2.1
D. 3.0

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

A. In a separate document
B. Before the version control table
C. After the version control table
D. At the beginning of the document

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

A. To explain terms, abbreviations, and acronyms used in the policy
B. To refer the reader to additional information
C. To provide the policy version number
D. To provide information about policy exceptions

What is the purpose of the policy definition section?

A. To explain terms, abbreviations, and acronyms used in the policy
B. To refer the reader to additional information
C. To provide the policy version number
D. To provide information about policy exceptions

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

A. Standards are mandatory, whereas guidelines are not.
B. Guidelines are mandatory, whereas standards are not.
C. Both standards and guidelines are mandatory.
D. Neither standards nor guidelines are mandatory.

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

A. Simple step
B. Flowchart
C. Hierarchical
D. Graphic

Which of the following best describes a baseline?

A. Specifications for implementation of a policy
B. Instructions on how a policy is carried out
C. Aggregate of implementation standards and security controls
D. Teaching tools that help people conform to a policy

Which of the following best describes a procedure?

A. Specifications for implementation of a policy
B. Instructions on how a policy is carried out
C. Aggregate of implementation standards and security controls
D. Teaching tools that help people conform to a policy

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

A. Policies are mandatory, whereas standards are not.
B. Standards are mandatory, whereas policies are not.
C. Both polices and standards are mandatory.
D. Neither policies nor standards are mandatory.

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

A. Standards
B. Baselines
C. Guidelines
D. Guiding principles

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

A. Use passive voice.

B. Use “shall” to indicate requirements.

C. Use long sentences.

D. Limit a paragraph to one subject.

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

A. Use active voice.

B. Write short sentences.

C. Use ‘shall’ instead of “must”.

D. Avoid double negatives.

What is the purpose of the policy exceptions section?

A. To define sanctions for violations

B. To convey intent

C. To define exclusions

D. To specify mandatory directives

Chapter 3

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

A. ISO
B. NIST
C. FIPS
D. IEC

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

A. ITL bulletins
B. FIPS
C. Special Publication 800 series
D. NIST interagency reports

Which of the following traces actions to their source?

A. Accountability
B. Accounting
C. Assurance
D. Authentication

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

A. Accountability
B. Authentication
C. Authorization
D. Assurance

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

A. Rotation of duties
B. Log analysis
C. Code testing
D. Digital signatures

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

A. File integrity monitoring
B. Separation of duties
C. Encryption
D. Digital signatures

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

A. Authentication, integrity, confidentiality
B. Availability, integrity, confidentiality
C. Access, integrity, confidentiality
D. Authorization, integrity, confidentiality

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

A. Botnet
B. Bot
C. Victim
D. Handler

Which of the following statement best describes NIST?

A. A regulatory government organization that enforces standards
B. A coalition of 146 countries that creates standards
C. A nonregulatory federal agency that develops and promotes standards
D. A nongovernment organizations that develops and promotes standards

Which of the following best describes accounting?

A. The logging of access and usage of information resources
B. The configuring of the Security log to record events
C. The process of tracing actions to their source
D. The process of identifying users who seek access to secure information

Which of the following best describes accountability?

A. The logging of access and usage of information resources
B. The configuring of the Security log to record events
C. The process of tracing actions to their source
D. The process of identifying users who seek access to secure information

Which of the following can achieve authentication?

A. Intrusion detection systems
B. Log files
C. Auditing
D. Tokens

Chapter4

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

A. Compliance is discretionary.
B. Security is the responsibility of the IT department.
C. Little or no organizational accountability exists.
D. All the above.

Which of the following is the objective of risk assessment?

A. Identify the inherent risk.
B. Determine the impact of a threat.
C. Calculate the likelihood of a threat occurrence.
D. All the above.

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

A. Ad-hoc
B. Defined process
C. Optimized
D. Nonexistent

Which of the following best describes residual risk?

A. The likelihood of occurrence of a threat
B. The level of risk before security measures are applied
C. The level of risk after security measures are applied
D. The impact of risk if a threat is realized

Which of the following statements best describes risk transfer?

A. It shifts a portion of the risk responsibility to another organization.
B. It shifts a portion of the risk liability to another organization.
C. It takes steps to eliminate or modify the risk.
D. It shifts the entire risk responsibility to another organization.

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

A. FAIR
B. OCTAVE
C. RMF
D. CMM

Which of the following risks relates to negative public opinion?

A. Operational risk
B. Strategic risk
C. Financial risk
D. Reputational risk

Which of the following statements best describes strategic risk?

A. Risk that relates to monetary loss
B. Risk that relates to adverse business decisions
C. Risk that relates to a loss from failed or inadequate systems and processes
D. Risk that relates to violation of laws, regulations, or policy

Which of the following is the magnitude of harm?

A. Risk
B. Threat
C. Impact
D. Vulnerability

Which of the following statement best describes NIST?

A. A regulatory government organization that enforces standards
B. A coalition of 146 countries that creates standards
C. A nonregulatory federal agency that develops and promotes standards
D. A nongovernment organizations that develops and promotes standards

Which of the following best describes accounting?

A. The logging of access and usage of information resources
B. The configuring of the Security log to record events
C. The process of tracing actions to their source
D. The process of identifying users who seek access to secure information

Which of the following best describes accountability?

A. The logging of access and usage of information resources
B. The configuring of the Security log to record events
C. The process of tracing actions to their source
D. The process of identifying users who seek access to secure information

Which of the following can achieve authentication?

A. Intrusion detection systems
B. Log files
C. Auditing
D. Tokens

Chapter5

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

A. No read up and write up
B. No write up and no write down
C. No read up and no write down
D. No read down and no write up

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

A. No read up and read down
B. No write up and no read up
C. No read up and no write down
D. No read down and no write up

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

A. Secret
B. Protected
C. Confidential
D. Top secret

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

A. Social Security number
B. List of upcoming trade shows
C. Nonsensitive client or vendor information
D. Laboratory research

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

A. Secret
B. Protected
C. Confidential
D. Sensitive but Unclassified

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

A. Protected
B. Secret
C. Internal use
D. Public

Which of the following statements describes reclassification?

A. The process of changing the classification level to a lower level
B. The process of upgrading a classification
C. The process of removing a classification
D. The process of assigning a classification

Which if the following statements best describes declassification?

A. The process of downgrading a classification
B. The process of upgrading a classification
C. The process of removing a classification
D. The process of assigning a new classification

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

A. IP domain name
B. MAC address
C. IPV4 address
D. IPv6 address

A MAC address is in which of the following formats?

A. Decimal
B. Binary
C. Hexadecimal
D. Unicode

Chapter 6

Why shouldn't information about specific systems be included in a job description?

A. To make sure candidates know all systems
B. To protect against social engineering and other attacks
C. To get as many candidates as possible
D. To get more knowledgeable candidates

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

A. Recruitment
B. Onboarding
C. User provisioning
D. Orientation

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

A. The employee is added to the organization's payroll.
B. The employee is provided with a username or smart card.
C. A background check is conducted for the employee.
D. The employee expectations of privacy are determined.

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

A. Onboarding
B. Recruitment
C. Termination
D. User provisioning

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

A. To teach skills that would allow a person to perform a certain function
B. To focus attention on security
C. To integrate all the security skills and competencies into a common body of knowledge
D. To involve management in the process

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

A. Short-term
B. Long-term
C. Intermediate
D. Upon hiring

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

A. To teach skills that would allow a person to perform a certain function
B. To focus attention on security
C. To integrate all the security skills and competencies into a common body of knowledge
D. To involve management in the process

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

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

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

A. Career development
B. Termination
C. User provisioning
D. Onboarding

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

A. Introduction
B. Data classification
C. Applicable policy statements
D. Handling standards

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

A. FACTA
B. HIPAA
C. FCRA
D. DPPA