Vendor: ISC

Exam Code: CISSP

Exam Name: Certified Information Systems Security Professional

Version: Demo

QUESTION 1
All of the following are basic components of a security policy EXCEPT the

A. definition of the issue and statement of relevant terms
B. statement of roles and responsibilities
C. statement of applicability and compliance requirements
D. statement of performance of characteristics and requirements

Correct Answer: D

QUESTION 2
A security policy would include all of the following EXCEPT

A. Background
B. Scope statement
C. Audit requirements
D. Enforcement

Correct Answer: B

QUESTION 3
Which one of the following is an important characteristic of an information security policy?

A. Identifies major functional areas of information.
B. Quantifies the effect of the loss of the information.
C. Requires the identification of information owners.
D. Lists applications that support the business function.

Correct Answer: A

QUESTION 4
Ensuring the integrity of business information is the PRIMARY concern of

A. Encryption Security
B. Procedural Security
C. Logical Security
D. On-line Security

Correct Answer: B

QUESTION 5
Which of the following would be the first step in establishing an information security program?

A. Adoption of a corporate information security policy statement.
B. Development and implementation of an information security standards manual.
C. Development of a security awareness-training program.
D. Purchase of security access control software.

Correct Answer: A

QUESTION 6
Which of the following department managers would be best suited to oversee the development of an information security policy?

A. Information Systems
B. Human Resources
C. Business operations
D. Security administration

Correct Answer: C

QUESTION 7
What is the function of a corporate information security policy?

A. Issue corporate standard to be used when addressing specific security problems.
B. Issue guidelines in selecting equipment, configuration, design, and secure operations.
C. Define the specific assets to be protected and identify the specific tasks which must be completed to secure them.
D. Define the main security objectives which must be achieved and the security framework to meet business objectives.

Correct Answer: D

QUESTION 8
Why must senior management endorse a security policy?

A. So that they will accept ownership for security within the organization.
B. So that employees will follow the policy directives.
C. So that external bodies will recognize the organizations commitment to security.
D. So that they can be held legally accountable.

Correct Answer: A

QUESTION 9
In which one of the following documents is the assignment of individual roles and responsibilities MOST appropriately defined?

A. Security policy
B. Enforcement guidelines
C. Acceptable use policy
D. Program manual

Correct Answer: C

QUESTION 10
Which of the following defines the intent of a system security policy?

A. A definition of the particular settings that have been determined to provide optimum security.
B. A brief, high-level statement defining what is and is not permitted during the operation of the system.
C. A definition of those items that must be excluded on the system.
D. A listing of tools and applications that will be used to protect the system.

Correct Answer: A

QUESTION 11
When developing an information security policy, what is the FIRST step that should be taken?

A. Obtain copies of mandatory regulations.
B. Gain management approval.
C. Seek acceptance from other departments.
D. Ensure policy is compliant with current working practices.

Correct Answer: B

QUESTION 12
Which one of the following should NOT be contained within a computer policy?

A. Definition of management expectations.
B. Responsibilities of individuals and groups for protected information.

C. Statement of senior executive support.
D. Definition of legal and regulatory controls.

Correct Answer: B

QUESTION 13
Which one of the following is NOT a fundamental component of a Regulatory Security Policy?

A. What is to be done?
B. When it is to be done?
C. Who is to do it?
D. Why is it to be done?

Correct Answer: C

QUESTION 14
Which one of the following statements describes management controls that are instituted to implement a security policy?

A. They prevent users from accessing any control function.
B. They eliminate the need for most auditing functions.
C. They may be administrative, procedural, or technical.
D. They are generally inexpensive to implement.

Correct Answer: C

QUESTION 15
Which must bear the primary responsibility for determining the level of protection needed for information systems resources?

A. IS security specialists
B. Senior Management
C. Seniors security analysts
D. system auditors

Correct Answer: B

QUESTION 16
Which of the following choices is NOT part of a security policy?

A. definition of overall steps of information security and the importance of security
B. statement of management intend, supporting the goals and principles of information security
C. definition of general and specific responsibilities for information security management
D. description of specific technologies used in the field of information security

Correct Answer: D

QUESTION 17
In an organization, an Information Technology security function should:

A. Be a function within the information systems functions of an organization.
B. Report directly to a specialized business unit such as legal, corporate security or insurance.
C. Be lead by a Chief Security Officer and report directly to the CEO.
D. Be independent but report to the Information Systems function.

Correct Answer: C

QUESTION 18
Which of the following embodies all the detailed actions that personnel are required to follow?

A. Standards
B. Guidelines
C. Procedures
D. Baselines

Correct Answer: C

QUESTION 19
A significant action has a state that enables actions on an ADP system to be traced to individuals who may then be held responsible. The action does NOT include:

A. Violations of security policy.
B. Attempted violations of security policy.
C. Non-violations of security policy.
D. Attempted violations of allowed actions.

Correct Answer: C