QUESTIONS & ANSWERS

Kill your exam at first Attempt

KILL EXAMS

ISC2

CISSP

Certified Information Systems Security Professional

QUESTION: 225
As part of the security assessment plan, the security professional has been asked to use a negative testing strategy on a new website. Which of the following actions would be performed?

A. Use a web scanner to scan for vulnerabilities within the website.
B. Perform a code review to ensure that the database references are properly addressed.
C. Establish a secure connection to the web server to validate that only the approved ports are open.
D. Enter only numbers in the web form and verify that the website prompts the user to enter a valid input.

Answer: D

QUESTION: 226
Who has the PRIMARY responsibility to ensure that security objectives are aligned with organization goals?

A. Senior management
B. Information security department
C. Audit committee
D. All users

Answer: C

QUESTION: 227
Which of the following alarm systems is recommended to detect intrusions through windows in a high-noise, occupied environment?

A. Acoustic sensor
B. Motion sensor
C. Shock sensor
D. Photoelectric sensor

Answer: C

QUESTION: 228
Which of the following is the MOST effective practice in managing user accounts when an employee is terminated?

A. Implement processes for automated removal of access for terminated employees.
B. Delete employee network and system IDs upon termination.
C. Manually remove terminated employee user-access to all systems and applications.
D. Disable terminated employee network ID to remove all access.

Answer: B

QUESTION: 229
Which of the following is the MOST important part of an awareness and training plan to prepare employees for emergency situations?

A. Having emergency contacts established for the general employee population to get information
B. Conducting business continuity and disaster recovery training for those who have a direct role in the recovery
C. Designing business continuity and disaster recovery training programs for different audiences
D. Publishing a corporate business continuity and disaster recovery plan on the corporate website

Answer: C

QUESTION: 230
What is the process of removing sensitive data from a system or storage device with the intent that the data cannot be reconstructed by any known technique?

A. Purging
B. Encryption
C. Destruction
D. Clearing

Answer: A

QUESTION: 231
Which one of the following considerations has the LEAST impact when considering transmission security?

A. Network availability
B. Node locations
C. Network bandwidth
D. Data integrity

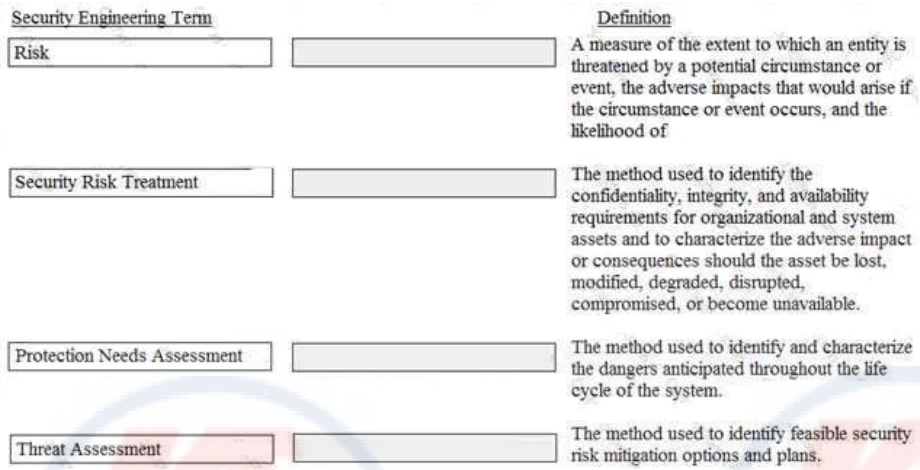
Answer: C

QUESTION: 232
The security accreditation task of the System Development Life Cycle (SDLC) process is completed at the end of which phase?

A. System acquisition and development
B. System operations and maintenance
C. System initiation
D. System implementation

Answer: B

QUESTION: 233
DRAG DROP
Drag the following Security Engineering terms on the left to the BEST definition on the right.



Answer:
Risk - A measure of the extent to which an entity is threatened by a potential circumstance of event, the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of occurrence. Protection Needs Assessment - The method used to identify the confidentiality, integrity, and availability requirements for organizational and system assets and to characterize the adverse impact or consequences should be asset be lost, modified, degraded, disrupted, compromised, or become unavailable. Threat assessment - The method used to identify and characterize the dangers anticipated throughout the life cycle of the system. Security Risk Treatment - The method used to identify feasible security risk mitigation options and plans.

QUESTION: 234
Which of the following is the BEST reason for the use of security metrics?

A. They ensure that the organization meets its security objectives.
B. They provide an appropriate framework for Information Technology (IT) governance.
C. They speed up the process of quantitative risk assessment.
D. They quantify the effectiveness of security processes.

Answer: B

QUESTION: 235
Which of the following is a benefit in implementing an enterprise Identity and Access Management (IAM) solution?

A. Password requirements are simplified.
B. Risk associated with orphan accounts is reduced.
C. Segregation of duties is automatically enforced.
D. Data confidentiality is increased.

Answer: A