



Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.



CISSP Dumps
CISSP Braindumps
CISSP Real Questions
CISSP Practice Test
CISSP Actual Questions



ISC2

CISSP

*Certified Information Systems Security Professional
- 2023*



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.

Security Engineering Term		Definition
Risk		A measure of the extent to which an entity is threatened by a potential circumstance or event, the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of
Security Risk Treatment		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 the asset be lost, modified, degraded, disrupted, compromised, or become unavailable.
Protection Needs Assessment		The method used to identify and characterize the dangers anticipated throughout the life cycle of the system.
Threat Assessment		The method used to identify feasible security risk mitigation options and plans.

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



SAMPLE QUESTIONS

*These questions are for demo purpose only. **Full version** is up to date and contains actual questions and answers.*

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:

Actual Exam Questions: *Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.*

Exam Dumps: *Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.*

Practice Tests: *Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.*

Guaranteed Success: *Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.*

Updated Content: *Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.*

Technical Support: *Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.*

For More exams visit <https://killexams.com/vendors-exam-list>
Kill your exam at First Attempt....Guaranteed!