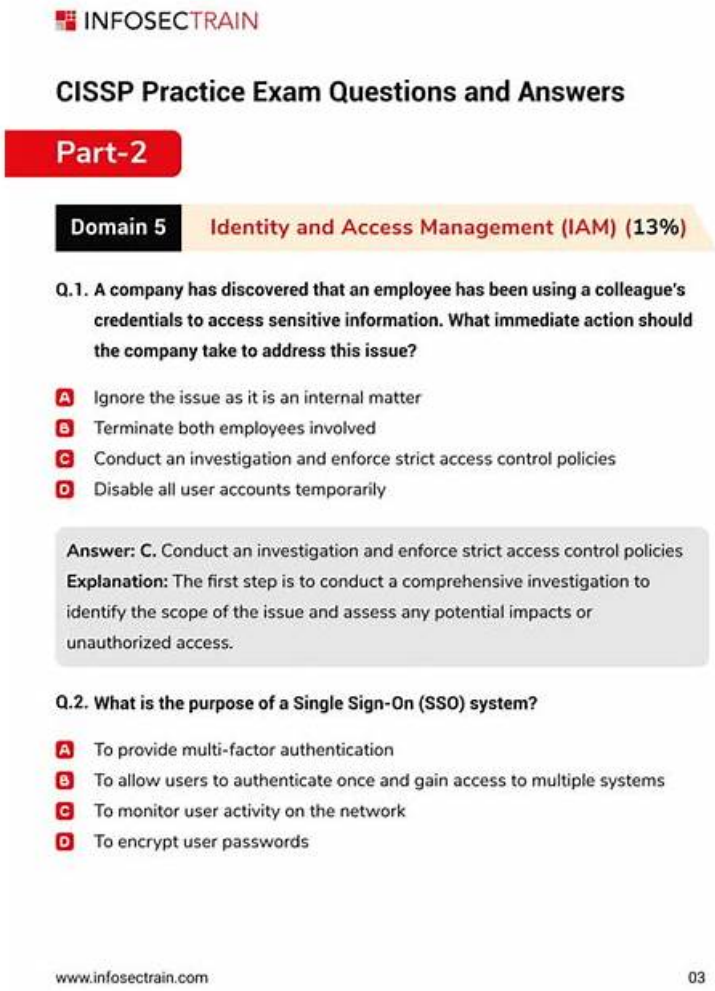
Three Formats for CISSP Practice Tests BraindumpsIT Exam Prep Solutions


INFOSECTRAIN

CISSP Practice Exam Questions and Answers

Part-2

Domain 5 Identity and Access Management (IAM) (13%)

Q.1. A company has discovered that an employee has been using a colleague's credentials to access sensitive information. What immediate action should the company take to address this issue?

A Ignore the issue as it is an internal matter
B Terminate both employees involved
C Conduct an investigation and enforce strict access control policies
D Disable all user accounts temporarily

Answer: C. Conduct an investigation and enforce strict access control policies
Explanation: The first step is to conduct a comprehensive investigation to identify the scope of the issue and assess any potential impacts or unauthorized access.

Q.2. What is the purpose of a Single Sign-On (SSO) system?

A To provide multi-factor authentication
B To allow users to authenticate once and gain access to multiple systems
C To monitor user activity on the network
D To encrypt user passwords

www.infosectrain.com 03

P.S. Free 2026 ISC CISSP dumps are available on Google Drive shared by BraindumpsIT: https://drive.google.com/open?id=1Wjx3Xb7f6eKZjTjpuggJHKv_W0zKCATp

When you choose to attempt the mock exam on the ISC CISSP practice software by BraindumpsIT, you have the leverage to custom the questions and attempt it at any time. Keeping a check on your Certified Information Systems Security Professional (CISSP) exam preparation will make you aware of your strong and weak points. You can also identify your speed on the practice software by BraindumpsIT and thus manage time more efficiently in the actual ISC exam.

Achieving the ISC CISSP Certification Exam demonstrates a high level of competence and expertise in the field of information security. It validates the skills and knowledge required to design, implement, and manage a comprehensive security program. Certified Information Systems Security Professional (CISSP) certification is highly valued by employers and is recognized globally as a standard of excellence in information security. It can also lead to greater career opportunities and higher salaries for certified professionals.

>> CISSP Guaranteed Success <<

CISSP Top Questions, New CISSP Test Camp

Certified Information Systems Security Professional (CISSP) Exam Questions save your study time and help you prepare in less

duration. We have hundreds of most probable questions which have a chance to appear in the real Certified Information Systems Security Professional (CISSP) exam. The ISC CISSP exam questions are affordable and 365 days free updated, and you can use them without any guidance. However, in case of any trouble, our support team is always available to sort out the problems. We will provide you with the information covered in the current test and incorporate materials that originate from ISC CISSP Exam Dumps.

ISC CISSP Exam is a challenging but rewarding certification for those interested in pursuing a career in information security. It is a testament to one's knowledge and skills in the field and can open up a world of opportunities for career advancement and professional growth.

ISC Certified Information Systems Security Professional (CISSP) Sample Questions (Q824-Q829):

NEW QUESTION # 824
What is called the formal acceptance of the adequacy of a system's overall security by the management?

- A. Accreditation
- B. Acceptance
- C. Evaluation
- D. Certification

Answer: A

Explanation:
Accreditation is the authorization by management to implement software or systems
in a production environment. This authorization may be either provisional or full.
The following are incorrect answers:
Certification is incorrect. Certification is the process of evaluating the security stance of the
software or system against a selected set of standards or policies. Certification is the technical
evaluation of a product. This may precede accreditation but is not a required precursor.
Acceptance is incorrect. This term is sometimes used as the recognition that a piece of software or
system has met a set of functional or service level criteria (the new payroll system has passed its
acceptance test). Certification is the better tem in this context.
Evaluation is incorrect. Evaluation is certainly a part of the certification process but it is not the
best answer to the question.
Reference(s) used for this question:
The Official Study Guide to the CBK from ISC2, pages 559-560
AIO3, pp. 314 - 317
AIOv4 Security Architecture and Design (pages 369 - 372)
AIOv5 Security Architecture and Design (pages 370 - 372)

NEW QUESTION # 825
What is the document that describes the measures that have been implemented or planned to correct any deficiencies noted during the assessment of the security controls?

- A. Security Assessment Plan (SAP)
- B. Business Impact Analysis (BIA)
- C. Plan of Action and Milestones (POA&M)
- D. Security Assessment Report (SAR)

Answer: C

Explanation:
The document that describes the measures that have been implemented or planned to correct any deficiencies noted during the assessment of the security controls is the Plan of Action and Milestones (POA&M). A POA&M is a tool that helps to track and manage the remediation actions for the identified weaknesses or gaps in the security controls. A POA&M typically includes the following elements: the description of the weakness, the source of the weakness, the risk level of the weakness, the proposed corrective action, the responsible party, the estimated completion date, and the status of the action. A POA&M can help to prioritize the remediation efforts, monitor the progress, and report the results.

NEW QUESTION # 826
Which of the following would best describe the difference between white-box testing and black-box testing?

- A. Black-box testing uses the bottom-up approach.
- B. White-box testing is performed by an independent programmer team.
- C. White-box testing examines the program internal logical structure.
- D. Black-box testing involves the business units

Answer: C

Explanation:
Black-box testing observes the system external behavior, while white-box testing is
a detailed exam of a logical path, checking the possible conditions.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor
2002 review manual, chapter 6: Business Application System Development, Acquisition,
Implementation and Maintenance (page 299).

NEW QUESTION # 827
Complete the following sentence. A digital signature is a:

- A. hash value that has been encrypted with the sender's private key
- B. hash value that has been encrypted with the sender's public key
- C. senders signature signed and scanned in a digital format
- D. hash value that has been encrypted with the senders Session key

Answer: A

Explanation:
Explanation/Reference:
Explanation:
A digital signature is a hash value that was encrypted with the sender's private key.
Digital signatures are based on public key cryptography, also known as asymmetric cryptography. Using a public key algorithm such as RSA, one can generate two keys that are mathematically linked: one private and one public. To create a digital signature, signing software (such as an email program) creates a one- way hash of the electronic data to be signed. The private key is then used to encrypt the hash. The encrypted hash -- along with other information, such as the hashing algorithm -- is the digital signature.
The reason for encrypting the hash instead of the entire message or document is that a hash function can convert an arbitrary input into a fixed length value, which is usually much shorter. This saves time since hashing is much faster than signing.
Incorrect Answers:
B: The hash value is signed with the sender's private key, not the public key to prove that the message came from the sender and has not been altered in transit.
C: A session key is not used to encrypt the hash value in a digital signature.
D: A digital signature is not a sender's signature signed and scanned in a digital format.
References:
Harris, Shon, All In One CISSP Exam Guide, 6th Edition, McGraw-Hill, 2013, p. 829
http://searchsecurity.techtarget.com/definition/digital-signature

NEW QUESTION # 828
Which choice below is an accurate statement about standards?

- A. Standards are senior management's directives to create a computer security program.
- B. Standards are the first element created in an effective security policy program.
- C. Standards are used to describe how policies will be implemented within an organization.
- D. Standards are the high-level statements made by senior management in support of information systems security.

Answer: C

Explanation:
The other options describe policies. Guidelines, standards, and procedures often accompany policy, but always follow the senior level management's statement of policy. Procedures, standards, and guidelines are used to describe how these policies will be

implemented within an organization. Simply put, the three break down as follows: Standards specify the use of specific technologies in a uniform way (for example, the standardization of operating procedures). Guidelines are similar to standards but are recommended actions. Procedures are the detailed steps that must be performed for any task.

NEW QUESTION # 829

.....