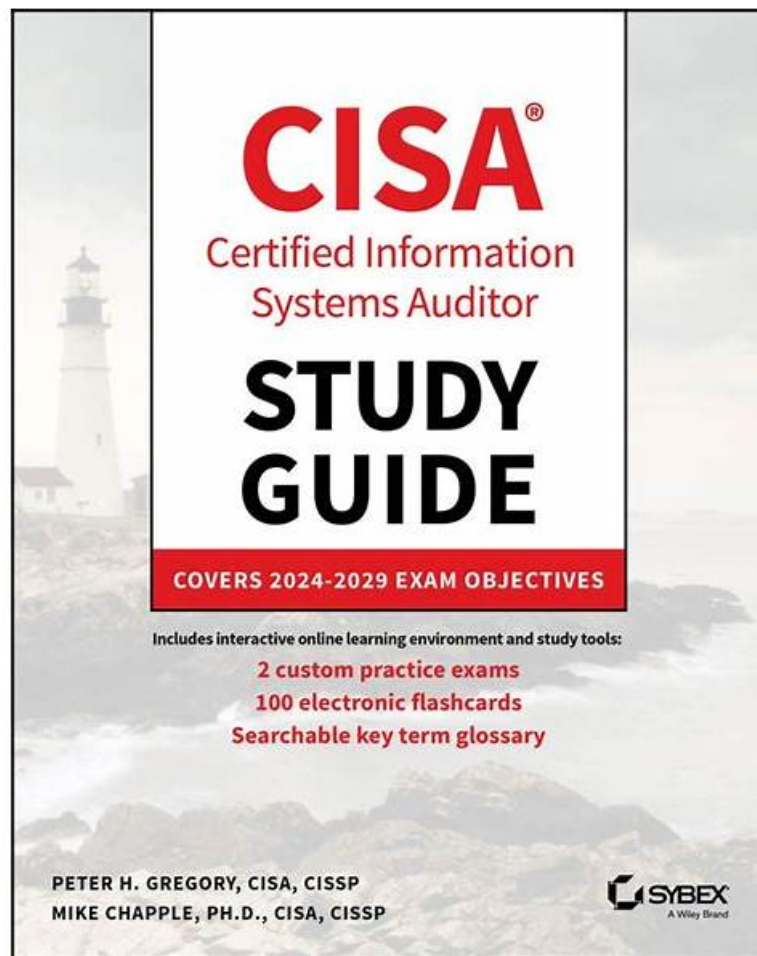


CISA Exam Objectives Pdf | CISA Updated Testkings



2026 Latest DumpExam CISA PDF Dumps and CISA Exam Engine Free Share: <https://drive.google.com/open?id=1glyd5RiJ7d2zXdl6KLF9vRmbUa6X1J0N>

Our CISA exam guide has high quality of service. We provide 24-hour online service on the CISA training engine. If you have any questions in the course of using the bank, you can contact us by email. We will provide you with excellent after-sales service with the utmost patience and attitude. And we will give you detailed solutions to any problems that arise during the course of using the CISA learning braindumps. And our CISA study materials welcome your supervision and criticism.

Who Should Take CISA Certification Exam?

The ISACA CISA certification exam is suitable for anyone who wants to develop skills in auditing, controlling, and keeping the highest standards in information security. This exam was designed for IT and IS auditors who want to take a step further in their careers. It was also developed for assurance, control, and information security specialists. When it comes to eligibility requirements, ISACA is very clear in offering the right information. Therefore, candidates should demonstrate that they should have a minimum of 5 years of experience in IT or IS audit. They should also be skilled in control, assurance, or security. Besides, experience waivers are also possible and they can be of a maximum of 3 years.

ISACA CISA (Certified Information Systems Auditor) Certification Exam is a globally recognized certification for professionals in the field of information systems auditing. It is designed to test the knowledge, skills, and abilities of candidates in five domains related to information systems auditing. Certified Information Systems Auditor certification is highly regarded in the industry and is recognized by employers worldwide, making it an excellent choice for professionals looking to advance their careers in this field.

The CISA Certification Exam covers a wide range of topics, including IS audit process, IT governance, system and infrastructure life cycle, information security management, and business continuity and disaster recovery. CISA exam is designed to test the candidate's knowledge and skills in these areas, as well as their ability to apply them in real-world scenarios. CISA exam consists of 150 multiple-choice questions and is four hours long.

High Pass-Rate CISA Exam Objectives Pdf & Leader in Certification Exams Materials & Effective CISA Updated Testkings

As we all know, it is a must for all of the candidates to pass the exam if they want to get the related CISA certification which serves as the best evidence for them to show their knowledge and skills. If you want to simplify the preparation process, here comes a piece of good news for you. Our CISA Exam Question has been widely praised by all of our customers in many countries and our company has become the leader in this field. Now I would like to give you some detailed information about the advantages of our CISA guide torrent.

ISACA Certified Information Systems Auditor Sample Questions (Q199-Q204):

NEW QUESTION # 199

What is a primary high-level goal for an auditor who is reviewing a system development project?

- A. To ensure that projects are monitored and administrated effectively
- B. To ensure that programming and processing environments are segregated
- C. To ensure that business objectives are achieved
- D. To ensure that proper approval for the project has been obtained

Answer: C

Explanation:

Section: Protection of Information Assets

Explanation:

A primary high-level goal for an auditor who is reviewing a systems- development project is to ensure that business objectives are achieved. This objective guides all other systems development objectives.

NEW QUESTION # 200

An IS auditor is concerned that unauthorized access to a highly sensitive data center might be gained by piggybacking or tailgating. Which of the following is the BEST recommendation? (Choose Correct answer and give explanation from CISA Certification - Information Systems Auditor official book)

- A. Airlock entrance
- B. Procedures for escorting visitors
- C. Biometrics
- D. Intruder alarms

Answer: A

Explanation:

Explanation

The best recommendation to prevent unauthorized access to a highly sensitive data center by piggybacking or tailgating is to use an airlock entrance. An airlock entrance is a type of access control system that consists of two doors that are interlocked, so that only one door can be opened at a time. This prevents an unauthorized person from following an authorized person into the data center without being detected. An airlock entrance can also be integrated with other security measures, such as biometrics, card readers, or PIN pads, to verify the identity and authorization of each person entering the data center.

Biometrics (option A) is a method of verifying the identity of a person based on their physical or behavioral characteristics, such as fingerprints, iris scans, or voice recognition. Biometrics can provide a high level of security, but they are not sufficient to prevent piggybacking or tailgating, as an unauthorized person can still follow an authorized person who has been authenticated by the biometric system.

Procedures for escorting visitors (option B) is a policy that requires all visitors to the data center to be accompanied by an authorized employee at all times. This can help prevent unauthorized access by visitors, but it does not address the risk of piggybacking or tailgating by other employees or contractors who may have legitimate access to the building but not to the data center.

Intruder alarms (option D) are devices that detect and alert when an unauthorized person enters a restricted area. Intruder alarms

can provide a deterrent and a response mechanism for unauthorized access, but they are not effective in preventing piggybacking or tailgating, as they rely on the detection of the intruder after they have already entered the data center.

References: 1: CISA Certification | Certified Information Systems Auditor | ISACA 2: CISA Certified Information Systems Auditor Study Guide, 4th Edition 3: CISA - Certified Information Systems Auditor Study Guide [Book]

NEW QUESTION # 201

Which of the following would a digital signature MOST likely prevent?

- A. Repudiation
- B. Unauthorized change
- C. Corruption
- D. Disclosure

Answer: C

Explanation:

Section: Protection of Information Assets

Explanation:

The main reason of using digital signature is to ensure message integrity. It also helps to ensure authenticity and non-repudiation of the message. A digital signature can never ensure the confidentiality of data.

NEW QUESTION # 202

Which of the following encrypt/decrypt steps provides the GREATEST assurance of achieving confidentiality, message integrity and nonrepudiation by either sender or recipient?

- A. The encrypted prehash code and the message are encrypted using a secret key.
- B. The recipient uses the sender's public key, verified with a certificate authority, to decrypt the prehash code.
- C. The recipient uses their private key to decrypt the secret key.
- D. The encrypted prehash code is derived mathematically from the message to be sent.

Answer: B

Explanation:

Section: Protection of Information Assets

Explanation:

Most encrypted transactions use a combination of private keys, public keys, secret keys, hash functions and digital certificates to achieve confidentiality, message integrity and nonrepudiation by either sender or recipient. The recipient uses the sender's public key to decrypt the prehash code into a posthash code, which when equaling the prehash code, verifies the identity of the sender and that the message has not been changed in route; this would provide the greatest assurance. Each sender and recipient has a private key known only to themselves and a public key, which can be known by anyone. Each encryption/decryption process requires at least one public key and one private key, and both must be from the same party. A single, secret key is used to encrypt the message, because secret key encryption requires less processing power than using public and private keys. A digital certificate, signed by a certificate authority, validates senders' and recipients' public keys.

NEW QUESTION # 203

Which of the following should an IS auditor recommend be done FIRST when an organization is planning to implement an IT compliance program?

- A. Identify applicable laws, regulations, and standards
- B. Research and purchase an industry-recognized IT compliance tool
- C. Identify staff training needs related to compliance requirements
- D. Analyze historical compliance-related audit findings

Answer: A

