Valid CISM Exam Camp Pdf | Certification CISM Torrent

P.S. Free 2026 ISACA CISM dumps are available on Google Drive shared by PassReview: https://drive.google.com/open?id=1xqWt8z1QUVCYWzRfcZIA3CCarpeakwky

The results prove that PassReview's CISM dumps work the best. And this is the reason that our CISM exam questions are gaining wide popularity among the ambitious professionals who want to enhance their workability and career prospects. Our experts have developed them into a specific number of CISM questions and answers encompassing all the important portions of the exam. They have keenly studied the previous CISM Exam Papers and consulted the sources that contain the updated and latest information on the exam contents. The end result of these strenuous efforts is set of CISM dumps that are in every respect enlightening and relevant to your to actual needs.

ISACA CISM certification exam is an essential certification for individuals who are responsible for managing and implementing information security programs in organizations. Certified Information Security Manager certification validates the individual's expertise in managing, designing, and assessing information security programs. It is a globally recognized credential that is recognized by organizations around the world and is a preferred certification for information security professionals.

The CISM certification exam covers four key domains: Information Security Governance, Information Risk Management and Compliance, Information Security Program Development and Management, and Information Security Incident Management. CISM Exam consists of 150 multiple-choice questions that must be completed within four hours. CISM exam is available in English, Chinese (Simplified and Traditional), French, German, Hebrew, Italian, Japanese, Korean, Portuguese (Brazilian), Spanish, and Turkish. To be eligible to take the exam, candidates must have at least five years of experience in information security, with at least three years of experience in information security management.

>> Valid CISM Exam Camp Pdf <<

Certification CISM Torrent | Valid Braindumps CISM Book

Our CISM learning guide beckons exam candidates around the world with our attractive characters. Our experts made significant contribution to their excellence. So we can say bluntly that our CISMsimulating exam is the best. Our effort in building the content of our CISM Study Materials lead to the development of learning guide and strengthen their perfection. You may find that there are always the latest information in our CISM practice engine and the content is very accurate.

Who should take the CISM exam

The ISACA Certified Information Security Manager CISM Exam certification is an internationally-recognized validation that identifies persons who earn it as possessing skilled as Certified Information Security Manager. If a candidate wants significant improvement in career growth needs enhanced knowledge, skills, and talents. The ISACA Certified Information Security Manager CISM Exam Certification provides proof of this advanced knowledge and skill. If a candidate has knowledge and skills that are required to pass the ISACA Certified Information Security Manager CISM Exam then he should take this exam.

ISACA Certified Information Security Manager Sample Questions (Q748-

Q753):

NEW QUESTION # 748

Which of the following is the BEST course of action when an information security manager identifies that systems are vulnerable to emerging threats?

- A. Notify senior management and key stakeholders of the threats.
- B. Frequently update systems and monitor the threat landscape.
- C. Increase awareness of the threats among employees who work with the systems.
- D. Monitor the network containing the affected systems for malicious traffic.

Answer: B

Explanation:
The best course of action when an information security manager identifies that systems are vulnerable to emerging threats is to frequently update systems and monitor the threat landscape, as this will help to reduce the exposure and impact of the threats, and enable timely detection and response. Updating systems involves applying patches, fixing vulnerabilities, and implementing security controls. Monitoring the threat landscape involves collecting and analyzing threat intelligence, identifying new attack vectors and techniques, and assessing the risk and impact of the threats.
Reference = CISM Review Manual, 27th Edition, Chapter 4, Section 4.2.1, page 2211; State of Cybersecurity 2023: Navigating Current and Emerging Threats2; CISM Online Review Course, Module 4, Lesson 2, Topic 13

NEW QUESTION # 749

After a recent malware Incident an organization's IT steering committee has asked the information security manager for a presentation on the status of the information security program. Which of the following is MOST important to address in the presentation?

- A. Disaster recovery and continuity program plans
- B. Measures taken to prevent the risk of a data breach
- C. Remediation schedule for patch management
- D. Antivirus program and incident response plans

Answer: D

NEW QUESTION # 750

Which of the following risks would BEST be assessed using qualitative risk assessment techniques?

- A. Power outage lasting 24 hours
- B. Theft of purchased software
- C. Permanent decline in customer confidence
- D. Temporary loss of e-mail due to a virus attack

Answer: C

Explanation:
Explanation/Reference:
Explanation:
A permanent decline in customer confidence does not lend itself well to measurement by quantitative techniques. Qualitative techniques are more effective in evaluating things such as customer loyalty and goodwill. Theft of software, power outages and temporary loss of e-mail can be quantified into monetary amounts easier than can be assessed with quantitative techniques.

NEW QUESTION # 751

What is the PRIMARY role of the information security program?

- A. To educate stakeholders regarding information security requirements
- B. To perform periodic risk assessments and business impact analyses (BIAs)
- C. To develop and enforce a set of security policies aligned with the business

- D. To provide guidance in managing organizational security risk

Answer: B

NEW QUESTION # 752

Which of the following BEST enables users to recover from ransomware or malware attacks?

- A. Frequent system backups
- B. Regular antivirus updates
- C. End-user awareness training
- D. Incident response plans

Answer: A

Explanation:

Frequent system backups (B) are the most effective means of recovery from ransomware or malware attacks. CISM emphasizes resilience and recoverability as critical aspects of incident management. While incident response plans (A), antivirus updates (C), and awareness training (D) help prevent or manage incidents, they do not guarantee restoration of data or systems. Reliable, tested backups allow organizations to restore operations without paying ransoms or suffering permanent data loss.
References: ISACA CISM Review Manual (Incident management-recovery and resilience); CISM Exam Content Outline (Domain 4).

NEW QUESTION # 753

......