CISM Q&As

Certified Information Security Manager

Pass Isaca CISM Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/cism.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Isaca Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Evidence from a compromised server has to be acquired for a forensic investigation. What would be the BEST source?

A. A bit-level copy of all hard drive data

B. The last verified backup stored offsite

C. Data from volatile memory

D. Backup servers

Correct Answer: A

The bit-level copy image file ensures forensic quality evidence that is admissible in a court of law. Choices B and D may not provide forensic quality data for investigative work, while choice C alone may not provide enough evidence.

QUESTION 2

Which of the following Is MOST useful to an information security manager when conducting a post-incident review of an attack?

A. Cost of the attack to the organization

B. Location of the attacker

C. Method of operation used by the attacker

D. Details from intrusion detection system (IDS) logs

Correct Answer: C

The method of operation used by the attacker is the most useful information for an information security manager when conducting a post-incident review of an attack. This information can help identify the root cause of the incident, the vulnerabilities exploited, the impact and severity of the attack, and the effectiveness of the existing security controls. The method of operation can also provide insights into the attacker\\'s motives, skills, and resources, which can help improve the organization\\'s threat intelligence and risk assessment. The cost of the attack to the organization, the location of the attacker, and the details from IDS logs are all relevant information for a post-incident review, but they are not as useful as the method of operation for improving the incident handling process and preventing future attacks. References: CISM Review Manual 2022, page 316; CISM Item Development Guide 2022, page 9; ISACA CISM: PRIMARY goal of a post-incident review should be to?

QUESTION 3

Which of the following is MOST closely associated with a business continuity program?

A. Confirming that detailed technical recovery plans exist

B. Periodically testing network redundancy

C. Updating the hot site equipment configuration every quarter

D. Developing recovery time objectives (RTOs) for critical functions

Correct Answer: D

Technical recovery plans, network redundancy and equipment needs are all associated with infrastructure disaster recovery. Only recovery time objectives (RTOs) directly relate to business continuity.

QUESTION 4

Which of the following is a PRIMARY responsibility of an information security governance committee?

A. Analyzing information security policy compliance reviews

B. Approving the purchase of information security technologies

C. Reviewing the information security strategy

D. Approving the information security awareness training strategy

Correct Answer: C

QUESTION 5

Which of the following is the MOST appropriate frequency for updating antivirus signature files for antivirus software on production servers?

A. Daily

B. Weekly

C. Concurrently with O/S patch updates

D. During scheduled change control updates

Correct Answer: A

New viruses are being introduced almost daily. The effectiveness of virus detection software depends on frequent updates to its virus signatures, which are stored on antivirus signature files so updates may be carried out several times during the day. At a minimum, daily updating should occur. Patches may occur less frequently. Weekly updates may potentially allow new viruses to infect the system.