

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.leads4pass.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

The MOST effective way to continuously monitor an organization's cybersecurity posture is to evaluate its:

- A. compliance with industry regulations.
- B. key performance indicators (KPIs).
- C. level of support from senior management.
- D. timeliness in responding to attacks.

Correct Answer: D

QUESTION 2

A serious vulnerability is reported in the firewall software used by an organization. Which of the following should be the immediate action of the information security manager?

- A. Ensure that all OS patches are up-to-date
- B. Block inbound traffic until a suitable solution is found
- C. Obtain guidance from the firewall manufacturer
- D. Commission a penetration test

Correct Answer: C

The best source of information is the firewall manufacturer since the manufacturer may have a patch to fix the vulnerability or a workaround solution. Ensuring that all OS patches are up-to-date is a best practice, in general, but will not necessarily address the reported vulnerability. Blocking inbound traffic may not be practical or effective from a business perspective. Commissioning a penetration test will take too much time and will not necessarily provide a solution for corrective actions.

QUESTION 3

Which of the following should be done FIRST when establishing a new data protection program that must comply with applicable data privacy regulations?

- A. Evaluate privacy technologies required for data protection.
- B. Encrypt all personal data stored on systems and networks.
- C. Update disciplinary processes to address privacy violations.
- D. Create an inventory of systems where personal data is stored.

Correct Answer: D

QUESTION 4

Which of the following would BEST help to identify vulnerabilities introduced by changes to an organization's technical infrastructure?

- A. An intrusion detection system
- B. Established security baselines
- C. Penetration testing
- D. Log aggregation and correlation

Correct Answer: C

QUESTION 5

Before engaging outsourced providers, an information security manager should ensure that the organization's data classification requirements:

- A. are compatible with the provider's own classification.
- B. are communicated to the provider.
- C. exceed those of the outsourcer.
- D. are stated in the contract.

Correct Answer: D

The most effective mechanism to ensure that the organization's security standards are met by a third party, would be a legal agreement. Choices A, B and C are acceptable options, but not as comprehensive or as binding as a legal contract.

[Latest CISM Dumps](#)

[CISM Practice Test](#)

[CISM Exam Questions](#)