



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

Which of the following will provide the MOST guidance when deciding the level of protection for an information asset?

- A. Impact on information security program
- B. Cost of controls
- C. Impact to business function
- D. Cost to replace

Correct Answer: C

When deciding the level of protection for an information asset, the most important factor to consider is the impact to the business function. The value of the asset should be evaluated in terms of its importance to the organization's operations and how its security posture affects the organization's overall security posture. Additionally, the cost of implementing controls, the potential impact on the information security program, and the cost to replace the asset should be taken into account when determining the appropriate level of protection for the asset.

QUESTION 2

Which of the following metrics would provide management with the MOST useful information about the effectiveness of a security awareness program?

- A. Increased number of downloads of the organization's security policy
- B. Decreased number of security incidents
- C. Increased number of reported security incidents
- D. Decreased number of phishing attacks

Correct Answer: B

QUESTION 3

The PRIMARY purpose of performing an internal attack and penetration test as part of an incident response program is to identify:

- A. weaknesses in network and server security.
- B. ways to improve the incident response process.
- C. potential attack vectors on the network perimeter.
- D. the optimum response to internal hacker attacks.

Correct Answer: A

An internal attack and penetration test are designed to identify weaknesses in network and server security. They do not



focus as much on incident response or the network perimeter.

QUESTION 4

When establishing metrics for an information security program, the BEST approach is to identify indicators that:

- A. support major information security initiatives.
- B. reflect the corporate risk culture.
- C. reduce information security program spending.
- D. demonstrate the effectiveness of the security program.

Correct Answer: D

QUESTION 5

Which would be one of the BEST metrics an information security manager can employ to effectively evaluate the results of a security program?

- A. Number of controls implemented
- B. Percent of control objectives accomplished
- C. Percent of compliance with the security policy
- D. Reduction in the number of reported security incidents

Correct Answer: B

Control objectives are directly related to business objectives; therefore, they would be the best metrics. Number of controls implemented does not have a direct relationship with the results of a security program. Percentage of compliance with the security policy and reduction in the number of security incidents are not as broad as choice B.

[Latest CISM Dumps](#)

[CISM VCE Dumps](#)

[CISM Exam Questions](#)