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 is MOST relevant for an information security manager to communicate to the board of directors?

A. Threat assessments

B. Vulnerability assessments

C. The level of exposure

D. The level of inherent risk

Correct Answer: D

QUESTION 2

The root cause of a successful cross site request forgery (XSRF) attack against an application is that the vulnerable application:

A. uses multiple redirects for completing a data commit transaction.

B. has implemented cookies as the sole authentication mechanism.

C. has been installed with a non-legitimate license key.

D. is hosted on a server along with other applications.

Correct Answer: B

XSRF exploits inadequate authentication mechanisms in web applications that rely only on elements such as cookies when performing a transaction. XSRF is related to an authentication mechanism, not to redirection. Option C is related to intellectual property rights, not to XSRF vulnerability. Merely hosting multiple applications on the same server is not the root cause of this vulnerability.

QUESTION 3

Which of the following would be the MOST effective incident response team structure for an organization with a large headquarters and worldwide branch offices?

A. Centralized

B. Coordinated

C. Outsourced

D. Decentralized

Correct Answer: B

QUESTION 4

From an information security perspective, information that no longer supports the main purpose of the business should be:

A. analyzed under the retention policy.

B. protected under the information classification policy.

C. analyzed under the backup policy.

D. protected under the business impact analysis (BIA).

Correct Answer: A

Option A is the type of analysis that will determine whether the organization is required to maintain the data for business, legal or regulatory reasons. Keeping data that are no longer required unnecessarily consumes resources, and, in the case of sensitive personal information, can increase the risk of data compromise. Options B. C and D are attributes that should be considered in the destruction and retention policy. A BIA could help determine that this information does not support the main objective of the business, but does not indicate the action to take.

QUESTION 5

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.