CISM$^{\text{Q\&As}}$

Certified Information Security Manager

Pass Isaca CISM Exam with 100% Guarantee

QUESTION 1

What should be the GREATEST concern for an information security manager of a large multinational organization when outsourcing data processing to a cloud service provider?

A. Local laws and regulations

B. Backup and restoration of data

C. Vendor service level agreements (SLAs)

D. Independent review of the vendor

Correct Answer: A

QUESTION 2

Which of the following is the MOST important driver when developing an effective information security strategy?

A. Information security standards

B. Business requirements

C. Benchmarking reports

D. Security audit reports

Correct Answer: B

QUESTION 3

Which of the following is a PRIMARY objective of an information security governance framework?

A. To provide the basis for action plans to achieve information security objectives organization-wide

B. To achieve the desired information security state as defined by business unit management

C. To align the relationships of stakeholders involved in developing and executing an information security strategy

D. To provide assurance that information assets are provided a level of protection proportionate to their inherent risk

Correct Answer: D

Reference: https://www.mossadams.com/articles/2021/08/information-security-governance-framework#:~:text=The%20goal%20of%20information%20security,IT%20strategies%20with%20organizational%20objectives

QUESTION 4

The systems administrator did not immediately notify the security officer about a malicious attack. An information security manager could prevent this situation by:

A. periodically testing the incident response plans.

B. regularly testing the intrusion detection system (IDS).

C. establishing mandatory training of all personnel.

D. periodically reviewing incident response procedures.

Correct Answer: A

Security incident response plans should be tested to find any deficiencies and improve existing processes. Testing the intrusion detection system (IDS) is a good practice but would not have prevented this situation. All personnel need to go through formal training to ensure that they understand the process, tools and methodology involved in handling security incidents. However, testing of the actual plans is more effective in ensuring the process works as intended. Reviewing the response procedures is not enough; the security response plan needs to be tested on a regular basis.

QUESTION 5

Phishing is BEST mitigated by which of the following?

A. Security monitoring software

B. Encryption

C. Two-factor authentication

D. User awareness

Correct Answer: D

Phishing can best be detected by the user. It can be mitigated by appropriate user awareness. Security monitoring software would provide some protection, but would not be as effective as user awareness. Encryption and two-factor authentication would not mitigate this threat.