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.pass4itsure.com/cism.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

A risk assessment study carried out by an organization noted that there is no segmentation of the local area network (LAN). Network segmentation would reduce the potential impact of which of the following?

A. Denial of service (DoS) attacks

B. Traffic sniffing

C. Virus infections

D. IP address spoofing

Correct Answer: B

Network segmentation reduces the impact of traffic sniffing by limiting the amount of traffic that may be visible on any one network segment. Network segmentation would not mitigate the risk posed by denial of service (DoS) attacks, virus infections or IP address spoofing since each of these would be able to traverse network segments.

QUESTION 2

An organization has detected sensitive data leakage caused by an employee of a third-party contractor. What is the BEST course of action to address this issue?

A. Activate the organization\\'s incident response plan

B. Include security requirements in outsourcing contracts

C. Terminate the agreement with the third-party contractor

D. Limit access to the third-party contractor

Correct Answer: A

QUESTION 3

Which of the following would help to change an organization\\'s security culture?

A. Develop procedures to enforce the information security policy

B. Obtain strong management support

C. Implement strict technical security controls

D. Periodically audit compliance with the information security policy

Correct Answer: B

Management support and pressure will help to change an organization\\'s culture. Procedures will support an information security policy, but cannot change the culture of the organization. Technical controls will provide more security to an information system and staff; however, this does not mean the culture will be changed. Auditing will help to ensure the effectiveness of the information security policy; however, auditing is not effective in changing the culture of the company.

QUESTION 4

During which phase of development is it MOST appropriate to begin assessing the risk of a new application system?

A. Feasibility

B. Design

C. Development

D. Testing

Correct Answer: A

Risk should be addressed as early in the development of a new application system as possible. In some cases, identified risks could be mitigated through design changes. If needed changes are not identified until design has already commenced, such changes become more expensive. For this reason, beginning risk assessment during the design, development or testing phases is not the best solution.

QUESTION 5

In which of the following system development life cycle (SDLC) phases are access control and encryption algorithms chosen?

A. Procedural design

B. Architectural design

C. System design specifications

D. Software development

Correct Answer: C

The system design specifications phase is when security specifications are identified. The procedural design converts structural components into a procedural description of the software. The architectural design is the phase that identifies the overall system design, hut not the specifics. Software development is too late a stage since this is the phase when the system is already being coded.