CISM$^{Q\&As}$

Certified Information Security Manager

Pass Isaca CISM Exam with 100% Guarantee

QUESTION 1

The FIRST step to create an internal culture that focuses on information security is to:

A. implement stronger controls.

B. conduct periodic awareness training.

C. actively monitor operations.

D. gain the endorsement of executive management.

Correct Answer: D

Endorsement of executive management in the form of policies provides direction and awareness. The implementation of stronger controls may lead to circumvention. Awareness training is important, but must be based on policies. Actively monitoring operations will not affect culture at all levels.

QUESTION 2

Which of the following should be the PRIMARY driver for selecting and implementing appropriate controls to address the risk associated with weak user passwords?

A. The organization\\'s risk tolerance

B. The organization\\'s culture

C. The cost of risk mitigation controls

D. Direction from senior management

Correct Answer: B

QUESTION 3

Business units within an organization are resistant to proposed changes to the information security program. Which of the following is the BEST way to address this issue?

A. Implementing additional security awareness training

B. Communicating critical risk assessment results to business unit managers

C. Including business unit representation on the security steering committee

D. Publishing updated information security policies

Correct Answer: B

QUESTION 4

Reviewing which of the following would be MOST helpful when a new information security manager is developing an information security strategy for a non-regulated organization?

A. Management\\'s business goals and objectives

B. Strategies of other non-regulated companies

C. Risk assessment results

D. Industry best practices and control recommendations

Correct Answer: A

QUESTION 5

Which of the following is the BEST approach for encouraging business units to assume their roles and responsibilities in an information security program?

A. Perform a risk assessment.

B. Conduct an awareness program.

C. Conduct a security audit.

D. Develop controls and countermeasures.

Correct Answer: B