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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which of the following is the BEST method to ensure the overall effectiveness of a risk management program?

A. User assessments of changes

B. Comparison of the program results with industry standards

C. Assignment of risk within the organization

D. Participation by all members of the organization

Correct Answer: D

Effective risk management requires participation, support and acceptance by all applicable members of the organization, beginning with the executive levels. Personnel must understand their responsibilities and be trained on how to fulfill their roles.

QUESTION 2

Calculation of the recovery time objective (RTO) is necessary to determine the:

A. time required to restore files

B. priority of restoration

C. point of synchronization

D. annual loss expectancy (ALE)

Correct Answer: B

QUESTION 3

Which of the following is necessary to determine what would constitute a disaster for an organization?

A. Recovery strategy analysis

B. Backup strategy analysis

C. Risk analysis

D. Threat probability analysis

Correct Answer: C

QUESTION 4

Who should determine the appropriate classification of accounting ledger data located on a database server and

maintained by a database administrator in the IT department?

A. Database administrator (DBA)

B. Finance department management

C. Information security manager

D. IT department management

Correct Answer: B

Data owners are responsible for determining data classification; in this case, management of the finance department would be the owners of accounting ledger data. The database administrator (DBA) and IT management are the custodians of the data who would apply the appropriate security levels for the classification, while the security manager would act as an advisor and enforcer.

QUESTION 5

To justify its ongoing security budget, which of the following would be of MOST use to the information security\\' department?

A. Security breach frequency

B. Annualized loss expectancy (ALE)

C. Cost-benefit analysis

D. Peer group comparison

Correct Answer: C

Cost-benefit analysis is the legitimate way to justify budget. The frequency of security breaches may assist the argument for budget but is not the key tool; it does not address the impact. Annualized loss expectancy (ALE) does not address the potential benefit of security investment. Peer group comparison would provide a good estimate for the necessary security budget but it would not take into account the specific needs of the organization.