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.lead4pass.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

Which of the following is the MOST effective way to ensure information security policies are followed?

A. Require sign-off on acceptable use policies.

B. Require regular security awareness training.

C. Provide detailed security procedures.

D. Perform a gap analysis.

Correct Answer: C

QUESTION 2

The FIRST step in developing an information security management program is to:

A. identify business risks that affect the organization.

B. clarify organizational purpose for creating the program.

C. assign responsibility for the program.

D. assess adequacy of controls to mitigate business risks.

Correct Answer: B

In developing an information security management program, the first step is to clarify the organization\\'s purpose for creating the program. This is a business decision based more on judgment than on any specific quantitative measures. After clarifying the purpose, the other choices are assigned and acted upon.

QUESTION 3

Spoofing should be prevented because it may be used to: A. assemble information, track traffic, and identify network vulnerabilities.

B. predict which way a program will branch when an option is presented.

C. gain illegal entry to a secure system by faking the sender\\'s address.

D. capture information such as password traveling through the network.

Correct Answer: C

QUESTION 4

The PRIMARY reason for involving information security at each stage in the systems development life cycle (SDLC) is to identify the security implications and potential solutions required for:

A. identifying vulnerabilities in the system.

B. sustaining the organization\\'s security posture.

C. the existing systems that will be affected.

D. complying with segregation of duties.

Correct Answer: B

It is important to maintain the organization\\'s security posture at all times. The focus should not be confined to the new system being developed or acquired, or to the existing systems in use. Segregation of duties is only part of a solution to improving the security of the systems, not the primary reason to involve security in the systems development life cycle (SDLC).

QUESTION 5

Nonrepudiation can BEST be ensured by using:

A. strong passwords.

B. a digital hash.

C. symmetric encryption.

D. digital signatures.

Correct Answer: D

Digital signatures use a private and public key pair, authenticating both parties. The integrity of the contents exchanged is controlled through the hashing mechanism that is signed by the private key of the exchanging party. A digital hash in itself helps in ensuring integrity of the contents, but not nonrepudiation.

Symmetric encryption wouldn\\'t help in nonrepudiation since the keys are always shared between parties. Strong passwords only ensure authentication to the system and cannot be used for nonrepudiation involving two or more parties.

QUESTION 6

Which of the following should be included in an annual information security budget that is submitted for management approval?

A. A cost-benefit analysis of budgeted resources

B. All of the resources that are recommended by the business

C. Total cost of ownership (TCO)

D. Baseline comparisons

Correct Answer: A

A brief of the benefit of expenditures in the budget helps to convey the context of how the purchases that are being

requested meet goals and objectives, which in turn helps build credibility for the information security function or program. Explanations of benefits also help engage senior management in the support of the information security program. While the budget should consider all inputs and recommendations that are received from the business, the budget that is ultimately submitted to management for approval should include only those elements that are intended for purchase. TCO may be requested by management and may be provided in an addendum to a given purchase request, but is not usually included in an annual budget. Baseline comparisons (cost comparisons with other companies or industries) may be useful in developing a budget or providing justification in an internal review for an individual purchase, but would not be included with a request for budget approval.

QUESTION 7

Risk assessment is MOST effective when performed:

A. at the beginning of security program development.

B. on a continuous basis.

C. while developing the business case for the security program.

D. during the business change process.

Correct Answer: B

Risk assessment needs to be performed on a continuous basis because of organizational and technical changes. Risk assessment must take into account all significant changes in order to be effective.

QUESTION 8

Which of the following BEST contributes to the successful management of security incidents?

A. Established procedures

B. Established policies

C. Tested controls

D. Current technologies

Correct Answer: B

QUESTION 9

Which of the following would BEST help to ensure the alignment between information security and business functions?

A. Establishing an information security governance committee

B. Developing information security policies

C. Providing funding for information security efforts

D. Establishing a security awareness program

Correct Answer: A

QUESTION 10

A third-party service provider is developing a mobile app for an organization\\'s customers.

Which of the following issues should be of GREATEST concern to the information security manager?

A. Software escrow is not addressed in the contract.

B. The contract has no requirement for secure development practices.

C. The mobile app\\'s programmers are all offshore contractors.

D. SLAs after deployment are not clearly defined.

Correct Answer: B

QUESTION 11

Which of the following should be determined FIRST when establishing a business continuity program?

A. Cost to rebuild information processing facilities

B. Incremental daily cost of the unavailability of systems

C. Location and cost of offsite recovery facilities

D. Composition and mission of individual recovery teams

Correct Answer: B

Prior to creating a detailed business continuity plan, it is important to determine the incremental daily cost of losing different systems. This will allow recovery time objectives to be determined which, in turn, affects the location and cost of offsite recovery facilities, and the composition and mission of individual recovery teams. Determining the cost to rebuild information processing facilities would not be the first thing to determine.

QUESTION 12

Risk management programs are designed to reduce risk to:

A. a level that is too small to be measurable.

B. the point at which the benefit exceeds the expense.

C. a level that the organization is willing to accept.

D. a rate of return that equals the current cost of capital.

Correct Answer: C

Risk should be reduced to a level that an organization is willing to accept. Reducing risk to a level too small to measure is impractical and is often cost-prohibitive. To tie risk to a specific rate of return ignores the qualitative aspects of risk that must also be considered. Depending on the risk preference of an organization, it may or may not choose to pursue risk mitigation to the point at which the benefit equals or exceeds the expense. Therefore, choice C is a more precise answer.

QUESTION 13

Which of the following has the MOST direct impact on the usability of an organization\\'s asset classification program?

A. The granularity of classifications in the hierarchy

B. The frequency of updates to the organization\\'s risk register

C. The business objectives of the organization

D. The support of senior management for the classification scheme

Correct Answer: A