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.leads4pass.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

Security audit reviews should PRIMARILY:

A. ensure that controls operate as required.

B. ensure that controls are cost-effective.

C. focus on preventive controls.

D. ensure controls are technologically current.

Correct Answer: A

The primary objective of a security review or audit should be to provide assurance on the adequacy of security controls. Reviews should focus on all forms of control, not just on preventive control. Cost-effectiveness and technological currency are important but not as critical.

QUESTION 2

Which of the following is MOST important for an information security manager to verify when selecting a third-party forensics provider?

A. Technical capabilities of the provider

B. Existence of the provider\\'s incident response plan

C. Results of the provider\\'s business continuity tests

D. Existence of a right-to-audit clause

Correct Answer: A

QUESTION 3

The chief information security officer (CISO) has developed an information security strategy, but is struggling to obtain senior management commitment for funds to implement the strategy.

Which of the following is the MOST likely reason?

A. The strategy does not include a cost-benefit analysis.

B. The CISO reports to the CIO.

C. There was a lack of engagement with the business during development.

D. The strategy does not comply with security standards.

Correct Answer: A

QUESTION 4

Priority should be given to which of the following to ensure effective implementation of information security governance?

A. Consultation

B. Negotiation

C. Facilitation

D. Planning

Correct Answer: D

Planning is the key to effective implementation of information security governance. Consultation, negotiation and facilitation come after planning.

QUESTION 5

An information security manager has contracted with a company to design security architecture for an application. Which of the following is accountable for identification associated with this initiative?

A. The project steering committee

B. The information security manager

C. The infrastructure management team

D. The application development team

Correct Answer: B

Reference: https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/toolkits/information-security-governance

QUESTION 6

Management decisions concerning information security investments will be MOST effective when they are based on:

A. an annual loss expectancy (ALE) determined from the history of security events.

B. the formalized acceptance of risk analysis by management.

C. the reporting of consistent and periodic assessments of risks.

D. a process for identifying and analyzing threats and vulnerabilities.

Correct Answer: C

QUESTION 7

Which of the following would help management determine the resources needed to mitigate a risk to the organization?

A. Risk analysis process

B. Business impact analysis (BIA)

C. Risk management balanced scorecard

D. Risk-based audit program

Correct Answer: B

The business impact analysis (BIA) determines the possible outcome of a risk and is essential to determine the appropriate cost of control. The risk analysis process provides comprehensive data, but does not determine definite resources to mitigate the risk as does the BIA. The risk management balanced scorecard is a measuring tool for goal attainment. A risk-based audit program is used to focus the audit process on the areas of greatest importance to the organization.

QUESTION 8

The PRIMARY goal of the eradication phase in an incident response process is to:

A. provide effective triage and containment of the incident.

B. remove the threat and restore affected systems.

C. maintain a strict chain of custody.

D. obtain forensic evidence from the affected system.

Correct Answer: B

QUESTION 9

The use of a business case to obtain funding for an information security investment is MOST effective when the business case:

A. relates information security policies and standards into business requirements

B. relates the investment to the organization\\'s strategic plan.

C. realigns information security objectives to organizational strategy.

D. articulates management\\'s intent and information security directives in clear language.

Correct Answer: B

QUESTION 10

Which of the following BEST ensures timely and reliable access to services?

A. Authenticity

B. Recovery time objective

C. Availability

D. Nonrepudiation

Correct Answer: C

Reference: https://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf

QUESTION 11

When segregation of duties concerns exists between IT support staff and end users, what would be a suitable compensating control?

A. Restricting physical access to computing equipment

B. Reviewing transaction and application logs

C. Performing background checks prior to hiring IT staff

D. Locking user sessions after a specified period of inactivity

Correct Answer: B

Only reviewing transaction and application logs directly addresses the threat posed by poor segregation of duties. The review is a means of detecting inappropriate behavior and also discourages abuse, because people who may otherwise be tempted to exploit the situation are aware of the likelihood of being caught. Inadequate segregation of duties is more likely to be exploited via logical access to data and computing resources rather than physical access. Choice C is a useful control to ensure IT staff are trustworthy and competent but does not directly address the lack of an optimal segregation of duties. Choice D acts to prevent unauthorized users from gaining system access, but the issue of a lack of segregation of duties is more the misuse (deliberately or inadvertently} of access privileges that have officially been granted.

QUESTION 12

Which of the following is the MOST important reason to conduct interviews as part of the business impact analysis (BIA) process?

A. To facilitate a qualitative risk assessment following the BIA

B. To increase awareness of information security among key stakeholders

C. To ensure the stakeholders providing input own the related risk

D. To obtain input from as many relevant stakeholders as possible

Correct Answer: D

Reference: https://www.techtarget.com/searchstorage/definition/business-impact-analysis#:~:text=A%20business%20impact%20analysis%20(BIA)%20is%20a%20systematic%20process%20to,a%20disaster%2C%20accident%20or%

20emergency

QUESTION 13

When electronically stored information is requested during a fraud investigation, which of the following should be the FIRST priority?

A. Assigning responsibility for acquiring the data

B. Locating the data and preserving the integrity of the data

C. Creating a forensically sound image

D. Issuing a litigation hold to all affected parties

Correct Answer: B

Locating the data and preserving data integrity is the only correct answer because it represents the primary responsibility of an investigator and is a complete and accurate statement of the first priority. While assigning responsibility for acquiring the data is a step that should be taken, it is not the first step or the highest priority. Creating a forensically sound image may or may not be a necessary step, depending on the type of investigation, but it would never be the first priority. Issuing a litigation hold to all affected parties might be a necessary step early on in an investigation of certain types, but not the first priority.

QUESTION 14

For the information security manager, integrating the various assurance functions of an organization is important PRIMARILY to enable:

A. consistent security.

B. a security-aware culture.

C. compliance with policy.

D. comprehensive audits.

Correct Answer: D

QUESTION 15

During an incident, which of the following entities would MOST likely be contacted directly by an organization\\'s incident response team without management approval?

A. Industry regulators

B. Technology vendor

C. Law enforcement

D. Internal audit

Correct Answer: D