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.passapply.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 BEST describes the scope of risk analysis?

A. Key financial systems

B. Organizational activities

C. Key systems and infrastructure

D. Systems subject to regulatory compliance

Correct Answer: B

Risk analysis should include all organizational activities. It should not be limited to subsets of systems or just systems and infrastructure.

QUESTION 2

What is the FIRST line of defense against criminal insider activities?

A. Stringent and enforced access controls

B. Monitoring employee activities

C. Validating the integrity of personnel

D. Signing security agreements by critical personnel

Correct Answer: C

QUESTION 3

Which of the following is the BEST indication of an effective information security awareness training program?

A. An increase in the frequency of phishing tests

B. An increase in positive user feedback

C. An increase in the speed of incident resolution

D. An increase in the identification rate during phishing simulations

Correct Answer: D

QUESTION 4

Which of the following would provide the BEST justification for a new information security investment?

A. Results of a comprehensive threat analysis.

B. Projected reduction in risk.

C. Senior management involvement in project prioritization.

D. Defined key performance indicators (KPIs)

Correct Answer: A

QUESTION 5

When creating an information security governance program, which of the following will BEST enable the organization to address regulatory compliance requirements?

A. Guidelines for processes and procedures

B. A security control framework

C. An approved security strategy plan

D. Input from the security steering committee

Correct Answer: A

QUESTION 6

Which of the following is MOST important to the effectiveness of an information security steering committee?

A. The committee has strong representation from IT

B. The committee has strong regulatory knowledge

C. The committee has cross-organizational representation

D. The committee is driven by industry best practices

Correct Answer: C

QUESTION 7

An incident management team is alerted to a suspected security event. Before classifying the suspected event as a security incident, it is MOST important for the security manager to:

A. conduct an incident forensic analysis.

B. fallow the incident response plan

C. notify the business process owner.

D. fallow the business continuity plan (BCP).

Correct Answer: C

QUESTION 8

Which of the following BEST promotes stakeholder accountability in the management of information security risks?

A. Targeted security procedures

B. Establishment of information ownership

C. Establishment of security baselines

D. Regular reviews for noncompliance

Correct Answer: B

QUESTION 9

Human resources (HR) is evaluating potential Software as a Service (SaaS) cloud services. Which of the following should the information security manager do FIRST to support this effort?

A. Conduct a security audit on the cloud service providers.

B. Perform a cost-benefit analysis of using cloud services.

C. Review the cloud service providers\\' controls reports.

D. Perform a risk assessment of adopting cloud services.

Correct Answer: D

Performing a risk assessment is the responsibility of the information security manager.

QUESTION 10

Which of the following Is MOST useful to an information security manager when conducting a post-incident review of an attack?

A. Cost of the attack to the organization

B. Location of the attacker

C. Method of operation used by the attacker

D. Details from intrusion detection system (IDS) logs

Correct Answer: C

QUESTION 11

Which of the following would be the MOST effective incident response team structure for an organization with a large headquarters and worldwide branch offices?

A. Centralized

B. Coordinated

C. Outsourced

D. Decentralized

Correct Answer: B

QUESTION 12

An organization is implementing an information security governance framework. To communicate the program\\'s effectiveness to stakeholders, it is MOST important to establish:

A. automated reporting to stakeholders.

B. a control self-assessment process.

C. metrics for each milestone.

D. a monitoring process for the security policy.

Correct Answer: C

QUESTION 13

Which of the following should be an information security manager\\'s FIRST course of action following a decision to implement a new technology?

A. Determine security controls needed to support the new technology.

B. Perform a business impact analysis (BIA) on the new technology.

C. Perform a return-on-investment (ROI) analysis for the new technology.

D. Determine whether the new technology will comply with regulatory requirements.

Correct Answer: B

QUESTION 14

Implementing a strong password policy is part of an organization\\'s information security strategy for the year. A business unit believes the strategy may adversely affect a client\\'s adoption of a recently developed mobile application and has decided not to implement the policy.

Which of the following is the information security manager\\'s BEST course of action?

A. Analyze the risk and impact of not implementing the policy.

B. Develop and implement a password policy for the mobile application.

C. Escalate non-implementation of the policy to senior management.

D. Benchmark with similar mobile applications to identify gaps.

Correct Answer: C

QUESTION 15

Which of the following would be the MOST effective incident response team structure for an organization with a large headquarters and worldwide branch offices?

A. Centralized

B. Coordinated

C. Outsourced

D. Decentralized

Correct Answer: B