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

When a large organization discovers that it is the subject of a network probe, which of the following actions should be taken?

A. Reboot the router connecting the DMZ to the firewall

B. Power down all servers located on the DMZ segment

C. Monitor the probe and isolate the affected segment

D. Enable server trace logging on the affected segment

Correct Answer: C

In the case of a probe, the situation should be monitored and the affected network segment isolated. Rebooting the router, powering down the demilitarized zone (DMZ) servers and enabling server trace routing are not warranted.

QUESTION 2

The PRIMARY benefit of integrating information security risk into enterprise risk management is to:

A. ensure timely risk mitigation.

B. justify the information security budget.

C. obtain senior management\\'s commitment.

D. provide a holistic view of risk.

Correct Answer: D

QUESTION 3

Which of the following is the PRIMARY reason for executive management to be involved in establishing an enterprise\\'s security management framework?

A. To determine the desired state of enterprise security

B. To establish the minimum level of controls needed

C. To satisfy auditors\\' recommendations for enterprise security

D. To ensure industry best practices for enterprise security are followed

Correct Answer: A

QUESTION 4

Reviewing which of the following would provide the GREATEST input to the asset classification process?

A. Risk assessment

B. Replacement cost of the asset

C. Sensitivity of the data

D. Compliance requirements

Correct Answer: C

QUESTION 5

A recent application security assessment identified a number of low- and medium-level vulnerabilities. Which of the following stakeholders is responsible for deciding the appropriate risk treatment option?

A. Security manager

B. Chief information security officer (CISO)

C. System administrator

D. Business owner

Correct Answer: B

Verified Answer: According to the CISM Review Manual, 15th Edition, Chapter 3, Section 3.2.1.3, "The appropriate risk treatment option is decided by the chief information security officer (CISO) or the designated risk owner."1 Comprehensive and Detailed The CISO is the senior executive who is responsible for overseeing and managing the information security program of an organization. The CISO has the authority and expertise to assess the risks, determine the risk appetite and tolerance levels, and select the most suitable risk treatment options for each risk. The CISO also has the accountability and responsibility for implementing, monitoring, and reporting on the risk treatment activities. References: 1: CISM Review Manual, 15th Edition, Chapter 3, Section 3.2.1.3

QUESTION 6

A web server in a financial institution that has been compromised using a super-user account has been isolated, and proper forensic processes have been followed. The next step should be to:

A. rebuild the server from the last verified backup.

B. place the web server in quarantine.

C. shut down the server in an organized manner.

D. rebuild the server with original media and relevant patches.

Correct Answer: D

The original media should be used since one can never be sure of all the changes a super-user may have made nor the timelines in which these changes were made. Rebuilding from the last known verified backup is incorrect since the verified backup may have been compromised by the super-user at a different time. Placing the web server in quarantine

should have already occurred in the forensic process. Shut down in an organized manner is out of sequence and no longer a problem. The forensic process is already finished and evidence has already been acquired.

QUESTION 7

Which of the following is the MOST effective, positive method to promote security awareness?

A. Competitions and rewards for compliance

B. Lock-out after three incorrect password attempts

C. Strict enforcement of password formats

D. Disciplinary action for noncompliance

Correct Answer: A

Competitions and rewards are a positive encouragement to user participation in the security program. Merely locking users out for forgetting their passwords does not enhance user awareness. Enforcement of password formats and disciplinary actions do not positively promote awareness.

QUESTION 8

Which of the following BEST enables an incident response team to determine appropriate actions during an initial investigation?

A. Feedback from affected departments

B. Historical data from past incidents

C. Technical capabilities of the team

D. Procedures for incident triage

Correct Answer: D

QUESTION 9

Several significant risks have been identified after a centralized risk register was compiled and prioritized. The information security manager\\'s most important action is to:

A. provide senior management with risk treatment options.

B. design and implement controls to reduce the risk.

C. consult external third parties on how to treat the risk.

D. ensure that employees are aware of the risk.

Correct Answer: A

QUESTION 10

Which of the following is MOST important for the effectiveness of an incident response function?

A. Enterprise security management system and forensic tools.

B. Establishing prior contacts with law enforcement

C. Training of all users on when and how to report

D. Automated incident tracking and reporting tools

Correct Answer: A

QUESTION 11

, page

A.

B.

C.

D.

Correct Answer:

QUESTION 12

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 13

Which of the following is MOST important when designing security controls for new cloud- based services?

A. Evaluating different types of deployment models according to the associated risks

B. Understanding the business and IT strategy for moving resources to the cloud

C. Defining an incident response policy to protect data moving between onsite and cloud applications

D. Performing a business impact analysis (BIA) to gather information needed to develop recovery strategies

Correct Answer: B

The most important factor when designing security controls for new cloud-based services is to understand the business and IT strategy for moving resources to the cloud. This will help to align the security controls with the business objectives,

requirements, and risks, and to select the appropriate cloud service delivery and deployment models. The security controls should also be based on the shared responsibility model, which defines the roles and responsibilities of the cloud

service provider and the cloud customer in ensuring the security of the cloud environment. Evaluating different types of deployment models, defining an incident response policy, and performing a business impact analysis are also important

activities, but they should be done after understanding the business and IT strategy.

References: CISM Review Manual, 16th Edition eBook1, Chapter 3: Information Security Program Development and Management, Section: Information Security Program Management, Subsection: Cloud Computing, Page 141-142.

QUESTION 14

Network isolation techniques are immediately implemented after a security breach to:

A. preserve evidence as required for forensics

B. reduce the extent of further damage.

C. allow time for key stakeholder decision making.

D. enforce zero trust architecture principles.

Correct Answer: B

Network isolation techniques are immediately implemented after a security breach to reduce the extent of further damage by limiting the access and communication of the compromised systems or networks with the rest of the environment. This can help prevent the spread of malware, the exfiltration of data, or the escalation of privileges by the attackers. Network isolation techniques can include disconnecting the affected systems or networks from the internet, blocking or filtering certain ports or protocols, or creating separate VLANs or subnets for the isolated systems or networks. Network isolation techniques are part of the incident response process and should be performed as soon as possible after detecting a security breach. References: CISM Review Manual 15th Edition, page 308-3091; CISM Review Questions, Answers and Explanations Database - 12 Month Subscription, Question ID: 1162

QUESTION 15

An organization has implemented a new customer relationship management (CRM) system. Who should be responsible for enforcing authorized and controlled access to the CRM data?

A. The information security manager

B. The data custodian

C. Internal IT audit

D. The data owner

Correct Answer: B

The data custodian is the person or role who is responsible for enforcing authorized and controlled access to the CRM data, according to the security policies and standards defined by the data owner. The data custodian implements and maintains the technical and operational controls, such as authentication, authorization, encryption, backup, and recovery, to protect the data from unauthorized access, modification, disclosure, or destruction. The data custodian also monitors and reports on the data access activities and incidents. References: Setting Up Access Controls and Permissions in Your CRM, Accountability for Information Security Roles and Responsibilities, Part 1, How to Meet the Shared Responsibility Model with CIS