Vendor: Isaca

Exam Code:CISM

Exam Name: Certified Information Security Manager

Version: Demo

QUESTION 1

Which of the following is the MOST important incident management consideration for an organization subscribing to a cloud service?

A. Decision on the classification of cloud-hosted data

B. Expertise of personnel providing incident response

C. Implementation of a SIEM in the organization

D. An agreement on the definition of a security incident

Correct Answer: D

QUESTION 2

An organization utilizes a third party to classify its customers\\' personally identifiable information (PII). What is the BEST way to hold the third party accountable for data leaks?

A. Include detailed documentation requirements within the formal statement of work.

B. Submit a formal request for proposal (RFP) containing detailed documentation of requirements.

C. Ensure a nondisclosure agreement is signed by both parties\\' senior management.

D. Require the service provider to sign off on the organization\\'s acceptable use policy.

Correct Answer: A

QUESTION 3

Which of the following is the GREATEST benefit of integrating information security program requirements into vendor management?

A. The ability to reduce risk in the supply chain

B. The ability to meet industry compliance requirements

C. The ability to define service level agreements (SLAs)

D. The ability to improve vendor performance

Correct Answer: A

QUESTION 4

Which of the following is the BEST indication of information security strategy alignment with the business?

A. Number of business objectives directly supported by information security initiatives.

B. Percentage of corporate budget allocated to information security initiatives.

C. Number of business executives who have attended information security awareness sessions.

D. Percentage of information security incidents resolved within defined service level agreements.

Correct Answer: A

QUESTION 5

An incident response team recently encountered an unfamiliar type of cyber event. Though the team was able to resolve the issue, it took a significant amount of time to identify. What is the BEST way to help ensure similar incidents are identified more quickly in the future?

A. Establish performance metrics for the team.

B. Perform a post-incident review.

C. Perform a threat analysis.

D. Implement a SIEM solution.

Correct Answer: B

QUESTION 6

What information is MOST helpful in demonstrating to senior management how information security governance aligns with business objectives?

A. Updates on information security projects in development

B. Drafts of proposed policy changes

C. Metrics of key information security deliverables

D. A list of monitored threats, risks, and exposures

Correct Answer: C

QUESTION 7

Which of the following presents the GREATEST challenge to the recovery of critical systems and data following a ransomware incident?

A. Lack of encryption for backup data in transit

B. Undefined or undocumented backup retention policies

C. Ineffective alert configurations for backup operations

D. Unavailable or corrupt data backups

Correct Answer: D

According to the Certified Information Security Manager (CISM) Study Guide, the greatest challenge to the recovery of critical systems and data following a ransomware incident is the availability and integrity of backups. If the backups are unavailable or corrupt, it becomes much more difficult, if not impossible, to recover the systems and data. This highlights the importance of regularly testing and verifying the backup and recovery process to ensure that the backups are available and can be used in the event of an incident. Additionally, it is important to ensure that backups are stored securely and off-line to prevent them from being encrypted or deleted by an attacker.

QUESTION 8

The PRIMARY advantage of challenge-response authentication over password authentication is that:

A. user accounts are less likely to be compromised

B. credentials sent across the network are encrypted

C. there is no requirement for end-to-end encryption

D. it is less expensive to implement

Correct Answer: A

QUESTION 9

Of the following, who should have PRIMARY responsibility for assessing the security risk associated with an outsourced cloud provider contract?

A. Information security manager

B. Compliance manager

C. Chief information officer

D. Service delivery manager

Correct Answer: D

QUESTION 10

Which of the following BEST validates that security controls are implemented in a new business process?

A. Assess the process according to information security policy.

B. Benchmark the process against industry practices.

C. Verify the use of a recognized control framework.

D. Review the process for conformance with information security best practices.

Correct Answer: A

QUESTION 11

Reviewing which of the following would BEST ensure that security controls are effective?

A. Risk assessment policies

B. Return on security investment

C. Security metrics

D. User access rights

Correct Answer: C

Reviewing security metrics provides senior management a snapshot view and trends of an organization\\'s security posture. Choice A is incorrect because reviewing risk assessment policies would not ensure that the controls are actually working. Choice B is incorrect because reviewing returns on security investments provides business justifications in implementing controls, but does not measure effectiveness of the control itself. Choice D is incorrect because reviewing user access rights is a joint responsibility of the data custodian and the data owner, and does not measure control effectiveness.

QUESTION 12

Information security managers should use risk assessment techniques to:

A. justify selection of risk mitigation strategies.

B. maximize the return on investment (ROD.

C. provide documentation for auditors and regulators.

D. quantify risks that would otherwise be subjective.

Correct Answer: A

Information security managers should use risk assessment techniques to justify and implement a risk mitigation strategy as efficiently as possible. None of the other choices accomplishes that task, although they are important components.