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

Which of the following if the MOST significant advantage of developing a well-defined information security strategy?

A. Support for buy-in from organizational employees

B. Allocation of resources to highest priorities

C. Prevention of deviations from risk tolerance thresholds

D. Increased maturity of incident response processes

Correct Answer: D

QUESTION 2

The MAIN goal of an information security strategic plan is to:

A. develop a risk assessment plan.

B. develop a data protection plan.

C. protect information assets and resources.

D. establish security governance.

Correct Answer: C

The main goal of an information security strategic plan is to protect information assets and resources. Developing a risk assessment plan and H data protection plan, and establishing security governance refer to tools utilized in the security strategic plan that achieve the protection of information assets and resources.

QUESTION 3

An information security manager has identified that privileged employee access requests to production servers are approved; but user actions are not logged. Which of the following should be the GREATEST concern with this situation?

A. Lack of availability

B. Lack of accountability

C. Improper authorization

D. Inadequate authentication

Correct Answer: B

Explanation: The greatest concern with the situation of privileged employee access requests to production servers being

approved but not logged is the lack of accountability, which means the inability to trace or verify the actions and decisions of the privileged users. Lack of accountability can lead to security risks such as unauthorized changes, data breaches, fraud, or misuse of privileges. Logging user actions is a key component of privileged access management (PAM), which helps to monitor, detect, and prevent unauthorized privileged access to critical resources. The other options, such as lack of availability, improper authorization, or inadequate authentication, are not directly related to the situation of not logging user actions. References: https://www.microsoft.com/en-us/security/business/security-101/what-is-privileged- access-management- pam https://www.ekransystem.com/en/blog/privileged-user-monitoring-best-practices https:// www.beyondtrust.com/resources/glossary/privileged-access-management- pam

QUESTION 4

The risk of mishandling alerts identified by an intrusion detection system (IDS) would be the GREATEST when:

A. standard operating procedures are not formalized.

B. the IT infrastructure is diverse.

C. IDS sensors are misconfigured.

D. operations and monitoring are handled by different teams.

Correct Answer: A

QUESTION 5

An information security team is planning a security assessment of an existing vendor. Which of the following approaches is MOST helpful for properly scoping the assessment?

A. Focus the review on the infrastructure with the highest risk

B. Review controls listed in the vendor contract

C. Determine whether the vendor follows the selected security framework rules

D. Review the vendor\\'s security policy

Correct Answer: B

Explanation: Reviewing controls listed in the vendor contract is the most helpful approach for properly scoping the security assessment of an existing vendor because it helps to determine the security requirements and expectations that the vendor has agreed to meet. A vendor contract is a legal document that defines the terms and conditions of the business relationship between the organization and the vendor, including the scope, deliverables, responsibilities, and obligations of both parties. A vendor contract should also specify the security controls that the vendor must implement and maintain to protect the organization\\'s data and systems, such as encryption, authentication, access control, backup, monitoring, auditing, etc. Reviewing controls listed in the vendor contract helps to ensure that the security assessment covers all the relevant aspects of the vendor\\'s security posture, as well as to identify any gaps or discrepancies between the contract and the actual practices. Therefore, reviewing controls listed in the vendor contract is the correct answer. References: https://medstack.co/blog/vendor-security-assessments-understanding-the-basics/ https:// www.ncsc.gov.uk/files/NCSC-Vendor-Security-Assessment.pdf https://securityscorecard.com/blog/how-to-conduct-vendor-security-assessment

CISM VCE Dumps CISM Study Guide CISM Exam Questions