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.geekcert.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

An organization has acquired a new system with strict maintenance instructions and schedules. Where should this information be documented?

A. Standards

B. Policies

C. Guidelines

D. Procedures

Correct Answer: D

Procedures are the detailed steps or instructions for performing specific tasks or activities. They are usually aligned with standards, policies and guidelines, but they are more specific and prescriptive. System maintenance instructions and schedules are examples of procedures that should be documented and followed to ensure the proper functioning and security of the system. References: The CISM Review Manual 2023 defines procedures as "the lowest level in the hierarchy of documentation. They are detailed steps that a user must follow to accomplish an activity" (p. 80). The CISM Item Development Guide also provides the following explanation for this answer: "Procedures are the correct answer because they provide the specific steps to be followed to maintain the system" (p. 11).

QUESTION 2

Which of the following trends would be of GREATEST concern when reviewing the performance of an organization\\'s intrusion detection systems (IDSs)?

A. Decrease in false positives

B. Increase in false positives

C. Increase in false negatives

D. Decrease in false negatives

Correct Answer: C

An increase in false negatives would be of greatest concern when reviewing the performance of an organization\\'s IDSs, because it means that the IDSs are failing to detect and alert on actual attacks that are occurring on the network. False negatives can lead to serious security breaches, data loss, reputational damage, and legal liabilities for the organization. False positives, on the other hand, are alerts that are triggered by benign or normal activities that are mistaken for attacks. False positives can cause annoyance, inefficiency, and desensitization, but they do not pose a direct threat to the security of the network. Therefore, a decrease in false positives would be desirable, and an increase in false positives would be less concerning than an increase in false negatives. References: CISM Review Manual, 16th Edition, page 2231; Intrusion Detection Systems | NIST

QUESTION 3

To justify the establishment of an incident management team, an information security manager would find which of the following to be the MOST effective?

A. Assessment of business impact of past incidents

B. Need of an independent review of incident causes

C. Need for constant improvement on the security level

D. Possible business benefits from incident impact reduction

Correct Answer: D

Business benefits from incident impact reduction would be the most important goal for establishing an incident management team. The assessment of business impact of past incidents would need to be completed to articulate the benefits. Having an independent review benefits the incident management process. The need for constant improvement on the security level is a benefit to the organization.

QUESTION 4

A validated patch to address a new vulnerability that may affect a mission-critical server has been released.

What should be done immediately?

A. Add mitigating controls.

B. Check the server\\'s security and install the patch.

C. Conduct an impact analysis.

D. Take the server off-line and install the patch.

Correct Answer: C

QUESTION 5

Which of the following environments represents the GREATEST risk to organizational security?

A. Locally managed file server

B. Enterprise data warehouse

C. Load-balanced, web server cluster

D. Centrally managed data switch

Correct Answer: A

A locally managed file server will be the least likely to conform to organizational security policies because it is generally subject to less oversight and monitoring. Centrally managed data switches, web server clusters and data warehouses are subject to close scrutiny, good change control practices and monitoring.