712-50 Q&As

EC-Council Certified CISO (CCISO)

Pass EC-COUNCIL 712-50 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/712-50.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

Instant Download After Purchase
100% Money Back Guarantee
365 Days Free Update
800,000+ Satisfied Customers

QUESTION 1

Scenario: A Chief Information Security Officer (CISO) recently had a third party conduct an audit of the security program. Internal policies and international standards were used as audit baselines. The audit report was presented to the CISO and a variety of high, medium and low rated gaps were identified. The CISO has validated audit findings, determined if compensating controls exist, and started initial remediation planning.

Which of the following is the MOST logical next step?

A. Create detailed remediation funding and staffing plans

B. Report the audit findings and remediation status to business stake holders

C. Validate the effectiveness of current controls

D. Review security procedures to determine if they need modified according to findings

Correct Answer: C

The most logical next step in this scenario would be option C: Validate the effectiveness of current controls. After identifying the gaps in the security program through the audit, it is essential to verify whether the existing controls are effectively

addressing the identified risks or if further adjustments are necessary. This validation helps ensure that the controls are providing the intended level of protection and mitigating the identified vulnerabilities.

In summary, validating the effectiveness of current controls is the most logical next step as it ensures that the existing controls are providing the intended level of protection. This step provides a solid foundation for creating detailed

remediation plans (option A) and reporting to business stakeholders (option B), while reviewing security procedures (option D) comes later in the process.

QUESTION 2

A Security Operations Manager is finding it difficult to maintain adequate staff levels to monitor security operations during off-hours. To reduce the impact of staff shortages and increase coverage during off-hours, the SecOps manager is considering outsourcing off-hour coverage.

What Security Operations Center (SOC) model does this BEST describe?

A. Virtual SOC

B. In-house SOC

C. Security Network Operations Center (SNOC)

D. Hybrid SOC

Correct Answer: D

Reference: https://www.techtarget.com/searchsecurity/tip/Benefits-of-virtual-SOCs-Enterprise-run-vs-fully-managed

QUESTION 3

You work as a project manager for TYU project. You are planning for risk mitigation. You need to quickly identify high-level risks that will need a more in-depth analysis.

Which one of the following approaches would you use?

A. Risk mitigation

B. Estimate activity duration

C. Quantitative analysis

D. Qualitative analysis

Correct Answer: D

QUESTION 4

Scenario: The new CISO was informed of all the Information Security projects that the section has in progress. Two projects are over a year behind schedule and way over budget. Which of the following will be most helpful for getting an Information Security project that is behind schedule back on schedule?

A. Upper management support

B. Involve internal audit

C. More frequent project milestone meetings

D. More training of staff members

Correct Answer: A

QUESTION 5

What are the common data hiding techniques used by criminals?

A. Unallocated space and masking

B. Website defacement and log manipulation

C. Disabled Logging and admin elevation

D. Encryption, Steganography, and Changing Metadata/Timestamps

Correct Answer: D

Reference: https://cisomag.eccouncil.org/challenges-and-applications-of-digital-forensics/

712-50 Practice Test 712-50 Study Guide 712-50 Braindumps