512-50$^{\text{Q\&As}}$

EC-Council Information Security Manager (E|ISM)

Pass EC-COUNCIL 512-50 Exam with 100% Guarantee

QUESTION 1

Which business stakeholder is accountable for the integrity of a new information system?

A. CISO

B. Compliance Officer

C. Project manager

D. Board of directors

Correct Answer: A

QUESTION 2

Scenario: You are the CISO and have just completed your first risk assessment for your organization. You find many risks with no security controls, and some risks with inadequate controls. You assign work to your staff to create or adjust

existing security controls to ensure they are adequate for risk mitigation needs.

When formulating the remediation plan, what is a required input?

A. Board of directors

B. Risk assessment

C. Patching history

D. Latest virus definitions file

Correct Answer: B

QUESTION 3

What role should the CISO play in properly scoping a PCI environment?

A. Validate the business units\\' suggestions as to what should be included in the scoping process

B. Work with a Qualified Security Assessor (QSA) to determine the scope of the PCI environment

C. Ensure internal scope validation is completed and that an assessment has been done to discover all credit card data

D. Complete the self-assessment questionnaire and work with an Approved Scanning Vendor (ASV) to determine scope

Correct Answer: C

QUESTION 4

One of your executives needs to send an important and confidential email. You want to ensure that the message cannot be read by anyone but the recipient. Which of the following keys should be used to encrypt the message?

A. Your public key

B. The recipient\\'s private key

C. The recipient\\'s public key

D. Certificate authority key

Correct Answer: C

QUESTION 5

Scenario: Your corporate systems have been under constant probing and attack from foreign IP addresses for more than a week. Your security team and security infrastructure have performed well under the stress. You are confident that your defenses have held up under the test, but rumors are spreading that sensitive customer data has been stolen and is now being sold on the Internet by criminal elements. During your investigation of the rumored compromise you discover that data has been breached and you have discovered the repository of stolen data on a server located in a foreign country. Your team now has full access to the data on the foreign server.

Your defenses did not hold up to the test as originally thought. As you investigate how the data was compromised through log analysis you discover that a hardworking, but misguided business intelligence analyst posted the data to an obfuscated URL on a popular cloud storage service so they could work on it from home during their off-time.

Which technology or solution could you deploy to prevent employees from removing corporate data from your network? Choose the BEST answer.

A. Security Guards posted outside the Data Center

B. Data Loss Prevention (DLP)

C. Rigorous syslog reviews

D. Intrusion Detection Systems (IDS)

Correct Answer: B