512-50 Q&As

EC-Council Information Security Manager (E|ISM)

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

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

https://www.pass4itsure.com/512-50.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Scenario: An organization has made a decision to address Information Security formally and consistently by adopting established best practices and industry standards. The organization is a small retail merchant but it is expected to grow to a global customer base of many millions of customers in just a few years.

Which of the following would be the FIRST step when addressing Information Security formally and consistently in this organization?

A. Contract a third party to perform a security risk assessment

B. Define formal roles and responsibilities for Internal audit functions

C. Define formal roles and responsibilities for Information Security

D. Create an executive security steering committee

Correct Answer: C

QUESTION 2

As a CISO you need to understand the steps that are used to perform an attack against a network. Put each step into the correct order.

1.Covering tracks 2.Scanning and enumeration 3.Maintaining Access 4.Reconnaissance 5.Gaining Access

A. 4, 2, 5, 3, 1

B. 2, 5, 3, 1, 4

C. 4, 5, 2, 3, 1

D. 4, 3, 5, 2, 1

Correct Answer: A

QUESTION 3

How often should an environment be monitored for cyber threats, risks, and exposures?

A. Weekly

B. Monthly

C. Quarterly

D. Daily

Correct Answer: D

QUESTION 4

Which technology can provide a computing environment without requiring a dedicated hardware backend?

A. Mainframe server

B. Virtual Desktop

C. Thin client

D. Virtual Local Area Network

Correct Answer: B

QUESTION 5

Regulatory requirements typically force organizations to implement

A. Mandatory controls

B. Discretionary controls

C. Optional controls

D. Financial controls

Correct Answer: A

QUESTION 6

When dealing with a risk management process, asset classification is important because it will impact the overall:

A. Threat identification

B. Risk monitoring

C. Risk treatment

D. Risk tolerance

Correct Answer: C

QUESTION 7

Using the Transport Layer Security (TLS) protocol enables a client in a network to be:

A. Provided with a digital signature

B. Assured of the server\\'s identity

C. Identified by a network

D. Registered by the server

Correct Answer: B

Reference: https://ukdiss.com/examples/tls.php

QUESTION 8

As the Business Continuity Coordinator of a financial services organization, you are responsible for ensuring assets are recovered timely in the event of a disaster. Which is the BEST Disaster Recovery performance indicator to validate that you are prepared for a disaster?

A. Recovery Point Objective (RPO)

B. Disaster Recovery Plan

C. Recovery Time Objective (RTO)

D. Business Continuity Plan

Correct Answer: D

Reference: https://www.resolver.com/resource/bcdr-metrics-that-matter/

QUESTION 9

Which of the following are not stakeholders of IT security projects?

A. Board of directors

B. Third party vendors

C. CISO

D. Help Desk

Correct Answer: B

QUESTION 10

The process for management approval of the security certification process which states the risks and mitigation of such risks of a given IT system is called

A. Security certification

B. Security system analysis

C. Security accreditation

D. Alignment with business practices and goals.

Correct Answer: C

QUESTION 11

What is the term describing the act of inspecting all real-time Internet traffic (i.e., packets) traversing a major Internet backbone without introducing any apparent latency?

A. Traffic Analysis

B. Deep-Packet inspection

C. Packet sampling

D. Heuristic analysis

Correct Answer: B

QUESTION 12

The PRIMARY objective of security awareness is to:

A. Ensure that security policies are read.

B. Encourage security-conscious employee behavior.

C. Meet legal and regulatory requirements.

D. Put employees on notice in case follow-up action for noncompliance is necessary

Correct Answer: B

QUESTION 13

The Security Operations Center (SOC) just purchased a new intrusion prevention system (IPS) that needs to be deployed in-line for best defense. The IT group is concerned about putting the new IPS in-line because it might negatively impact network availability. What would be the BEST approach for the CISO to reassure the IT group?

A. Work with the IT group and tell them to put IPS in-line and say it won\\'t cause any network impact

B. Explain to the IT group that the IPS won\\'t cause any network impact because it will fail open

C. Explain to the IT group that this is a business need and the IPS will fail open however, if there is a network failure the CISO will accept responsibility

D. Explain to the IT group that the IPS will fail open once in-line however it will be deployed in monitor mode for a set period of time to ensure that it doesn\\'t block any legitimate traffic

Correct Answer: D

QUESTION 14

Network Forensics is the prerequisite for any successful legal action after attacks on your Enterprise Network. Which is the single most important factor to introducing digital evidence into a court of law?

A. Comprehensive Log-Files from all servers and network devices affected during the attack

B. Fully trained network forensic experts to analyze all data right after the attack

C. Uninterrupted Chain of Custody

D. Expert forensics witness

Correct Answer: C

QUESTION 15

Involvement of senior management is MOST important in the development of:

A. IT security implementation plans.

B. Standards and guidelines.

C. IT security policies.

D. IT security procedures.

Correct Answer: C