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.passapply.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

With a focus on the review and approval aspects of board responsibilities, the Data Governance Council recommends that the boards provide strategic oversight regarding information and information security, include these four things:

A. Metrics tracking security milestones, understanding criticality of information and information security, visibility into the types of information and how it is used, endorsement by the board of directors

B. Annual security training for all employees, continual budget reviews, endorsement of the development and implementation of a security program, metrics to track the program

C. Understanding criticality of information and information security, review investment in information security, endorse development and implementation of a security program, and require regular reports on adequacy and effectiveness

D. Endorsement by the board of directors for security program, metrics of security program milestones, annual budget review, report on integration and acceptance of program

Correct Answer: C

Reference: https://nanopdf.com/download/information-security-governance-guidance-for-boards-of_pdf (9)

QUESTION 2

The amount of risk an organization is willing to accept in pursuit of its mission is known as

A. Risk mitigation

B. Risk transfer

C. Risk tolerance

D. Risk acceptance

Correct Answer: C

QUESTION 3

A system was hardened at the Operating System level and placed into the production environment. Months later an audit was performed and it identified insecure configuration different from the original hardened state. Which of the following security issues is the MOST likely reason leading to the audit findings?

A. Lack of asset management processes

B. Lack of change management processes

C. Lack of hardening standards

D. Lack of proper access controls

Correct Answer: B

QUESTION 4

An organization is required to implement background checks on all employees with access to databases containing credit card information. This is considered a security

A. Procedural control

B. Management control

C. Technical control

D. Administrative control

Correct Answer: B

QUESTION 5

When managing the security architecture for your company you must consider:

A. Security and IT Staff size

B. Company Values

C. Budget

D. All of the above

Correct Answer: D

QUESTION 6

What is the SECOND step to creating a risk management methodology according to the National Institute of Standards and Technology (NIST) SP 800-30 standard?

A. Determine appetite

B. Evaluate risk avoidance criteria

C. Perform a risk assessment

D. Mitigate risk

Correct Answer: D

QUESTION 7

A severe security threat has been detected on your corporate network. As CISO you quickly assemble key members of the Information Technology team and business operations to determine a modification to security controls in response to the threat. This is an example of:

A. Change management

B. Business continuity planning

C. Security Incident Response

D. Thought leadership

Correct Answer: C

QUESTION 8

Which of the following is a countermeasure to prevent unauthorized database access from web applications?

A. Session encryption

B. Removing all stored procedures

C. Input sanitization

D. Library control

Correct Answer: C

QUESTION 9

When you develop your audit remediation plan what is the MOST important criteria?

A. To remediate half of the findings before the next audit.

B. To remediate all of the findings before the next audit.

C. To validate that the cost of the remediation is less than the risk of the finding.

D. To validate the remediation process with the auditor.

Correct Answer: C

QUESTION 10

What type of attack requires the least amount of technical equipment and has the highest success rate?

A. War driving

B. Operating system attacks

C. Social engineering

D. Shrink wrap attack

Correct Answer: C

QUESTION 11

The formal certification and accreditation process has four primary steps, what are they?

A. Evaluating, describing, testing and authorizing

B. Evaluating, purchasing, testing, authorizing

C. Auditing, documenting, verifying, certifying

D. Discovery, testing, authorizing, certifying

Correct Answer: A

QUESTION 12

A company wants to fill a Chief Information Security Officer position in the organization. They need to define and implement a more holistic security program. Which of the following qualifications and experience would be MOST desirable to find in a candidate?

A. Multiple certifications, strong technical capabilities and lengthy resume

B. Industry certifications, technical knowledge and program management skills

C. College degree, audit capabilities and complex project management

D. Multiple references, strong background check and industry certifications

Correct Answer: B

QUESTION 13

As the Chief Information Security Officer, you want to ensure data shared securely, especially when shared with third parties outside the organization. What protocol provides the ability to extend the network perimeter with the use of encapsulation and encryption?

A. File Transfer Protocol (FTP)

B. Virtual Local Area Network (VLAN)

C. Simple Mail Transfer Protocol

D. Virtual Private Network (VPN)

Correct Answer: D

Reference: https://searchnetworking.techtarget.com/definition/virtual-private-network

QUESTION 14

The FIRST step in establishing a security governance program is to?

A. Conduct a risk assessment.

B. Obtain senior level sponsorship.

C. Conduct a workshop for all end users.

D. Prepare a security budget.

Correct Answer: B

QUESTION 15

Which of the following is the MOST important component of any change management process?

A. Scheduling

B. Back-out procedures

C. Outage planning

D. Management approval

Correct Answer: D