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.certbus.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

QUESTION 1

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 adjusting the controls to mitigate the risks, how often should the CISO perform an audit to verify the controls?

A. Never

B. Quarterly

C. Annually

D. Semi-annually

Correct Answer: A

QUESTION 2

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. Deep-Packet inspection

B. Traffic Analysis

C. Heuristic analysis

D. Packet sampling

Correct Answer: A

QUESTION 3

Which of the following represents the MOST negative impact resulting from an ineffective security governance program?

A. Improper use of information resources

B. Reduction of budget

C. Decreased security awareness

D. Fines for regulatory non-compliance

Correct Answer: D

QUESTION 4

Which of the following is used to lure attackers into false environments so they can be monitored, contained, or blocked from reaching critical systems?

A. Segmentation controls.

B. Shadow applications.

C. Deception technology.

D. Vulnerability management.

Correct Answer: B

QUESTION 5

The PRIMARY objective for information security program development should be:

A. Reducing the impact of the risk to the business.

B. Establishing incident response programs.

C. Establishing strategic alignment with business continuity requirements.

D. Identifying and implementing the best security solutions.

Correct Answer: A

QUESTION 6

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 hardening standards

C. Lack of proper access controls

D. Lack of change management processes

Correct Answer: D

QUESTION 7

What is meant by password aging?

A. An expiration date set for passwords

B. A Single Sign-On requirement

C. Time in seconds a user is allocated to change a password

D. The amount of time it takes for a password to activate

Correct Answer: C

QUESTION 8

Scenario: Your company has many encrypted telecommunications links for their world-wide operations. Physically distributing symmetric keys to all locations has proven to be administratively burdensome, but symmetric keys are preferred to other alternatives.

How can you reduce the administrative burden of distributing symmetric keys for your employer?

A. Use certificate authority to distribute private keys

B. Symmetrically encrypt the key and then use asymmetric encryption to unencrypt it

C. Use a self-generated key on both ends to eliminate the need for distribution

D. Use asymmetric encryption for the automated distribution of symmetric key

Correct Answer: D

QUESTION 9

Scenario: You are the newly hired Chief Information Security Officer for a company that has not previously had a senior level security practitioner. The company lacks a defined security policy and framework for their Information Security Program. Your new boss, the Chief Financial Officer, has asked you to draft an outline of a security policy and recommend an industry/sector neutral information security control framework for implementation.

Your Corporate Information Security Policy should include which of the following?

A. Roles and responsibilities

B. Information security theory

C. Incident response contacts

D. Desktop configuration standards

Correct Answer: A

QUESTION 10

An audit was conducted and many critical applications were found to have no disaster recovery plans in place. You conduct a Business Impact Analysis (BIA) to determine impact to the company for each application.

What should be the NEXT step?

A. Create technology recovery plans

B. Determine the annual loss expectancy (ALE)

C. Build a secondary hot site

D. Create a crisis management plan

Correct Answer: A

QUESTION 11

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. Thought leadership

C. Business continuity planning

D. Security Incident Response

Correct Answer: D

QUESTION 12

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

A. Evaluating, describing, testing and authorizing

B. Auditing, documenting, verifying, certifying

C. Evaluating, purchasing, testing, authorizing

D. Discovery, testing, authorizing, certifying

Correct Answer: A

QUESTION 13

A bastion host should be placed: A. Inside the DMZ

B. In-line with the data center firewall

C. Beyond the outer perimeter firewall

D. As the gatekeeper to the organization\\'s honeynet

Correct Answer: C

Reference: https://www.skillset.com/questions/a-bastion-host-is-which-of-the-following

QUESTION 14

In accordance with best practices and international standards, how often is security awareness training provided to employees of an organization?

A. Every 18 months

B. Every 12 months

C. High risk environments 6 months, low-risk environments 12 months

D. Every 6 months

Correct Answer: B

QUESTION 15

According to the National Institute of Standards and Technology (NIST) SP 800-40, which of the following considerations are MOST important when creating a vulnerability management program?

A. Susceptibility to attack, expected duration of attack, and mitigation availability

B. Attack vectors, controls cost, and investigation staffing needs

C. Susceptibility to attack, mitigation response time, and cost

D. Vulnerability exploitation, attack recovery, and mean time to repair

Correct Answer: C