712-50$^{\text{Q\&As}}$

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: 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 implemented remediation activities.

Which of the following is the MOST logical next step?

A. Validate the effectiveness of applied controls

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

C. Validate security program resource requirements

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

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. You have identified potential solutions for all of your risks that do not have security controls.

What is the NEXT step?

A. Create a risk metrics for all unmitigated risks

B. Get approval from the board of directors

C. Verify that the cost of mitigation is less than the risk

D. Screen potential vendor solutions

Correct Answer: C

QUESTION 3

Which wireless encryption technology makes use of temporal keys?

A. Wi-Fi Protected Access version 2 (WPA2)

B. Wireless Equivalence Protocol (WEP)

C. Wireless Application Protocol (WAP)

D. Extensible Authentication Protocol (EAP)

Correct Answer: A

QUESTION 4

A security officer wants to implement a vulnerability scanning program. The officer is uncertain of the state of vulnerability resiliency within the organization\\'s large IT infrastructure.

What would be the BEST approach to minimize scan data output while retaining a realistic view of system vulnerability?

A. Decrease the vulnerabilities within the scan tool settings

B. Scan a representative sample of systems

C. Filter the scan output so only pertinent data is analyzed

D. Perform the scans only during off-business hours

Correct Answer: B

QUESTION 5

As the CISO, you need to create an IT security strategy.

Which of the following is the MOST important thing to review before you start writing the plan?

A. The existing IT environment

B. Other corporate technology trends

C. The company business plan

D. The present IT budget

Correct Answer: C

QUESTION 6

What is the MOST important reason for monitoring Key Risk Indicators (KRIs)?

A. The organization\\'s risk profile is subject to change

B. The processes used to develop KRIs can be fraught with errors and must be rechecked periodically

C. Effective KRIs will reduce the time to implement risk treatment options

D. A large number of KRIs is a critical part of continuous improvement of management

Correct Answer: A

Reference: https://searchcio.techtarget.com/definition/key-risk-indicator-KRI

QUESTION 7

After a risk assessment is performed, a particular risk is considered to have the potential of costing the organization 1.2 Million USD. This is an example of____________.

A. Qualitative risk analysis

B. Risk Appetite

C. Quantitative risk analysis

D. Risk Tolerance

Correct Answer: C

QUESTION 8

Which of the following is the MOST important for a CISO to understand when identifying threats?

A. How the security operations team will behave to reported incidents

B. How vulnerabilities can potentially be exploited in systems that impact the organization

C. How the firewall and other security devices are configured to prevent attacks

D. How the incident management team prepares to handle an attack

Correct Answer: B

QUESTION 9

When would it be more desirable to develop a set of decentralized security policies and procedures within an enterprise environment?

A. When there is a variety of technologies deployed in the infrastructure.

B. When it results in an overall lower cost of operating the security program.

C. When there is a need to develop a more unified incident response capability.

D. When the enterprise is made up of many business units with diverse business activities, risks profiles and regulatory requirements.

Correct Answer: D

QUESTION 10

When selecting a security solution with recurring maintenance costs after the first year, the CISO should:

A. Defer selection until the market improves and cash flow is positive

B. Implement the solution and ask for the increased operating cost budget when it is time

C. Communicate future operating costs to the CIO/CFO and seek commitment from them to ensure the new solution\\'s continued use

D. Cut other essential programs to ensure the new solution\\'s continued use

Correct Answer: C

Reference: https://books.google.com/books?id=kiE_EAAAQBAJandpg=PT59andlpg=PT59anddq=Communicate+future+operating+costs+to+the+CIO/CFO+and+seek+commitment+from+them+to+ensure+the+new+solution%E2%80%99s +continued+useandsource=blandots=3MNR-uuPjRandsig=ACfU3U1ibTQwVjKcrliRd3Dl-jpgY5Xlxwandhl=enandsa=Xandved=2ahUKEwiTjoDpuLv0AhU_SvEDHUvgCY4Q6AF6BAhAEAM#v=onepageandq=Communicate%20future%20operating%20costs% 20to%20the%20CIO%2FCFO%20and%20seek%20commitment%20from%20them%20to%20ensure%20the%20new%20solution%E2%80%99s%20continued%20useandf=false

QUESTION 11

A security manager has created a risk program. Which of the following is a critical part of ensuring the program is successful?

A. Ensuring developers include risk control comments in code

B. Creating risk assessment templates based on specific threats

C. Providing a risk program governance structure

D. Allowing for the acceptance of risk for regulatory compliance requirements

Correct Answer: C

QUESTION 12

Securing facilities with Faraday cages or applying TEMPEST standards prevents the ability to monitor which of the following?

A. Electro-magnetic emanations

B. Wired network junction points

C. Environmental control systems

D. Badge entry points

Correct Answer: A

QUESTION 13

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. The organization has already been subject to a significant amount of credit card fraud.

Which of the following is the MOST likely reason for this fraud?

A. Lack of compliance to the Payment Card Industry (PCI) standards

B. Ineffective security awareness program

C. Lack of technical controls when dealing with credit card data

D. Security practices not in alignment with ISO 27000 frameworks

Correct Answer: A

QUESTION 14

The process to evaluate the technical and non-technical security controls of an IT system to validate that a given design and implementation meet a specific set of security requirements is called____________________.

A. Security certification

B. Security accreditation

C. Alignment with business practices and goals.

D. Security system analysis

Correct Answer: A

QUESTION 15

You have been hired as the CISO for a hospital. The hospital currently deploys a hybrid cloud model using a Software as a Service (SaaS) product for healthcare clearinghouse services. The Health Insurance Portability and Accountability Act (HIPAA) require an agreement between Cloud Service Providers (CSP) and the covered entity. Based on HIPAA, once the agreement between the covered entity and the CSP signed, the CSP is ____________?

A. Partially liable for compliance with the applicable requirements of the HIPAA Rules

B. Directly liable for compliance with the applicable requirements of the HIPAA Rules

C. Not liable for compliance with the applicable requirements of the HIPAA Rules

D. Indirectly liable for compliance with the applicable requirements of the HIPAA Rules

Correct Answer: A