Vendor:EC-COUNCIL

Exam Code:712-50

Exam Name:EC-Council Certified CISO (CCISO)

Version: Demo

QUESTION 1

A department within your company has proposed a third party vendor solution to address an urgent, critical business need. As the CISO you have been asked to accelerate screening of their security control claims.

Which of the following vendor provided documents is BEST to make your decision?

A. Vendor provided reference from an existing reputable client detailing their implementation

B. Vendor\\'s client list of reputable organizations currently using their solution

C. Vendor provided internal risk assessment and security control documentation

D. Vendor provided attestation of the detailed security controls from a reputable accounting firm

Correct Answer: D

QUESTION 2

Scenario: The new CISO was informed of all the Information Security projects that the section has in progress. Two projects are over a year behind schedule and way over budget. Using the best business practices for project management, you determine that the project correctly aligns with the organization goals.

What should be verified next?

A. Scope

B. Constraints

C. Resources

D. Budget

Correct Answer: A

QUESTION 3

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 4

The newly appointed CISO of an organization is reviewing the IT security strategic plan. Which of the following is the MOST important component of the strategic plan?

A. There is a clear definition of the IT security mission and vision.

B. The plan requires return on investment for all security projects.

C. There is integration between IT security and business staffing

D. There is an auditing methodology in place.

Correct Answer: A

QUESTION 5

When considering using a vendor to help support your security devices remotely, what is the BEST choice for allowing access?

A. Vendor uses their own laptop and logins using two factor authentication with their own unique credentials

B. Vendor uses a company supplied laptop and logins using two factor authentication wit same admin credentials your security team uses

C. Vendor uses a company supplied laptop and logins using two factor authentication with their own unique credentials

D. Vendors uses their own laptop and logins with same admin credentials your security team uses

Correct Answer: C

QUESTION 6

Physical security measures typically include which of the following components?

A. Strong password, Biometric, Common Access Card

B. Technical. Strong Password, Operational

C. Operational, Biometric, Physical

D. Physical, Technical, Operational

Correct Answer: D

QUESTION 7

The Information Security Management program MUST protect:

A. Audit schedules and findings

B. Intellectual property released into the public domain

C. all organizational assets

D. critical business processes and revenue streams

Correct Answer: D

QUESTION 8

Which of the following set of processes is considered to be one of the cornerstone cycles of the International Organization for Standardization (ISO) 27001 standard?

A. Plan-Check-Do-Act

B. Plan-Select-Implement-Evaluate

C. Plan-Do-Check-Act

D. SCORE (Security Consensus Operational Readiness Evaluation)

Correct Answer: C

QUESTION 9

Risk appetite directly affects what part of a vulnerability management program?

A. Scope

B. Schedule

C. Staff

D. Scan tools

Correct Answer: A

QUESTION 10

Which of the following activities results in change requests?

A. Corrective actions

B. Defect repair

C. Preventive actions

D. Inspection

Correct Answer: C

QUESTION 11

Which of the following is the MOST important benefit of an effective security governance process?

A. Senior management participation in the incident response process

B. Better vendor management

C. Reduction of security breaches

D. Reduction of liability and overall risk to the organization

Correct Answer: D

QUESTION 12

A business unit within your organization intends to deploy a new technology in a manner that places it in violation of existing information security standards.

What immediate action should the information security manager take?

A. Enforce the existing security standards and do not allow the deployment of the new technology.

B. If the risks associated with that technology are not already identified, perform a risk analysis to quantify the risk, and allow the business unit to proceed based on the identified risk level.

C. Amend the standard to permit the deployment.

D. Permit a 90-day window to see if an issue occurs and then amend the standard if there are no issues.

Correct Answer: B