DUMPSARENA

# EC-Council Certified CISO (CCISO)

## ECCouncil 712-50

## Version Demo

**Total Demo Questions: 20**

**Total Premium Questions: 458**

**Buy Premium PDF**

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

## QUESTION NO: 1

What process defines the framework of rules and practices by which a board of directors ensure accountability, fairness and transparency in an organization's relationship with its shareholders?

**A.** Internal Audit

**B.** Corporate governance

**C.** Risk Oversight

**D.** Key Performance Indicators

## ANSWER: B

**Explanation:**

Reference: https://www.igi-global.com/dictionary/corporate-governance/5957

## QUESTION NO: 2

When measuring the effectiveness of an Information Security Management System which one of the following would be MOST LIKELY used as a metric framework?

**A.** ISO 27001

**B.** ISO 27004

**C.** PRINCE2

**D.** ITILv3

## ANSWER: B

## QUESTION NO: 3

When working in the Payment Card Industry (PCI), how often should security logs be review to comply with the standards?

**A.** Monthly

**B.** Hourly

**C.** Weekly

**D.** Daily

**ANSWER: D**

**QUESTION NO: 4**

The single most important consideration to make when developing your security program, policies, and processes is:

**A.** Alignment with the business

**B.** Budgeting for unforeseen data compromises

**C.** Establishing your authority as the Security Executive

**D.** Streaming for efficiency

**ANSWER: A**

**QUESTION NO: 5**

An organization information security policy serves to_____.

**A.** define security configurations for systems

**B.** establish budgetary input in order to meet compliance requirements

**C.** establish acceptable systems and user behavior

**D.** define relationships with external law enforcement agencies

**E.** None

**ANSWER: C**

**QUESTION NO: 6**

In order for a CISO to have true situational awareness there is a need to deploy technology that can give a real-time view of security events across the enterprise.

Which of the following tools represents the BEST choice to achieve this awareness?

**A.** Intrusion Detection System (IDS), firewall, switch, syslog

**B.** Security Incident Event Management (SIEM), IDS, router, syslog

**C.** VMware, router, switch, firewall, syslog, vulnerability management system (VMS)

**D.** SIEM, IDS, firewall, VMS

**ANSWER: D**

## QUESTION NO: 7

Which of the following is the MOST effective way to measure the effectiveness of security controls on a perimeter network?

**A.** Perform a vulnerability scan of the network

**B.** Internal Firewall ruleset reviews

**C.** Implement network intrusion prevention systems

**D.** External penetration testing by a qualified third party

**ANSWER: D**

## QUESTION NO: 8

What is the main result of a company keeping its information security functions siloed in different business units?

**A.** Overlapping security initiatives, with wasted resources, or major gaps that can lead to serious security compromises

**B.** Board of Directors gains greater insight into the overall functions of the company and the separate security processes

**C.** Greater integration between groups that takes greater effort and expense but results in close execution of processes

**D.** Security and risk management teams have a responsibility to learn every aspect of the company and find ways to integrate into each silo

**ANSWER: A**

**Explanation:**

Reference: https://www.plixer.com/blog/data-silo-what-is-it-why-is-it-bad/

## QUESTION NO: 9

How often should the Statements of Standards for Attestation Engagements-16 (SSAE16)/International Standard on Assurance Engagements 3402 (ISAE3402) report of your vendors be reviewed?

**A.** Annually

**B.** Quarterly

**C.** Bi-annually

**D.** Semi-annually

**ANSWER: A**

## QUESTION NO: 10

From an information security perspective, information that no longer supports the main purpose of the business should be:

**A.** protected under the information classification policy

**B.** analyzed under the data ownership policy

**C.** assessed by a business impact analysis.

**D.** analyzed under the retention policy.

**ANSWER: D**

## QUESTION NO: 11

An example of professional unethical behavior is:

**A.** Sharing copyrighted material with other members of a professional organization where all members have legitimate access to the material

**B.** Copying documents from an employer's server which you assert that you have an intellectual property claim to possess, but the company disputes

**C.** Storing client lists and other sensitive corporate internal documents on a removable thumb drive

**D.** Gaining access to an affiliated employee's work email account as part of an officially sanctioned internal investigation

**ANSWER: B**

## QUESTION NO: 12

Within an organization's vulnerability management program, who has the responsibility to implement remediation actions?

**A.** Data owner

**B.** Data center manager

**C.** Network architect

**D.** System administrator

**ANSWER: D**

## QUESTION NO: 13

The remediation of a specific audit finding is deemed too expensive and will not be implemented.

Which of the following is a TRUE statement?

**A.** The audit findings is incorrect

**B.** The asset is more expensive than the remediation

**C.** The asset being protected is less valuable than the remediation costs

**D.** The remediation costs are irrelevant; it must be implemented regardless of cost.

**ANSWER: C**

## QUESTION NO: 14

Which of the following has the GREATEST impact on the implementation of an information security governance model?

**A.** Complexity of organizational structure

**B.** Distance between physical locations

**C.** Organizational budget

**D.** Number of employees

**ANSWER: A**

## QUESTION NO: 15

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

**ANSWER: D**

## QUESTION NO: 16

Your company has limited resources to spend on security initiatives. The Chief Financial Officer asks you to prioritize the protection of information resources based on their value to the company. It is essential that you be able to communicate in language that your fellow executives will understand.

You should:

**A.** Create a detailed technical executive summary

**B.** Create timelines for mitigation

**C.** Calculate annual loss expectancy

**D.** Develop a cost-benefit analysis

**ANSWER: D**

## QUESTION NO: 17

Annual Loss Expectancy is derived from the function of which two factors?

**A.** Annual rate of Occurrence and Single Loss Expectancy

**B.** Annual rate of Occurrence and Asset Value

**C.** Safeguard value and Annual Rate of Occurrence

**D.** Single Loss Expectancy and Exposure factor

**ANSWER: A**

## QUESTION NO: 18

Which of the following represents the BEST reason for an organization to use the Control Objectives for Information and Related Technology (COBIT) as an Information Technology (IT) framework?

**A.** Information Security (IS) procedures often require augmentation with other standards

**B.** Implementation of it eases an organization’s auditing and compliance burden

**C.** It provides for a consistent and repeatable staffing model for technology organizations

**D.** It allows executives to more effectively monitor IT implementation costs

**ANSWER: B**

## QUESTION NO: 19

The network administrator wants to strengthen physical security in the organization. Specifically, to implement a solution stopping people from entering certain restricted zones without proper credentials. Which of following physical security measures should the administrator use?

**A.** Video surveillance

**B.** Mantrap

**C.** Bollards

**D.** Fence

**ANSWER: D**

## QUESTION NO: 20

What oversight should the information security team have in the change management process for application security?

**A.** Information security should be aware of any significant application security changes and work with developer to test for vulnerabilities before changes are deployed in production

**B.** Information security should be aware of all application changes and work with developers before changes and deployed in production

**C.** Information security should be informed of changes to applications only

**D.** Development team should tell the information security team about any application security flaws

**ANSWER: A**