# 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**

Information security policies should be reviewed:

A. by stakeholders at least annually

B. by the CISO when new systems are brought online

C. by the Incident Response team after an audit

D. by internal audit semiannually

Correct Answer: A

**QUESTION 2**

Knowing the potential financial loss an organization is willing to suffer if a system fails is a determination of which of the following?

A. Cost benefit

B. Risk appetite

C. Business continuity

D. Likelihood of impact

Correct Answer: B

**QUESTION 3**

Providing oversight of a comprehensive information security program for the entire organization is the primary responsibility of which group under the InfoSec governance framework?

A. Senior Executives

B. Office of the Auditor

C. Office of the General Counsel

D. All employees and users

Correct Answer: A

**QUESTION 4**

Your penetration testing team installs an in-line hardware key logger onto one of your network machines. Which of the following is of major concern to the security organization?

A. In-line hardware keyloggers don\\'t require physical access

B. In-line hardware keyloggers don\\'t comply to industry regulations

C. In-line hardware keyloggers are undetectable by software

D. In-line hardware keyloggers are relatively inexpensive

Correct Answer: C

**QUESTION 5**

Which of the following is a fundamental component of an audit record?

A. Date and time of the event

B. Failure of the event

C. Originating IP-Address

D. Authentication type

Correct Answer: A

**QUESTION 6**

Scenario: As you begin to develop the program for your organization, you assess the corporate culture and determine that there is a pervasive opinion that the security program only slows things down and limits the performance of the "real workers."

What must you do first in order to shift the prevailing opinion and reshape corporate culture to understand the value of information security to the organization?

A. Cite compliance with laws, statutes, and regulations ?explaining the financial implications for the company for non-compliance

B. Understand the business and focus your efforts on enabling operations securely

C. Draw from your experience and recount stories of how other companies have been compromised

D. Cite corporate policy and insist on compliance with audit findings

Correct Answer: B

**QUESTION 7**

Which of the following illustrates an operational control process:

A. Classifying an information system as part of a risk assessment

B. Installing an appropriate fire suppression system in the data center

C. Conducting an audit of the configuration management process

D. Establishing procurement standards for cloud vendors

Correct Answer: B

**QUESTION 8**

The Annualized Loss Expectancy (Before) minus Annualized Loss Expectancy (After) minus Annual Safeguard Cost is the formula for determining:

A. Safeguard Value

B. Cost Benefit Analysis

C. Single Loss Expectancy

D. Life Cycle Loss Expectancy

Correct Answer: B

**QUESTION 9**

When analyzing and forecasting an operating expense budget what are not included?

A. Software and hardware license fees

B. Utilities and power costs

C. Network connectivity costs

D. New datacenter to operate from

Correct Answer: D

**QUESTION 10**

An anonymity network is a series of?

A. Covert government networks

B. War driving maps

C. Government networks in Tora

D. Virtual network tunnels

Correct Answer: D

**QUESTION 11**

When dealing with risk, the information security practitioner may choose to:

A. assign

B. transfer

C. acknowledge

D. defer

Correct Answer: C

**QUESTION 12**

Your company has a "no right to privacy" notice on all logon screens for your information systems and users sign an Acceptable Use Policy informing them of this condition. A peer group member and friend comes to you and requests access to one of her employee\\'s email account. What should you do? (choose the BEST answer):

A. Grant her access, the employee has been adequately warned through the AUP.

B. Assist her with the request, but only after her supervisor signs off on the action.

C. Reset the employee\\'s password and give it to the supervisor.

D. Deny the request citing national privacy laws.

Correct Answer: B

**QUESTION 13**

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 14**

Your incident response plan should include which of the following?

A. Procedures for litigation

B. Procedures for reclamation

C. Procedures for classification

D. Procedures for charge-back

Correct Answer: C

**QUESTION 15**

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. External penetration testing by a qualified third party

C. Internal Firewall ruleset reviews

D. Implement network intrusion prevention systems

Correct Answer: B

**QUESTION 16**

Which of the following intellectual Property components is focused on maintaining brand recognition?

A. Trademark

B. Patent

C. Research Logs

D. Copyright

Correct Answer: A

**QUESTION 17**

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

A. Security officer

B. Data owner

C. Vulnerability engineer

D. System administrator

Correct Answer: D

**QUESTION 18**

You manage a newly created Security Operations Center (SOC), your team is being inundated with security alerts and don\\'t know what to do. What is the BEST approach to handle this situation?

A. Tell the team to do their best and respond to each alert

B. Tune the sensors to help reduce false positives so the team can react better

C. Request additional resources to handle the workload

D. Tell the team to only respond to the critical and high alerts

Correct Answer: B

**QUESTION 19**

Which of the following statements about Encapsulating Security Payload (ESP) is true?

A. It is an IPSec protocol.

B. It is a text-based communication protocol.

C. It uses TCP port 22 as the default port and operates at the application layer.

D. It uses UDP port 22

Correct Answer: A

**QUESTION 20**

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

**QUESTION 21**

Developing effective security controls is a balance between:

A. Risk Management and Operations

B. Corporate Culture and Job Expectations

C. Operations and Regulations

D. Technology and Vendor Management

Correct Answer: A

**QUESTION 22**

To get an Information Security project back on schedule, which of the following will provide the MOST help?

A. Upper management support

B. More frequent project milestone meetings

C. Stakeholder support

D. Extend work hours

Correct Answer: A

**QUESTION 23**

Which of the following are not stakeholders of IT security projects?

A. Board of directors

B. Third party vendors

C. CISO

D. Help Desk

Correct Answer: B

**QUESTION 24**

An organization licenses and uses personal information for business operations, and a server containing that information has been compromised. What kind of law would require notifying the owner or licensee of this incident?

A. Data breach disclosure

B. Consumer right disclosure

C. Security incident disclosure

D. Special circumstance disclosure

Correct Answer: A

**QUESTION 25**

Information Security is often considered an excessive, after-the-fact cost when a project or initiative is completed. What can be done to ensure that security is addressed cost effectively?

A. User awareness training for all employees

B. Installation of new firewalls and intrusion detection systems

C. Launch an internal awareness campaign

D. Integrate security requirements into project inception

Correct Answer: D

**QUESTION 26**

An IT auditor has recently discovered that because of a shortage of skilled operations personnel, the security administrator has agreed to work one late night shift a week as the senior computer operator. The most appropriate course of action for the IT auditor is to:

A. Inform senior management of the risk involved.

B. Agree to work with the security officer on these shifts as a form of preventative control.

C. Develop a computer assisted audit technique to detect instances of abuses of the arrangement.

D. Review the system log for each of the late night shifts to determine whether any irregular actions occurred.

Correct Answer: A

**QUESTION 27**

The implementation of anti-malware and anti-phishing controls on centralized email servers is an example of what type of security control?

A. Organization control

B. Procedural control

C. Management control

D. Technical control

Correct Answer: D

**QUESTION 28**

The MOST common method to get an unbiased measurement of the effectiveness of an Information Security Management System (ISMS) is to

A. assign the responsibility to the information security team.

B. assign the responsibility to the team responsible for the management of the controls.

C. create operational reports on the effectiveness of the controls.

D. perform an independent audit of the security controls.

Correct Answer: D

**QUESTION 29**

Scenario: Your program is developed around minimizing risk to information by focusing on people, technology, and operations.

An effective way to evaluate the effectiveness of an information security awareness program for end users, especially senior executives, is to conduct periodic:

A. Controlled spear phishing campaigns

B. Password changes

C. Baselining of computer systems

D. Scanning for viruses

Correct Answer: A

**QUESTION 30**

The security team has investigated the theft/loss of several unencrypted laptop computers containing sensitive corporate information. To prevent the loss of any additional corporate data it is unilaterally decided by the CISO that all existing and future laptop computers will be encrypted. Soon, the help desk is flooded with complaints about the slow performance of the laptops and users are upset. What did the CISO do wrong? (choose the BEST answer):

A. Failed to identify all stakeholders and their needs

B. Deployed the encryption solution in an inadequate manner

C. Used 1024 bit encryption when 256 bit would have sufficed

D. Used hardware encryption instead of software encryption

Correct Answer: A

**QUESTION 31**

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

A. Daily

B. Hourly

C. Weekly

D. Monthly

Correct Answer: A

**QUESTION 32**

A new CISO just started with a company and on the CISO\\'s desk is the last complete Information Security Management audit report. The audit report is over two years old. After reading it, what should be the CISO\\'s FIRST priority?

A. Have internal audit conduct another audit to see what has changed.

B. Contract with an external audit company to conduct an unbiased audit

C. Review the recommendations and follow up to see if audit implemented the changes

D. Meet with audit team to determine a timeline for corrections

Correct Answer: C

**QUESTION 33**

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 timelines for mitigation

B. Develop a cost-benefit analysis

C. Calculate annual loss expectancy

D. Create a detailed technical executive summary

Correct Answer: B

**QUESTION 34**

SCENARIO: A CISO has several two-factor authentication systems under review and selects the one that is most sufficient and least costly. The implementation project planning is completed and the teams are ready to implement the solution. The CISO then discovers that the product it is not as scalable as originally thought and will not fit the organization\\'s needs.

The CISO discovers the scalability issue will only impact a small number of network segments. What is the next logical step to ensure the proper application of risk management methodology within the two-facto implementation project?

A. Create new use cases for operational use of the solution

B. Determine if sufficient mitigating controls can be applied

C. Decide to accept the risk on behalf of the impacted business units

D. Report the deficiency to the audit team and create process exceptions

Correct Answer: B

**QUESTION 35**

How often should the SSAE16 report of your vendors be reviewed?

A. Quarterly

B. Semi-annually

C. Annually

D. Bi-annually

Correct Answer: C

**QUESTION 36**

When should IT security project management be outsourced?

A. When organizational resources are limited

B. When the benefits of outsourcing outweigh the inherent risks of outsourcing

C. On new, enterprise-wide security initiatives

D. On projects not forecasted in the yearly budget

Correct Answer: B

**QUESTION 37**

A method to transfer risk is to:

A. Implement redundancy

B. move operations to another region

C. purchase breach insurance

D. Alignment with business operations

Correct Answer: C

**QUESTION 38**

Which of the following is MOST beneficial in determining an appropriate balance between uncontrolled innovation and excessive caution in an organization?

A. Define the risk appetite

B. Determine budget constraints

C. Review project charters

D. Collaborate security projects

Correct Answer: A

**QUESTION 39**

Credit card information, medical data, and government records are all examples of:

A. Confidential/Protected Information

B. Bodily Information

C. Territorial Information

D. Communications Information

Correct Answer: A

**QUESTION 40**

When creating contractual agreements and procurement processes why should security requirements be included?

A. To make sure they are added on after the process is completed

B. To make sure the costs of security is included and understood

C. To make sure the security process aligns with the vendor\\'s security process

D. To make sure the patching process is included with the costs

Correct Answer: B

To Read the Whole Q&As, please purchase the Complete Version from Our website.

# Try our product !

100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.certbus.com/allproducts

## Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket: