Updated Jul 13, 2022 Verified Pass 712-50 Exam in First Attempt Guaranteed [Q207-Q228

Updated Jul 13, 2022 Verified Pass 712-50 Exam in First Attempt Guaranteed
Free 712-50 Sample Questions and 100% Cover Real Exam Questions (Updated 447 Questions)

Ending Notes

To become a dependable Certified CISO, one needs to have a unique blend of IT and leadership qualities that can only be gained with the EC-Council 712-50 exam. It is the key to a secure and promising career. Success in this test will take your career at zeniths and will make you an ideal candidate for information security job roles. But, don't forget to refer to only quality books from Amazon for self-study. With them, the career path will be easy-to-accomplish and enjoyable.

EC-Council Certified CISO 712-50 Exam

EC-Council Certified CISO 712-50 Exam which is related to EC-Council Certified CISO certification. This 712-50 exam validates the ability to a candidate to implement, manage and maintain an information security governance program, Coordinate the application of information security strategies, plans, policies, and procedures to reduce regulatory risk, control Information Security Management, Identify, negotiate and manage vendor agreement and community, Identify the basic network architecture, models, protocols and components such as routers and hubs that play a role in network security.

QUESTION 207

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?

* There is integration between IT security and business staffing.
* There is a clear definition of the IT security mission and vision.
* There is an auditing methodology in place.
* The plan requires return on investment for all security projects.

ECCouncil 712-50 : Practice Test

QUESTION 208

Which of the following is critical in creating a security program aligned with an organization’s goals?

* Ensure security budgets enable technical acquisition and resource allocation based on internal compliance requirements
* Develop a culture in which users, managers and IT professionals all make good decisions about information risk
* Provide clear communication of security program support requirements and audit schedules
* Create security awareness programs that include clear definition of security program goals and charters

QUESTION 209

Who in the organization determines access to information?
* Compliance officer
* Legal department
* Data Owner
* Information security officer

QUESTION 210

Which of the following reports should you as an IT auditor use to check on compliance with a service level agreement’s requirement for uptime?
* Systems logs
* Hardware error reports
* Utilization reports
* Availability reports

QUESTION 211

An organization information security policy serves to
* establish budgetary input in order to meet compliance requirements
* establish acceptable systems and user behavior
* define security configurations for systems
* define relationships with external law enforcement agencies

QUESTION 212

Which of the following is the MOST important reason to measure the effectiveness of an Information Security Management System (ISMS)?
* Meet regulatory compliance requirements
* Better understand the threats and vulnerabilities affecting the environment
* Better understand strengths and weaknesses of the program
* Meet legal requirements

QUESTION 213

When managing the security architecture for your company you must consider:
* Security and IT Staff size
* Company Values
* Budget
* All of the above

QUESTION 214

Which represents PROPER separation of duties in the corporate environment?

* Information Security and Identity Access Management teams perform two distinct functions
* Developers and Network teams both have admin rights on servers
* Finance has access to Human Resources data
* Information Security and Network teams perform two distinct functions

QUESTION 215

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:
* Create timelines for mitigation
* Develop a cost-benefit analysis
* Calculate annual loss expectancy
* Create a detailed technical executive summary

QUESTION 216

A newly appointed security officer finds data leakage software licenses that had never been used. The officer decides to implement a project to ensure it gets installed, but the project gets a great deal of resistance across the organization.

Which of the following represents the MOST likely reason for this situation?
* The project was initiated without an effort to get support from impacted business units in the organization
* The security officer should allow time for the organization to get accustomed to her presence before initiating security projects
* The software is out of date and does not provide for a scalable solution across the enterprise
* The software license expiration is probably out of synchronization with other software licenses

QUESTION 217

Scenario: An organization has recently appointed a CISO. This is a new role in the organization and it signals the increasing need to address security consistently at the enterprise level. This new CISO, while confident with skills and experience, is constantly on the defensive and is unable to advance the IT security centric agenda.

The CISO has been able to implement a number of technical controls and is able to influence the Information Technology teams but has not been able to influence the rest of the organization.

From an organizational perspective, which of the following is the LIKELY reason for this?
* The CISO reports to the IT organization
* The CISO has not implemented a policy management framework
* The CISO does not report directly to the CEO of the organization
* The CISO has not implemented a security awareness program

QUESTION 218

Which of the following is a strong post designed to stop a car?
* Fence
* Bollard
* Reinforced rebar
* Gate

Explanation/Reference:

QUESTION 219

A company wants to fill a Chief Information Security Officer position in the organization. They need to define and implement a more holistic security program. Which of the following qualifications and experience would be MOST desirable to find in a candidate?

* Multiple certifications, strong technical capabilities and lengthy resume
* Industry certifications, technical knowledge and program management skills
* College degree, audit capabilities and complex project management
* Multiple references, strong background check and industry certifications

QUESTION 220

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?

* In-line hardware keyloggers are undetectable by software
* In-line hardware keyloggers are relatively inexpensive
* In-line hardware keyloggers don’t require physical access
* In-line hardware keyloggers don’t comply to industry regulations

QUESTION 221

An organization’s firewall technology needs replaced. A specific technology has been selected that is less costly than others and lacking in some important capabilities. The security officer has voiced concerns about sensitive data breaches but the decision is made to purchase.

What does this selection indicate?

* A high threat environment
* A low vulnerability environment
* A high risk tolerance environment
* A low risk tolerance environment

QUESTION 222

The executive board has requested that the CISO of an organization define and Key Performance Indicators (KPI) to measure the effectiveness of the security awareness program provided to call center employees.

Which of the following can be used as a KPI?

* Number of successful social engineering attempts on the call center
* Number of callers who abandon the call before speaking with a representative
* Number of callers who report a lack of customer service from the call center
* Number of callers who report security issues.

QUESTION 223

SCENARIO: Critical servers show signs of erratic behavior within your organization’s intranet. Initial information indicates the systems are under attack from an outside entity. As the Chief Information Security Officer (CISO), you decide to deploy the Incident Response Team (IRT) to determine the details of this incident and take action according to the information available to the team.

In what phase of the response will the team extract information from the affected systems without altering original data?
* Response
* Investigation
* Recovery
* Follow-up

Scenario4

QUESTION 224

When managing the critical path of an IT security project, which of the following is MOST important?
* Knowing who all the stakeholders are.
* Knowing the people on the data center team.
* Knowing the threats to the organization.
* Knowing the milestones and timelines of deliverables.

QUESTION 225

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?
* Have internal audit conduct another audit to see what has changed.
* Contract with an external audit company to conduct an unbiased audit
* Review the recommendations and follow up to see if audit implemented the changes
* Meet with audit team to determine a timeline for corrections

QUESTION 226

As the CISO, you have been tasked with the execution of the company’s key management program. You MUST ensure the integrity of encryption keys at the point of generation. Which principal of encryption key control will ensure no single individual can constitute or re-constitute a key?
* Dual Control
* Separation of Duties
* Split Knowledge
* Least Privilege

Explanation/Reference: https://info.townsendsecurity.com/bid/23881/PCI-DSS-2-0-and-Encryption-Key-Management

QUESTION 227

As the CISO for your company you are accountable for the protection of information resources commensurate with:
* Customer demand
* Cost and time to replace
* Insurability tables
* Risk of exposure

QUESTION 228

Which of the following is the MAIN security concern for public cloud computing?
* Unable to control physical access to the servers
* Unable to track log on activity
* Unable to run anti-virus scans
* Unable to patch systems as needed

Download Real EC-COUNCIL 712-50 Exam Dumps Test Engine Exam Questions:
https://www.test4engine.com/712-50_exam-latest-braindumps.html]