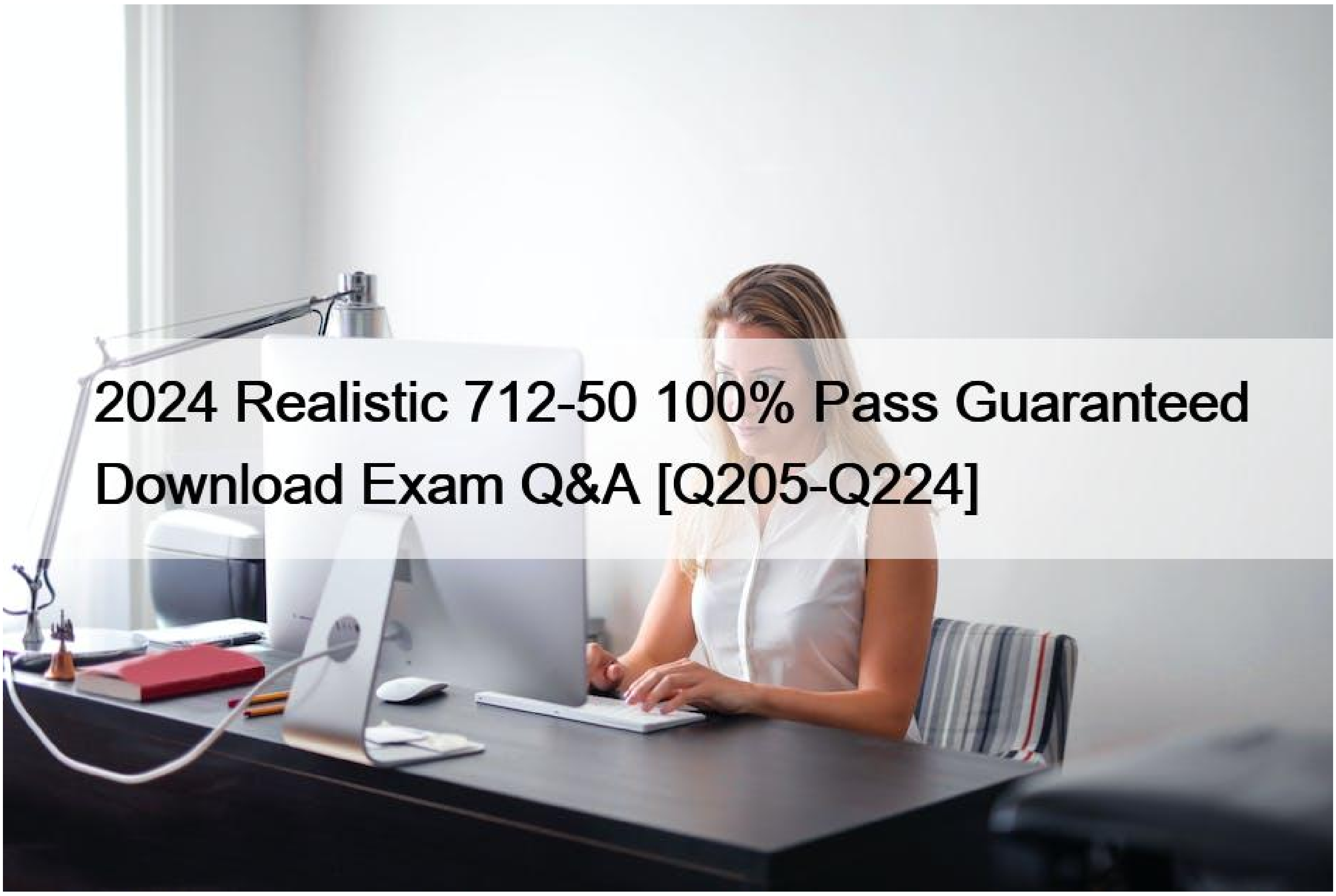
# 2024 Realistic 712-50 100% Pass Guaranteed Download Exam Q&A [Q205-Q224


2024 Realistic 712-50 100% Pass Guaranteed
Download Exam Q&A [Q205-Q224]

**2024 Realistic 712-50 100% Pass Guaranteed Download  Exam Q&A Accurate 712-50 Answers 365 Days Free Updates**

The EC-Council Certified CISO (CCISO) certification is a globally recognized certification program that validates the knowledge, skills, and abilities of professionals in the field of information security. The EC-Council 712-50 exam is a critical step towards becoming a certified CISO. 712-50 exam covers five critical domains, and candidates must have at least five years of experience in three or more of these domains to be eligible to take the exam. The CCISO certification is highly respected by employers and is a testament to the skills and expertise of an individual in the field of information security.

EC-COUNCIL 712-50 exam is a challenging exam that requires candidates to have a deep understanding of the principles, concepts, and best practices of information security management. Candidates must also have a solid foundation in technical security controls, as well as a strong understanding of the business and regulatory environment in which they operate.

**NEW QUESTION 205**

An organization has implemented a change management process for all changes to the IT production environment. This change

management process follows best practices and is expected to help stabilize the availability and integrity of the organization&#8217;s IT environment. Which of the following can be used to measure the effectiveness of this newly implemented process:
* Number of change orders rejected
* Number and length of planned outages
* Number of unplanned outages
* Number of change orders processed

**NEW QUESTION 206**

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.

Which of the following is the reason the CISO has not been able to advance the security agenda in this organization?
* Lack of identification of technology stake holders
* Lack of business continuity process
* Lack of influence with leaders outside IT
* Lack of a security awareness program

**NEW QUESTION 207**

Which of the following international standards can be BEST used to define a Risk Management process in an organization?
* National Institute for Standards and Technology 800-50 (NIST 800-50)
* International Organization for Standardizations &#8211; 27005 (ISO-27005)
* Payment Card Industry Data Security Standards (PCI-DSS)
* International Organization for Standardizations &#8211; 27004 (ISO-27004)
ECCouncil 712-50 : Practice Test

**NEW QUESTION 208**

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.

Which of the following will be most helpful for getting an Information Security project that is behind schedule back on schedule?
* Upper management support
* More frequent project milestone meetings
* More training of staff members
* Involve internal audit
Scenario10

**NEW QUESTION 209**

When is an application security development project complete?
* When the application is retired.
* When the application turned over to production.
* When the application reaches the maintenance phase.
* After one year.

**NEW QUESTION 210**

An access point (AP) is discovered using Wireless Equivalent Protocol (WEP). The ciphertext sent by the AP is encrypted with the same key and cipher used by its stations. What authentication method is being used?
* Shared key
* Asynchronous
* Open
* None

**NEW QUESTION 211**

A method to transfer risk is to______________.
* Implement redundancy
* Move operations to another region
* Alignment with business operations
* Purchase breach insurance

**NEW QUESTION 212**

Which of the following is the MOST effective method for discovering common technical vulnerabilities within the IT environment?
* Reviewing system administrator logs
* Auditing configuration templates
* Checking vendor product releases
* Performing system scans

**NEW QUESTION 213**

What is the primary reason for performing vendor management?
* To understand the risk coverage that are being mitigated by the vendor
* To establish a vendor selection process
* To document the relationship between the company and the vendor
* To define the partnership for long-term success

**NEW QUESTION 214**

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?
* Data breach disclosure
* Consumer right disclosure
* Security incident disclosure
* Special circumstance disclosure

**NEW QUESTION 215**

Which of the following is the MOST important for a CISO to understand when identifying threats?
* How vulnerabilities can potentially be exploited in systems that impact the organization
* How the security operations team will behave to reported incidents
* How the firewall and other security devices are configured to prevent attacks
* How the incident management team prepares to handle an attack

**NEW QUESTION 216**

A CISO implements smart cards for credential management, and as a result has reduced costs associated with help desk operations supporting password resets.

This demonstrates which of the following principles?
* Increased security program presence
* Regulatory compliance effectiveness
* Security organizational policy enforcement
* Proper organizational policy enforcement

**NEW QUESTION 217**

Which regulation or policy governs protection of personally identifiable user data gathered during a cyber investigation?
* ITIL
* Privacy Act
* Sarbanes Oxley
* PCI-DSS

**NEW QUESTION 218**

A recent audit has identified a few control exceptions and is recommending the implementation of technology and processes to address the finding.

Which of the following is the MOST likely reason for the organization to reject the implementation of the recommended technology and processes?
* The organization has purchased cyber insurance
* The risk tolerance of the organization permits this risk
* The CIO of the organization disagrees with the finding
* The auditors have not followed proper auditing processes

**NEW QUESTION 219**

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

**NEW QUESTION 220**

The company decides to release the application without remediating the high-risk vulnerabilities. Which of the following is the MOST likely reason for the company to release the application?
* The company lacks a risk management process
* The company does not believe the security vulnerabilities to be real
* The company has a high risk tolerance
* The company lacks the tools to perform a vulnerability assessment

**NEW QUESTION 221**

A missing/ineffective security control is identified.

Which of the following should be the NEXT step?
*  Perform an audit to measure the control formally
*  Escalate the issue to the IT organization
*  Perform a risk assessment to measure risk
*  Establish Key Risk Indicators

**NEW QUESTION 222**

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.

After determining the audit findings are accurate, which of the following is the MOST logical next activity?
*  Validate gaps with the Information Technology team
*  Begin initial gap remediation analyses
*  Review the security organization&#8217;s charter
*  Create a briefing of the findings for executive management

**NEW QUESTION 223**

Which of the following strategies provides the BEST response to a ransomware attack?
*  Real-time off-site replication
*  Daily incremental backup
*  Daily full backup
*  Daily differential backup

**NEW QUESTION 224**

Who is responsible for securing networks during a security incident?
*  Chief Information Security Officer (CISO)
*  Security Operations Center (SO
*  Disaster Recovery (DR) manager
*  Incident Response Team (IRT)

**712-50 dumps Exam Material with 447 Questions:** https://www.validexam.com/712-50-latest-dumps.html]