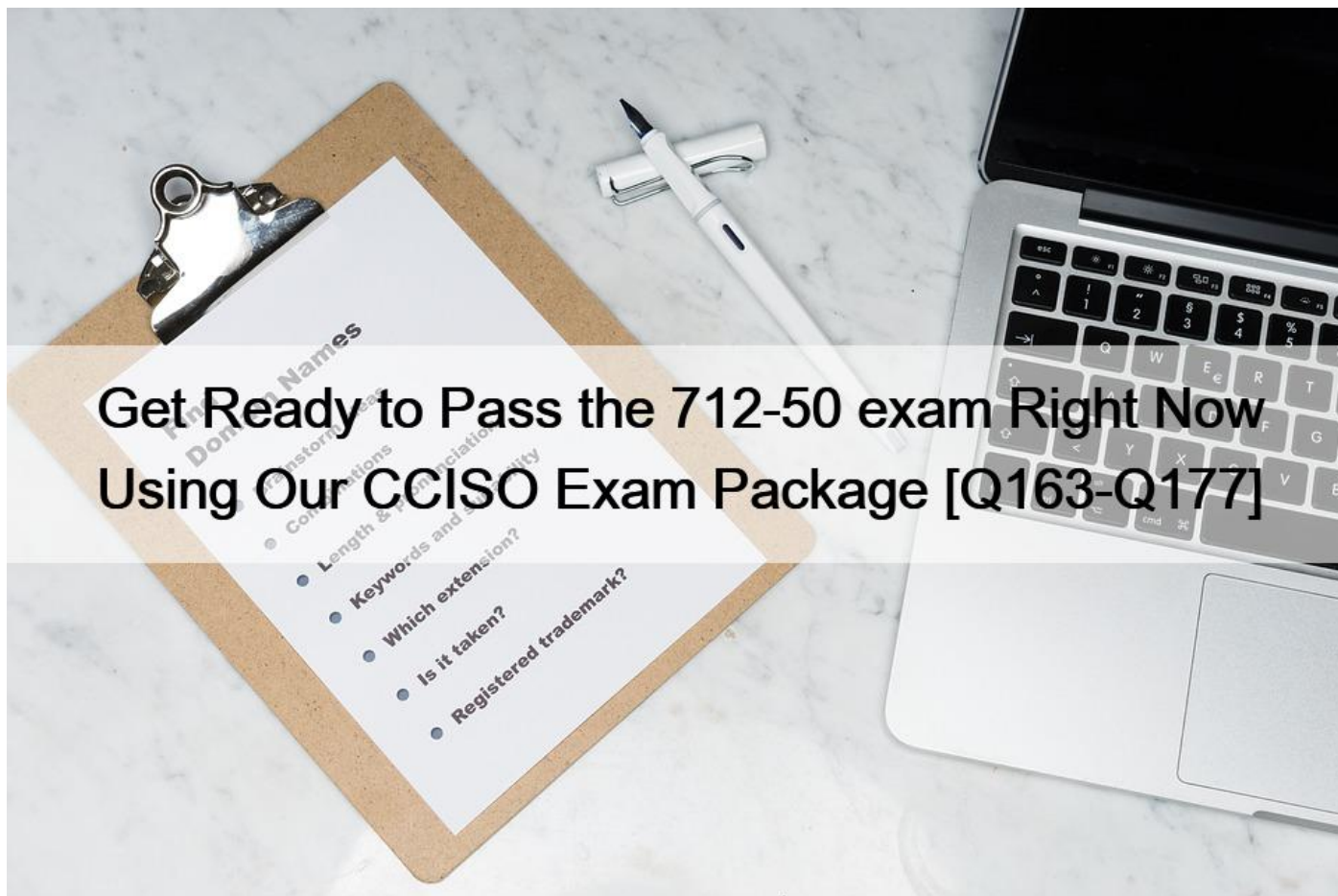


Get Ready to Pass the 712-50 exam Right Now Using Our CCISO Exam Package [Q163-Q177]



Get Ready to Pass the 712-50 exam Right Now Using Our CCISO Exam Package Enhance Your Career With Available Preparation Guide for 712-50 Exam

EC-Council 712-50: Overview EC-Council 712-50 is a certification test covering 150 multiple-choice questions that you need to answer within 2.5 hours. The exam questions require thorough evaluation and extensive thoughts. This means that the interested candidates must gain competence in the topics before attempting the test. The highlights of these subject areas covered in the exam are enumerated below: **Strategic Planning, Procurement, Finance, & 3rd-Party Management: 19%** This module covers the applicants' skills in designing, maintaining, and developing enterprise information security architecture through the alignment of business processes, local & wide area networks, IT software & hardware, projects, and operations with the overall security strategy of an organization. It is focused on the strategic planning as well and covers one's proficiency in various domains of the third-party management & finance. **Security Program Operations & Management: 21%** In this topic, you will cover the development of the clear project scope statements for every information systems project to align with the objectives of the organization. It also entails the skills in defining activities required for executing an information systems program successfully and estimating activity duration while developing staffing plans and schedules. The potential candidates also need the expertise in developing, monitoring, and managing the information systems program budgets and controlling & estimating the individual projects. It also covers the skills in everything about security program operations. **Information Security Controls & Audit Management: 20%** This area measures the students' skills in identifying the operational objectives and processes of the organization

as well as designing information systems control to align with the organizational goals and needs while conducting the tests before implementation for effectiveness. It also covers the details of the evaluation & implementation techniques and tools for automating information systems procedures. **Information Security Core Competencies: 19%** This section requires the learners' competence in identifying criteria for discretionary and mandatory access control as well as implementing & managing access control plans to align with basic principles governing access control systems. It also covers the skills in identifying various access control systems, understanding the significance of warning banners in implementing access rules, designing response plans for identifying theft incidences, as well as identifying & designing plans to overcome phishing attacks. This part also covers a broad skill range in physical security, firewall, Network Defense Systems, IDS/IPS, as well as business continuity & disaster recovery planning. The examinees should also gain the expertise in other areas, including wireless security, security of coding best practices & web applications security, virus, malware, Trojans, as well as other malicious code threats. **Governance, Compliance, & Risk: 21%** This domain requires the individuals' skills in defining, managing, maintaining, and implementing information security governance programs that entail organizational processes, structures, and leadership. The interested learners also need to understand how to align the framework of the information security governance with the organization governance and goals, including leadership style, standards, policies, and values. It also covers their skills in creating risk management program charter & policies, risk assessment framework & methodology, as well as managing risk register.

How much 712-50 Exam Cost

The price of the 712-50 exam is \$950 USD.

NEW QUESTION 163

Which of the following provides an audit framework?

- * Control Objectives for IT (COBIT)
- * International Organization Standard (ISO) 27002
- * Payment Card Industry -Data Security Standard (PCI-DSS)
- * National Institute of Standards and technology (NIST) SP 800-30

NEW QUESTION 164

Which of the following functions implements and oversees the use of controls to reduce risk when creating an information security program?

- * Risk Assessment
- * Incident Response
- * Risk Management
- * Network Security administration

NEW QUESTION 165

The amount of risk an organization is willing to accept in pursuit of its mission is known as _____.

- * risk transfer
- * risk mitigation
- * risk acceptance
- * risk tolerance

NEW QUESTION 166

In terms of supporting a forensic investigation, it is now imperative that managers, first-responders, etc., accomplish the following actions to the computer under investigation:

- * Secure the area and shut-down the computer until investigators arrive

- * Secure the area and attempt to maintain power until investigators arrive
- * Immediately place hard drive and other components in an anti-static bag
- * Secure the area.

NEW QUESTION 167

Which of the following information may be found in table top exercises for incident response?

- * Security budget augmentation
- * Process improvements
- * Real-time to remediate
- * Security control selection

NEW QUESTION 168

As the Business Continuity Coordinator of a financial services organization, you are responsible for ensuring assets are recovered timely in the event of a disaster. Which is the BEST Disaster Recovery performance indicator to validate that you are prepared for a disaster?

- * Recovery Point Objective (RPO)
- * Disaster Recovery Plan
- * Recovery Time Objective (RTO)
- * Business Continuity Plan

NEW QUESTION 169

The CIO of an organization has decided to assign the responsibility of internal IT audit to the IT team. This is consider a bad practice MAINLY because

- * The IT team is not familiar in IT audit practices
- * This represents a bad implementation of the Least Privilege principle
- * This represents a conflict of interest
- * The IT team is not certified to perform audits

NEW QUESTION 170

According to ISO 27001, of the steps for establishing an Information Security Governance program listed below, which comes first?

- * Identify threats, risks, impacts and vulnerabilities
- * Decide how to manage risk
- * Define the budget of the Information Security Management System
- * Define Information Security Policy

NEW QUESTION 171

Which of the following are the MOST important factors for proactively determining system vulnerabilities?

- * Subscribe to vendor mailing list to get notification of system vulnerabilities
- * Deploy Intrusion Detection System (IDS) and install anti-virus on systems
- * Configure firewall, perimeter router and Intrusion Prevention System (IPS)
- * Conduct security testing, vulnerability scanning, and penetration testing

NEW QUESTION 172

What is the primary reason for performing vendor management?

- * To define the partnership for long-term success
- * 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 vendor

Explanation/Reference:

NEW QUESTION 173

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:

- * Inform senior management of the risk involved.
- * Agree to work with the security officer on these shifts as a form of preventative control.
- * Develop a computer assisted audit technique to detect instances of abuses of the arrangement.
- * Review the system log for each of the late night shifts to determine whether any irregular actions occurred.

NEW QUESTION 174

Quantitative Risk Assessments have the following advantages over qualitative risk assessments:

- * They are objective and can express risk / cost in real numbers
- * They are subjective and can be completed more quickly
- * They are objective and express risk / cost in approximates
- * They are subjective and can express risk /cost in real numbers

NEW QUESTION 175

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 auditors have not followed proper auditing processes
- * The CIO of the organization disagrees with the finding
- * The risk tolerance of the organization permits this risk
- * The organization has purchased cyber insurance

NEW QUESTION 176

To have accurate and effective information security policies how often should the CISO review the organization policies?

- * Every 6 months
- * Quarterly
- * Before an audit
- * At least once a year

NEW QUESTION 177

An organization is required to implement background checks on all employees with access to databases containing credit card information. This is considered a security_____.

- * Technical control
- * Management control
- * Procedural control
- * Administrative control

Explanation/Reference:

Get Special Discount Offer of 712-50 Certification Exam Sample Questions and Answers:

<https://www.examcollectionpass.com/EC-COUNCIL/712-50-practice-exam-dumps.html>