EDUSUM
#1 Online Certification Guide

EC-COUNCIL 712-50

EC-Council CCISO Certification Questions & Answers

Exam Summary – Syllabus –Questions

712-50
EC-Council Certified Chief Information Security Officer (CCISO)
150 Questions Exam – 72% Cut Score – Duration of 150 minutes

Table of Contents:

Know Your 712-50 Certification Well:

The 712-50 is best suitable for candidates who want to gain knowledge in the EC-Council Cyber Security. Before you start your 712-50 preparation you may struggle to get all the crucial CCISO materials like 712-50 syllabus, sample questions, study guide.

But don't worry the 712-50 PDF is here to help you prepare in a stress free manner. The PDF is a combination of all your queries like-

- What is in the 712-50 syllabus?
- How many questions are there in the 712-50 exam?
- Which Practice test would help me to pass the 712-50 exam at the first attempt?

Passing the 712-50 exam makes you EC-Council Certified Chief Information Security Officer (CCISO). Having the CCISO certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

EC-Council 712-50 CCISO Certification Details:

Exam Name	EC-Council Certified Chief Information Security Officer (CCISO)
Exam Code	712-50
Exam Price	$999 (USD)
Duration	150 mins
Number of Questions	150
Passing Score	72%
Books / Training	Courseware
Schedule Exam	Pearson VUE OR ECC Exam Center
Sample Questions	EC-Council CCISO Sample Questions
Practice Exam	**EC-Council 712-50 Certification Practice Exam**

712-50 Syllabus:

Topic	Details
Governance, Risk, Compliance - 21%	
Governance	- Define, implement, manage and maintain an information security governance program that includes leadership, organizational structures, and processes. - Align information security governance framework with organizational goals and governance, i.e., leadership style, philosophy, values, standards, and policies. - Establish information security management structure. - Establish a framework for information security governance monitoring (considering cost/benefits analyses of controls and ROI). - Understand standards, procedures, directives, policies, regulations, and legal issues that affect the information security program. - Understand the enterprise information security compliance program and manage the compliance team.
Risk Management	- Create a risk management program policy and charter - Create a risk assessment methodology and framework - Create and manage risk register - Create risk assessment schedule and check lists - Create risk reporting metrics and processes
Compliance	- Analyze and understand common external laws, regulations, standards, best practices applicable to the organization, and organizational ethics. - Be familiar with international security and risk standards such as ISO 27000 and 31000 series - Implement and manage information security strategies, plans, policies, and procedures to reduce regulatory risk - Understand the importance of regulatory information security organizations and appropriate industry groups and stakeholders - Understand information security changes, trends, and best practices - Understand and manage enterprise compliance program controls, information security compliance process and procedures, compliance auditing, and certification programs - Understand the information security compliance process and procedures - Compile, analyze, and report compliance programs

Topic	Details
	- Understand the compliance auditing and cortication programs - Follow organizational ethics

Information Security Controls and Audit Management - 20%

Topic	Details
Information Security Management Controls	- Identify the organization's operational process and objectives - Design information systems controls in alignment with the operational needs and goals and conduct testing prior to implementation to ensure effectiveness - Identify and select the resources required to effectively implement and maintain information systems controls. Such resources can include human capital, information, infrastructure, and architecture (e.g., platforms, operating systems, networks, databases, applications) - Design and implement information systems controls to mitigate risk. Monitor and document the information systems control performance in meeting organizational objectives by identifying and measuring metrics and key performance indicators - Design and conduct testing of information security controls to ensure effectiveness, discover deficiencies, and ensure alignment with the organization's risk management program - Design and implement processes to appropriately remediate deficiencies and evaluate problem management practices to ensure that errors are recorded, analyzed, and resolved in a timely manner - Assess and implement tools and techniques to automate information systems control processes. - Measure, manage, and report on security control implementation and effectiveness
Audit Management	- Understand the IT audit process and be familiar with IT audit standards - Apply information systems audit principles, skills and techniques in reviewing and testing information systems technology and applications to design and implement a thorough risk-based IT audit strategy - Execute the audit process in accordance with established standards and interpret results against defined criteria to ensure that the information systems are protected, controlled and effective in supporting organization's objectives - Evaluate audit results, weighing the relevancy, accuracy, and perspective of conclusions against the accumulated audit evidence - Assess the exposures resulting from ineffective or missing control practices and formulate a practical and cost-effective plan to

Topic	Details
	improve those areas - Develop an IT audit documentation process and share reports with relevant stakeholders as the basis for decision-making - Ensure that the necessary changes based on the audit findings are effectively implemented in a timely manner
Security Program Management & Operations - 21%	
Security Program Management	- For each information systems project develop a clear project scope statement in alignment with organizational objectives - Define activities needed to successfully execute the information systems program, estimate activity duration, and develop a schedule and staffing plan - Develop, manage and monitor the information systems program budget, estimate and control costs of individual project - Identify, negotiate, acquire and manage the resources needed for successful design and implementation of the information systems program (e.g., people, infrastructure, and architecture) - Acquire, develop and manage information security project team - Assign clear information security personnel job functions and provide continuous training to ensure effective performance and accountability - Direct information security personnel and establish communications, and team activities, between the information systems team and other security-related personnel (e.g., technical support, incident management, security engineering)
Security Program Operations	- Resolve personnel and teamwork issues within time, cost, and quality constraints - Identify, negotiate and manage vendor agreement and community - Participate with vendors and stakeholders to review/assess recommended solutions; identify incompatibilities, challenges, or issues with proposed solutions - Evaluate the project management practices and controls to determine whether business requirements are achieved in a cost-effective manner while managing risks to the organization - Develop a plan to continuously measure the effectiveness of the information systems projects to ensure optimal system performance - Identify stakeholders, manage stakeholders' expectations, and communicate effectively to report progress and performance - Ensure that necessary changes and improvements to the information systems processes are implemented as required

Topic	Details
Information Security Core Competencies - 19%	
Access Control	- Identify the criteria for mandatory and discretionary access control, understand the different factors that help in implementation of access controls and design an access control plan - Implement and manage an access control plan in alignment with the basic principles that govern the access control systems such as need-to-know - Identify different access control systems such as ID cards and biometrics - Understand the importance of warning banners for implementing access rules - Develop procedures to ensure system users are aware of their IA responsibilities before granting access to the information systems
Social Engineering, Phishing Attacks, Identity Theft	- Understand various social engineering concepts and their role in insider attacks and develop best practices to counter social engineering attacks - Design a response plan to identity theft incidences - Identify and design a plan to overcome phishing attacks
Physical Security	- Identify standards, procedures, directives, policies, regulations, and laws for physical security - Determine the value of physical assets and the impact if unavailable - Design, implement and manage a comprehensive, coordinated, and holistic physical security plan to ensure overall organizational security including an audit schedule and performance metrics
Disaster Recovery and Business Continuity Planning	- Develop, implement, and monitor business continuity, business recovery, contingency planning, and disaster recovery plans in case of disruptive events and ensure alignment with organizational goals andobjectives - Direct contingency planning, operations, and programs to manage risk - Design documentation process as part of the continuity of operations program - Design and execute a testing and updating plan for the continuity of operations program - Understand the importance of integration of IA requirements into the Continuity of Operations Plan (COOP).
Firewall, IDS/IPS and Network Defense Systems	- Understand and manage network cloud security - Identify the appropriate intrusion detection and prevention systems for organizational information security

Topic	Details
	- Design and develop a program to monitor firewalls and identify firewall configuration issues - Understand perimeter defense systems such as grid sensors and access control lists on routers, firewalls, and other network devices - Identify the basic network architecture, models, protocols and components such as routers and hubs that play a role in network security - Understand the concept of network segmentation - Manage DMZs, VPN and telecommunication technologies such as PBX and VoIP - Identify network vulnerabilities and explore network security controls such as use of SSL and TLS for transmission security - Support, monitor, test, and troubleshoot issues with hardware and software - Manage accounts, network rights, and access to systems and equipment
Wireless Security	- Identify vulnerability and attacks associated with wireless networks and manage different wireless network security tools
Virus, Trojans and Malware, and other Malicious Code Threats	- Assess the threat of virus, Trojan and malware to organizational security and identify sources and mediums of malware infection - Deploy and manage anti-virus systems - Develop process to counter virus, Trojan, and malware threats including training both security teams and non-security teams on secure development processes
Secure Coding Best Practices and Securing Web Applications	- Develop and maintain software assurance programs in alignment with the secure coding principles and each phase of System Development Life Cycle (SDLC) - Understand various system-engineering practices - Configure and run tools that help in developing secure programs - Understand software vulnerability analysis techniques including static code, dynamic code, and software composition analysis. - Install and operate the IT systems in a test configuration manner that does not alter the program code or compromise security safeguards - Identify web application vulnerabilities and attacks and web application security tools to counter attacks
OS Hardening	- Identify various OS vulnerabilities and attacks and develop a plan for hardening OS systems - Understand system logs, patch management process and configuration management for information system security

Topic	Details
Encryption Technologies	- Understand the concept of encryption and decryption, digital certificates, public key infrastructure and the key differences between cryptography and steganography - Identify the different components of a cryptosystem - Develop a plan for information security encryption techniques
Vulnerability Assessment and Penetration Testing	- Design, develop and implement a penetration testing program based on penetration testing methodology to ensure organizational security - Identify different vulnerabilities associated with information systems and legal issues involved in penetration testing - Develop pre and post testing procedures - Develop a plan for pen test reporting and implementation of technical vulnerability corrections - Develop vulnerability management systems
Threat Management	- Create and manage a threat management program including threat intelligence, third-party threats, and security bulletins regarding hardware and software, particularly open-source software
Incident Response and Computer Forensics	- Develop a plan to identify a potential security violation and take appropriate action to report the incident - Comply with system termination procedures and incident reporting requirements related to potential security incidents or actual breaches - Assess potential security violations to determine if the network security policies have been breached, assess the impact, and preserve evidence - Diagnose and resolve IA problems in response to reported incidents - Design incident response procedures including testing, table top exercises, and playbooks - Develop guidelines to determine whether a security incident is indicative of a violation of law that requires special legal action - Identify the volatile and persistent system information - Set up and manage forensic labs and programs - Understand various digital media devices, e-discovery principles and practices and different file systems - Develop and manage an organizational digital forensic program - Establish, develop and manage forensic investigation teams - Design investigation processes such as evidence collection, imaging, data acquisition, and analysis - Identify the best practices to acquire, store and process digital evidence

Topic	Details
	- Configure and use various forensic investigation tools - Design anti-forensic techniques

Strategic Planning, Finance, Procurement, and Third-Party Management - 19%

Topic	Details
Strategic Planning	- Design, develop and maintain enterprise information security architecture (EISA) by aligning business processes, IT software and hardware, local and wide area networks, people, operations, and projects with the organization's overall security strategy - Perform external analysis of the organization (e.g., analysis of customers, competitors, markets and industry environment) and internal analysis (risk management, organizational capabilities, performance measurement etc.) and utilize them to align information security program with organization's objectives - Identify and consult with key stakeholders to ensure understanding of organization's objectives - Define a forward-looking, visionary and innovative strategic plan for the role of the information security program with clear goals, objectives and targets that support the operational needs of the organization - Define key performance indicators and measure e effectiveness on continuous basis - Assess and adjust security resources to ensure they support the organization's strategic objectives - Monitor and update activities to ensure accountability and progress
Finance	- Analyze, forecast and develop the operational budget of the security department - Acquire and manage the necessary resources for implementation and management of information security plan - Allocate financial resources to projects, processes and units within information security program - Monitor and oversee cost management of information security projects, return on investment (ROI) of key purchases related to IT infrastructure and security and ensure alignment with the strategic plan - Identify and report financial metrics to stakeholders - Balance the IT security investment portfolio based on EISA considerations and enterprise security priorities - Understand the acquisition life cycle and determine the importance of procurement by performing Business Impact Analysis

Topic	Details
	- Identify different procurement strategies and understand the importance of costbenefit analysis during procurement of an information system - Understand the basic procurement concepts such as Statement of Objectives (SOO), Statement of Work (SOW), and Total Cost of Ownership (TCO) - Collaborate with various stakeholders (which may include internal client, lawyers, IT security professionals, privacy professionals, security engineers, suppliers, and others) on the procurement of IT security products and services - Include risk-based security requirements in acquisition plans, cost estimates, statements of work, contracts, and evaluation factors for award, service level agreements, and other pertinent procurement documents - Design vendor selection process and management policy - Develop contract administration policies that direct the evaluation and acceptance of delivered IT security products and services under a contract, as well as the security evaluation of IT and software being procured - Develop measures and reporting standards to measure and report on key objectives in procurements aligned with IT security policies and procedures - Understand the IA security requirements to be included in statements of work and other appropriate procurement documents
Third Party Management	- Design third party selection process - Design third party management policy, metrics, and processes - Design and manage the third party assessment process including ongoing compliance management - Develop measures and reporting standards to measure and report on key objectives in procurements aligned with IT security policies and procedures - Include risk-based security requirements in acquisition plans, cost estimates, statements of work, contracts, and evaluation factors for award, service level agreements, and other pertinent procurement documents - Understand the security, privacy, and compliance requirements to be included in Statements of Work (SOW), Master Service Agreements (MSA), and other appropriate procurement documents

EC-Council 712-50 Sample Questions:

Question: 1

A disgruntled employee breaks into the organization and steals critical data after finding out he will be laid off due to downsizing. This is an example of what type of physical security threat?

a) Manmade threat
b) Natural threat
c) Environmental threat
d) Supply system threat

Answer: a

Question: 2

A publicly traded company collects cardholder data in the course of business operations. The organization's CEO recognizes the importance of information security and hires a CISO. Which of the following must the CISO ensure the business is compliant

with?

a) GDPR and FISMA
b) PCI DSS and GDPR
c) PCI DSS and SOX
d) GDPR and SOX

Answer: c

Question: 3

Of the methods listed, what is the best countermeasure against social engineering attacks?

a) Training
b) Practice and drills
c) Observation
d) Reading

Answer: b

Question: 4

An organization wants to purchase a turnkey inventory management system consisting of hardware and software. The organization wants to keep the price low, but its most important criteria are the experience and capabilities of the contractor.

Which procurement method is best for this situation?

a) Best value
b) Lowest price technically acceptable (LPTA)
c) Cost plus
d) Time and materials

Answer: a

Question: 5

The CISO is writing an organization security policy. This is an example of which of the following control types?

a) Administrative
b) Technical
c) Physical
d) Detective

Answer: a

Question: 6

Which of the following best describes the critical path in project management?

a) Activities that, if changed, will change the end date of the project
b) Activities that will change the end date of the project
c) Activities that are critical to the project
d) Activities that are not critical to the project

Answer: d

Question: 7

NIST SP 800-53 outlines management, operational, and technical classes. Which of the following NIST control families is an example of a management control class?

    a) Risk Assessment
    b) Awareness and Training
    c) Physical and Environmental Protection
    d) Personnel Security

Answer: a

Question: 8

Which of the following would not be considered an essential component of the strategic planning process?

    a) Select the right people to be on the team
    b) Acquire a planning tool
    c) Select a model to follow
    d) Set a schedule

Answer: b

Question: 9

A security analyst is reviewing the security logs of a web server for indicators of compromise. Which of the following control functionalities is this an example of?

    a) Detective
    b) Preventive
    c) Recovery
    d) Directive

Answer: a

Question: 10

An e-commerce site that accepts online payment is expanding and hires a CISO to ensure that the organization is complying with industry regulations and standards.

Which of the following fraameworks is of greatest concern to the CISO for ensuring compliance?

a) SOX
b) FISMA
c) ISO/IEC 27001
d) PCI DSS

Answer: d

Study Guide to Crack EC-Council CCISO 712-50 Exam:

- Getting details of the 712-50 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the 712-50 exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the EC-Council provided training for 712-50 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the 712-50 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on 712-50 practice tests is must. Continuous practice will make you an expert in all syllabus areas.

Reliable Online Practice Test for 712-50 Certification

Make EduSum.com your best friend during your EC-Council Chief Information Security Officer exam preparation. We provide authentic practice tests for the 712-50 exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual 712-50 exam. We guarantee you 100% success in your first exam attempt if you continue practicing regularly. Don't bother if you don't get 100% marks in initial practice exam attempts. Just utilize the result section to know your strengths and weaknesses and prepare according to that until you get 100% with our practice tests. Our evaluation makes you confident, and you can score high in the 712-50 exam.

Start Online practice of 712-50 Exam by visiting URL
https://www.edusum.com/ec-council/712-50-ec-council-chief-information-security-officer