THINQTANK® LEARNING

EC-COUNCIL CERTIFIED CHIEF INFORMATION SECURITY OFFICER

Exam 712-50 (CCISO)

Our Learning Exclusive

- Custom exam prep software and materials
- Exam delivery in classroom with 98% success
- Course specific thinQtank® Learning publications to promote fun exciting learning
- Extended hours of training including immersive hands-on exercises
- WE DO NOT "TEACH THE TEST" We always deliver valuable hands-on experience
- Receive all reading material and study guides when you register
- All courses taught by certified expert engineers

Course Duration

- Five days of instructor-led learning
- 90% lecture, 10% hands-on labs/demonstrations

Prerequisites

- Candidates must submit the Exam Eligibility Application proving they have at least five years of experience in each of the five CCISO domains.

Target Audience

- CCISO certification is beneficial to IT consultants, managers, security policy writers, privacy officers, information security officers, network administrators, security device administrators, and security engineers.

Exam Information

- 712-50 – Certified Chief Information Security Officer

Delivery Methods

- Instructor-Led Training
- Immersive Live-Online Training
- On-Site and Custom Delivery

Exclusive Tools and Learning Package

- Comprehensive video training package
- CCISO Body of Knowledge 11th hour package
- iLearn Self-Paced Online Security Management Training Package
- Value-added evening review sessions covering 100% up-to-date materials on the latest version of the CCISO exam

EC-Council Accredited Training Center

thinQtank® LEARNING

Course Overview

thinQtank® Learning is offering a unique five-day training camp comprised of five days of instructor-led learning for Certified Chief Information Security Officer. As with all our EC-Council Training Experiences – exams are delivered in the classroom.

The CCISO Certification is an industry-leading program that recognizes the real-world experience necessary to succeed at the highest executive levels of information security. Bringing together all the components required for a C-Level positions, the CCISO program combines audit management, governance, IS controls, human capital management, strategic program development, and the financial expertise vital to leading a highly successful IS program. Material in the CCISO Program assumes a high-level understanding of technical topics and doesn't spend much time on strictly technical information, but rather on the application of technical knowledge to an information security executive's day-to-day work. The CCISO aims to bridge the gap between the executive management knowledge that CISOs need and the technical knowledge that many aspiring CISOs have. This can be a crucial gap as practitioners endeavor to move from mid-management to upper, executive management roles. Much of this is traditionally learned as on the job training, but the CCISO Training Program can be the key to a successful transition to the highest ranks of information security management.

Our instructors are well-versed in accelerated learning concepts and exam preparation. During our CCISO boot camp, the experience of working with thousands of exam takers give our team unique insight into the learning requirements needed for success. They are recognized industry experts in the fields of cyber security, risk management, and business continuity.

Application Process

To qualify to take the CCISO Exam, applicants must fill out the CCISO Exam Eligibility Application. Applications should be emailed to cciso@eccouncil.org. If the applicant is attempting the exam without taking EC-Council Authorized Training, five years of experience in each of the five CCISO Domains is required (experience can be overlapping) and a $100 application fee is due with the application. If an applicant has purchased EC-Council Authorized Training, there is no application fee due and only five years of experience in three of the five domains is required. Application processing time varies since part of the process involves reaching out to verifiers indicated by the applicants as able to verify their experience. To speed up this process, applicants can assist the application processing team by reaching out to their verifiers to ensure they have received the required forms from EC-Council and understand what is required. Applications from students in EC-Council Authorized Training are prioritized and expedited to ensure testing can occur at the time of the class if the student desires.

EC-COUNCIL CERTIFIED CHIEF INFORMATION SECURITY OFFICER

Exam 712-50 (CCISO)

Course Modules

GOVERNANCE AND RISK MANAGEMENT (21%)

- Define, Implement, Manage, and Maintain an Information Security Governance Program
- Information Security Drivers
- Establishing an information security management structure
- Laws/Regulations/Standards as drivers of Organizational Policy/Standards/Procedures
- Managing an enterprise information security compliance program
- Introduction to Risk Management

INFORMATION SECURITY CONTROLS, COMPLIANCE, AND AUDIT MANAGEMENT (20%)

- Information Security Controls
- compliance Management
- Guidelines, Good and Best Practices
- Audit Management

SECURITY PROGRAM MANAGEMENT & OPERATIONS (21%)

- Program Management
- Operations Management

INFORMATION SECURITY CORE COMPETENCIES (19%)

- Access Control
- Physical Security
- Network Security
- Wireless Security
- Endpoint Protection
- Application Security
- Encryption Technologies
- Virtualization Security
- Cloud Computing Security

STRATEGIC PLANNING, FINANCE, PROCUREMENT AND VENDOR MANAGEMENT (19%)

- Strategic Planning
- Designing, Developing, and Maintaining an Enterprise Information Security Program
- Understanding the Enterprise Architecture (EA)
- Finance
- Procurement
- Vendor Management

EC-COUNCIL CCISO EXAM REVIEW

- Exam Structure
- Exam Registration Process
- Time Management
- Topics and Concepts
- CCISO Certification Question Structure
- Vendor Interpretation Techniques

EC-COUNCIL CERTIFIED CHIEF INFORMATION SECURITY OFFICER

Exam 712-50 (CCISO)

CCISO Body of Knowledge Details

DOMAIN 1 – 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 framework for information security governance monitoring (considering cost/benefits analyses controls/ROI).
- Understand standards, procedures, directives, policies, regulations, legal issues that affect information security program.
- Understand the enterprise information security compliance program and manage the compliance team.

DOMAIN 1 – 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/appropriate industry groups/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
- Understand the compliance auditing and cortication programs
- Follow organizational ethics

DOMAIN 1 – 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

DOMAIN 2 – 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

EC-COUNCIL CERTIFIED CHIEF INFORMATION SECURITY OFFICER

Exam 712-50 (CCISO)

CCISO Body of Knowledge Details Continued

DOMAIN 2 – 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 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

DOMAIN 3 – 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)

DOMAIN 3 – 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

EC-COUNCIL CERTIFIED CHIEF INFORMATION SECURITY OFFICER

Exam 712-50 (CCISO)

CCISO Body of Knowledge Details Continued

DOMAIN 4 – 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

DOMAIN 4 – 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

DOMAIN 4 – 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

DOMAIN 4 – 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 and objectives
- 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).

DOMAIN 4 – 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
- 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

DOMAIN 4 – WIRELESS SECURITY

- Identify vulnerability and attacks associated with wireless networks and manage different wireless network security tools

EC-COUNCIL CERTIFIED CHIEF INFORMATION SECURITY OFFICER

Exam 712-50 (CCISO)

CCISO Body of Knowledge Details Continued

DOMAIN 4 – 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

DOMAIN 4 – 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

DOMAIN 4 – 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

DOMAIN 4 – 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

DOMAIN 4 – 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

DOMAIN 4 – 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

EC-COUNCIL CERTIFIED CHIEF INFORMATION SECURITY OFFICER
Exam 712-50 (CCISO)

CCISO Body of Knowledge Details Continued

DOMAIN 4 – 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
- Configure and use various forensic investigation tools
- Design anti-forensic techniques

DOMAIN 5 – 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

EC-COUNCIL CERTIFIED CHIEF INFORMATION SECURITY OFFICER

Exam 712-50 (CCISO)

CCISO Body of Knowledge Details Continued

DOMAIN 5 – 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
- Identify different procurement strategies and understand the importance of cost benefit 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

DOMAIN 5 – 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 CERTIFIED CHIEF INFORMATION SECURITY OFFICER

Exam 712-50 (CCISO)

thinQtank® Global, Inc. dba thinQtank® Learning P.O. Box 803215, Valencia, CA 91380 USA
Tel 855-TO-THINQ Fax 208-979-0668 www.thinqtanklearning.com