



CERTIFIED CHIEF INFORMATION SECURITY OFFICER



**Well Trained People,
Better Served Customers.**

COURSE OVERVIEW

Certified Chief Information Security Officer EC-Council's CCISO Program has certified leading information security professionals around the world. A core group of high-level information security executives, the CCISO Advisory Board, contributed by forming the foundation of the program and outlining the content that would be covered by the exam, body of knowledge, and training. Some members of the Board contributed as authors, others as exam writers, others as quality assurance checks, and still others as trainers. Each segment of the program was developed with the aspiring CISO in mind and looks to transfer the knowledge of seasoned professionals to the next generation in the areas that are most critical in the development and maintenance of a successful information security program.

DURATION: 40 HOURS | EXAM CODE: 712-50

COURSE OBJECTIVE

Upon Completion of this Course, you will accomplish following:

- Define, implement, and manage an information security governance program that includes leadership, organizational structures and processes.
- Assess the major enterprise risk factors for compliance.
- Design and develop a program to monitor firewalls and identify firewall configuration issues.
- Identify vulnerability and attacks associated with wireless networks and manage different wireless network security tools.
- Deploy and manage anti-virus systems.
- Understand various system-engineering practices.
- Identify the volatile and persistent system information.
- Develop and manage an organizational digital forensic program.
- Identify the best practices to acquire, store and process digital evidence.
- Define key performance indicators and measure effectiveness on continuous basis.
- Allocate financial resources to projects, processes and units within information security program.
- Identify and report financial metrics to stakeholders.
- Understand the IA security requirements to be included in statements of work and other appropriate procurement documents in this
- CCISO certification training program.

COURSE PREREQUISITES

Candidates interested in earning the C|CISO Certification must qualify via EC-Council's Exam Eligibility application before sitting for the C|CISO Exam. Only students with at least five years of experience in three of the five domains are permitted to sit for the C|CISO Exam. Any student who does not qualify to sit for the exam or who does not fill out the application will be permitted to take the EC-Council Information Security Manager (EISM) exam and earn that certification. EISMs may then apply for the CCISO Exam once they have achieved the required years of experience.

TARGET AUDIENCE

- This course is designed for the aspiring or sitting upper-level manager striving to advance his or her career by learning to apply their existing deep technical knowledge to business problems.

COURSE OUTLINE

Domain 1: Governance (Policy, Legal & Compliance)

- Information Security Management Program
- Defining an Information Security Governance Program
- Regulatory and Legal Compliance
- Risk Management

Domain 2 -IS Management Controls and Auditing Management

- Designing, deploying, and managing security controls
- Understanding security controls types and objectives
- Implementing control assurance frameworks
- Understanding the audit management process

Domain 3 of the C|CISO program covers the day--to--day responsibilities of a CISO, including:

- The role of the CISO
- Information Security Projects
- Integration of security requirements into other operational processes (change management, version control, disaster recovery, etc.)

Domain 4 of the CCISO program covers, from an executive perspective, the technical aspects of the CISO job including:

- Access Controls
- Physical Security
- Disaster Recovery and Business Continuity Planning
- Network Security
- Threat and Vulnerability Management
- Application Security
- System Security
- Encryption
- Vulnerability Assessments and Penetration Testing
- Computer Forensics and Incident Response

Domain 5 of the CCISO program is concerned with the area with which many more technically inclined professionals may have the least experience, including:

- Security Strategic Planning
 - Alignment with business goals and risk tolerance
 - Security emerging trends
 - Key Performance Indicators (KPI)
 - Financial Planning
 - Development of business cases for security
 - Analyzing, forecasting, and developing a capital expense budget
 - Analyzing, forecasting, and developing an operating expense budget
 - Return on Investment (ROI) and cost-benefit analysis
 - Vendor management
 - Integrating security requirements into the contractual agreement and procurement process
- Taken together, these five Domains of the C|CISO program translate to a thoroughly knowledgeable, competent executive information security practitioner.



410, AL-DANA CENTER, AL MAKTOUM ROAD DEIRA, DUBAI, UAE

 +971 55 3575426  +971 4 2238786  training@sanisoft-it.com    