Certified Chief Information Security Officer (CCISO)

Duration: 5 Days

Method: Instructor-Led (ILT) Training

Certification: *Certified Chief Information Security Officer (CCISO)*

Course Description

The Certified Chief Information Security Officer (CCISO) program is the first of its kind training and certification program aimed at producing top-level Information Security Executives. The program does not focus solely on technical knowledge but on the application of information security management principles from an executive management point of view. 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 a practitioner endeavours 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.

Target Audience

This course is intended for:

- Senior Security Officers/Professionals
- Security Auditors
- Site Administrators
- Computer Forensic Investigators
- Upper-level managers striving to advance and apply their existing technical knowledge in solving business problems
- Persons who are concerned about the integrity of their IT assets and network infrastructure

Prerequisites

To attend this course and take the exam, participants should have:

- **Minimum five (5) years** of experience in three (3) of the five (5) Domains shown in the Course Content
- Qualified via EC-Council's Exam Eligibility application before sitting the CCISO Exam

  NOTE: Candidates who do not yet meet the CCISO prerequisites but are interested in information security management or who do not want to go through the application process can pursue the *EC-Council Information Security Management (EISM)* certification.

Exam Details

Exam Tile:	• EC-Council Certified Chief Information Security Officer (CCISO)
Exam Code:	• CCISO
Length of Exam:	• 2.5 Hours
Number of Questions:	• 150
Availability:	• Pearson VUE OR ECC Exam Center
Question Format:	• Multiple Choice Questions

Course Content

Domain 1: Governance (Policy, Legal & Compliance) & Risk Management

- Definitions
- Information Security Management Program
- Information Security Laws, Regulations & Guidelines
- Privacy Laws

Domain 2: Information Security (IS) Management Controls & Auditing Management

- Design, Deploy and Manage Security Controls in Alignment with Business Goals, Risk Tolerance, and Policies and Standards
- Information Security Risk Assessment
- Risk Treatment
- Residual Risk
- Risk Acceptance
- Risk Management Feedback Loops
- Business Goals
- Risk Tolerance
- Policies and Standards
- Understanding Security Controls Types and Objectives: Management Controls, Technical Controls, Policy and Procedural Controls, Organization Controls, and more
- Implement Control Assurance Frameworks to: Define Key Performance Indicators (KPIs), Measure and Monitor Control Effectiveness, and Automate Controls
- COBIT (Control Objectives for Information and Related Technology)
- BAI06 Manage Changes
- COBIT 4.1 vs. COBIT 5
- ISO 27001/27002
- Automate Controls
- Understanding the Audit Management Process

Course Content *Continued*

Domain 3: Management – Projects and Operations (Projects, Technology & Operations)

- The Role of the CISO
- Information Security Projects
- Security Operations Management

Domain 4: Information Security Core Competencies

- Access Control
- Physical Security
- Disaster Recovery
- Network Security
- Threat and Vulnerability Management
- Application Security
- Systems Security
- Encryption
- Computer Forensics and Incident Response

Domain 5: Strategic Planning & Finance

- Introduction to Security Strategic Planning
- Alignment with Business Goals and Risk Tolerance
- The relationship between Security, Compliance, & Privacy
- Leadership
- Enterprise Information Security Architecture (EISA) Models, Frameworks and Standards
- Emerging Trends in Security
- It's all about the Data (Stradley 2009)
- Systems Certification and Accreditation Process
- Resource Planning
- Financial Planning
- Procurement
- Vendor Management
- Request for Proposal (RFP) Process
- Integrate Security Requirements into the Contractual Agreement and Procurement Process
- Statement of Work
- Service Level Agreements

ACTIVITIES INCLUDED