EC-Council Certified Chief Information Security Officer (C|CISO)

Overview

In this course, students will learn in-depth content in each of the 5 CCISO Domains

Prerequisite Comments

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

1 - Domain 1 – Governance (Policy, Legal, and Compliance)

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

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

3 - 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.)

4 - 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

5 - 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.