EC-Council Certified CISO Training CCISO v3

Course: **00080**
Filter: **Beginner**
Duration: **20 hours**
Category:: **Gouvernance, Risk and Compliance**
Price: **3000,00 €**

About Course

The Certified CISO (CCISO) EC-Council program is the first of its kind training and certification program aimed at producing top-level information security executives. The CCISO does not focus solely on technical knowledge but on applying information security management principles from an executive management point of view. Each segment of the program has been developed with the aspiring CISO in mind and looks to transfer the knowledge of seasoned professionals to the next generation in the most critical areas in developing and maintaining a successful information security program. In addition to meeting ISACA's certification requirements, passing the CISM Certification Exam meets U.S. DoD Directive 8140/8570.01 Management (IAM) Level-II, Management (IAM) Level-III and CSSP Manager requirements.

What you'll learn

- Prepare for the CCISO exam.
- Navigate the day-to-day responsibilities of a CISO.
- Consider the technical aspects of the CISO role from an executive perspective.
- Plan security and financial strategies.
- Align CISO tasks with business goals and risk tolerance.

Pre-requisites

- Five years of IS management experience in each of the 5 CCISO domains verified via the Exam Eligibility Application

Curriculum

Module 1: Governance (Policy, Legal, and Compliance)

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

Module 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

Module 3: Security Program Management & Operations

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

Module 4: Information Security Core Concepts

- 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

Module 5: Strategic Planning, Finance, & Vendor Management

- 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