Course Outline

EC-Council Chief Information Security Officer (CCISO)

Course Summary

Description

EC-Council's CCISO Program has certified leading information security professionals around the world. 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.

The Certified CISO (CCISO) 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 the application of information security management principles from an executive management point of view. The program was developed by sitting CISOs for current and aspiring CISOs.

In order to sit for the CCISO exam and earn the certification, candidates must meet the basic CCISO requirements. Candidates who do not yet meet the CCISO requirements but are interested in information security management can pursue the EC-Council Information Security Management (EISM) certification

Topics

- Governance
- Is Risk, Controls & Auditing Management
- Information Security Leadership – Projects & Operations
- ISCoreCompetencies
- Strategic Planning & Finance

Prerequisite

There are no prerequisites for this course.

Duration

Five Days

Course Outline

EC-Council Chief Information Security Officer (CCISO)

Course Outline

I. Governance

A. Information program security management
B. Information security governance program
C. Regulatory and legal compliance
D. Risk management

II. Is Risk, Controls & Auditing Management

A. Design, Deploy and Manage Security Controls
B. Security Control Types and Objectives
C. Implement Control Assurance Frameworks Audit Management

III. Information Security Leadership – Projects & Operations

A. The role of the CISO
B. Information security projects
C. Integration of security requirements into other operational processes (change management, version control, disaster recovery, etc.)

IV. ISCoreCompetencies

A. Access controls
B. Physical security
C. Disaster recovery and business continuity planning
D. Network security
E. Threat and vulnerability management
F. Application security
G. Encryption
H. Vulnerability assessments and penetration testing
I. Computer forensics and incident response

V. Strategic Planning & Finance

A. Security Strategic Planning
B. Alignment with Business Goals and Risk Tolerance
C. Security emerging trends
D. Key Performance Indicators (KPI)
E. Financial Planning
F. Development of business cases for security
G. Analyzing, forecasting, and developing a capital expense budget
H. Analyzing, forecasting, and developing an operating expense budget
I. Return on investment (ROI) and cost-benefit analysis
J. Vendor management
K. Integrating security requirements into the contractual agreement and procurement process
L. Taken together, these five domains translate to a thoroughly knowledgeable, competent executive information security practitioner