CERTIFIED CHIEF INFORMATION SECURITY OFFICER

DURATION: 5 DAYS

COURSE OVERVIEW

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.

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.

COURSE OBJECTIVES

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

Domain 1: Governance (Policy, Legal & Compliance)

1. The first Domain of the C|CISO program is concerned with the following:
2. Information Security Management Program
3. Defining an Information Security Governance Program
4. Regulatory and Legal Compliance
5. Risk Management

Domain 2 -- IS Management Controls and Auditing Management

1. Designing, deploying, and managing security controls
2. Understanding security controls types and objectives
3. Implementing control assurance frameworks
4. Understanding the audit management process

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

1. The role of the CISO
2. Information Security Projects
3. 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:

1. Access Controls
2. Physical Security
3. Disaster Recovery and Business Continuity Planning
4. Network Security
5. Threat and Vulnerability Management
6. Application Security
7. System Security
8. Encryption
9. Vulnerability Assessments and Penetration Testing
10. 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:

1. Security Strategic Planning
2. Alignment with business goals and risk tolerance
3. Security emerging trends
4. Key Performance Indicators (KPI)
5. Financial Planning
6. Development of business cases for security
7. Analyzing, forecasting, and developing a capital expense budget
8. Analyzing, forecasting, and developing an operating expense budget
9. Return on Investment (ROI) and cost-benefit analysis

10. Vendor management
11. 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.