INFOSECTRAIN
Educate. Excel. Empower.

EC-Council Accredited Training Center

CCISO

Certified Chief Information Security Officer

Training & Certification

INFOSECTRAIN

Course Highlights

- **40-Hour LIVE** Instructor-Led Training
- Learn with Real-world Scenarios
- Training Certificate
- Highly Interactive and Dynamic Sessions
- **98%** Success Rate
- Learn from Industry Experts
- Career Guidance and Mentorship
- Extended Post Training Support
- Access to Recorded Sessions

INFOSECTRAIN

About Course

CISO, or Chief Information Security Officer, is an established top-level executive position in the industry, similar to CEO or CTO. CISO is the highest-level executive in an organization charged with information security.

The CCISO certification training aims to provide the learners with comprehensive knowledge and skills regarding the information security domain. The Chief Information Security Officer Certification Training covers vital areas such as policy setting, project management, audit management, executive strategy, contract management, and financial expertise. These areas of knowledge are essential for leading a successful IS program. The CCISO certification validates the competence of a professional in handling top-level executive tasks and in effectively leading an information security program.

Course Objectives

This CCISO Specialist training course will allow you to:

- Create an information security governance framework aligned with policies and compliance standards.
- Navigate and implement regulatory and legal compliance measures.
- Identify and mitigate information security risks effectively.
- Design and manage various security controls to protect information assets.
- Apply frameworks to evaluate and enhance control effectiveness.
- Learn the audit management process for information security.
- Manage the role of CISO and execute information security projects.
- Incorporate security requirements into operational processes.
- Understand access controls, physical security, network security, and encryption.
- Align security strategies with business goals, manage budgets, and ensure vendor compliance with security standards.

INFOSECTRAIN

Target Audience

- Network Engineers with security specialization
- Experienced IT Professionals engaged in information security management
- Those who perform CISO functions, but don't have an official title
- All the professionals who aspire to reach top-level position in information security profession

Pre-requisites

- Candidates who are sitting for the exam without training must have 5 years of experience in the 5 core CCISO domains verified via the Exam Eligibility Application.
- Candidates who have taken training must possess 3 years of IS management experience in 3 of the 5 core CCISO domains verified via the Exam Eligibility Application.

INFOSECTRAIN

Exam Information

Certification	**Certified Chief Information Security Officer (CCISO)**
Exam Format	Multiple-choice Questions
Number of Questions	150 Questions
Exam Duration	150 Minutes
Exam Language	English

Note: To maintain the quality and fairness of certification exams, the exams are offered in multiple sets with different question banks. Each question is assigned a difficulty rating, which helps determine the passing score, also known as the "cut score." Since some exam sets may be slightly more difficult than others, the cut score is determined separately for each set to ensure fair evaluation standards. Therefore, the passing score can range from 60% to 85%, depending on the exam version taken.

INFOSECTRAIN

Course Content

Domain 1 Governance (Policy, Legal, and Compliance)

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

Domain 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

Domain 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.)

Domain 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

Domain 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

INFOSECTRAIN
Educate. Excel. Empower.

Contact us

www.infosectrain.com
sales@infosectrain.com

Follow us on

Version 3