

## Certified Chief Information Security Officer

**Course Duration: 40 Hrs.**

**Course code: 712-50**

### Course Overview

The CCISO course, offered by EC-Council, aims to equip aspiring and current CISOs with the knowledge and skills needed for executive-level information security leadership, covering topics like governance, risk management, and strategic program development.

### What you'll learn?

❖ **Risk Management:**

Develop skills to assess, identify, and mitigate information security risks, aligning security programs with organizational goals.

❖ **Compliance:**

Understand and implement regulatory and legal compliance measures, ensuring adherence to industry standards and best practices.

❖ **Security Program Management:**

Learn to design, implement, and manage a comprehensive information security program, including security controls, policies, and procedures.

❖ **Strategic Planning and Finance:**

Gain expertise in aligning security strategies with business goals, managing budgets, and ensuring vendor compliance with security standards.

### Target Audience

❖ **Current CISOs:** To improve their technical and management skills and align information security programs with business goals.

❖ **Aspiring CISOs:** To develop the necessary knowledge and skills to lead information security programs.

- ❖ **Senior IT Professionals:** Including those in roles like Vice Presidents of Information Security, Information Security Directors/Managers, and CIOs involved in information security governance.
- ❖ **Information Security Consultants and Advisors:** To enhance their expertise in information security management.

## Pre-Requisites

To attend the CCISO training, there are no prerequisites, but to sit for the CCISO exam, you must demonstrate 5 years of experience in 3 of the 5 C/CISO domains, verified via EC-Council's exam eligibility application.

## Course content

### Module 1 Governance and risk management

- A. Define, Implement, Manage, and Maintain an Information Security Governance Program
- B. Information Security Drivers
- C. Establishing an information security management structure
- D. Laws/Regulations/Standards as drivers of Organizational Policy/Standards/Procedures
- E. Managing an enterprise information security compliance program
- F. Risk Management
- G. Risk mitigation, risk treatment, and acceptable risk
- H. Risk management frameworks.
- I. NIST
- J. Other Frameworks and Guidance (ISO 31000, TARA, OCTAVE, FAIR, COBIT, and ITIL)
- K. Risk management plan implementation.
- L. Ongoing third-party risk management
- M. Risk management policies and processes.
- N. Conclusion

### Module 2 Security Risk Management, Controls, & Audit Management

- A. INFORMATION SECURITY CONTROLS
- B. COMPLIANCE MANAGEMENT
- C. GUIDELINES, GOOD AND BEST PRACTICES
- D. AUDIT MANAGEMENT
- E. SUMMARY

### **Module 3 Security Program Management and Operations**

- A. PROGRAM MANAGEMENT
- B. OPERATIONS MANAGEMENT
- C. Summary

### **Module 4 Information Security Core Competencies**

- A. ACCESS CONTROL
- B. PHYSICAL SECURITY
- C. NETWORK SECURITY
- D. ENDPOINT PROTECTION
- E. APPLICATION SECURITY
- F. ENCRYPTION TECHNOLOGIES
- G. VIRTUALIZATION SECURITY
- H. CLOUD COMPUTING SECURITY
- I. TRANSFORMATIVE TECHNOLOGIES
- J. Summary

### **Module 5 Strategic Planning, Finance, Procurement and Vendor Management**

- A. STRATEGIC PLANNING
- B. Designing, Developing, and Maintaining an Enterprise Information Security Program
- C. Understanding the Enterprise Architecture (EA)
- D. FINANCE
- E. PROCUREMENT
- F. VENDOR MANAGEMENT
- G. Summary

## Exam Preference

Exam Code	712-50
Length Of Test	150 Minutes
Passing Score	Min. 72%
No. Of Questions	150

