

EC-Council Chief Certified Information Security Officer (C|CISO)

TRAINING DATASHEET

This industry-leading certificate trains professionals to succeed at the highest executive levels of the security industry.

We will equip you with the business and technical expertise: Information security management principles, Business acumen, General technical knowledge, Strategic security portfolio management, and Financial management.

COURSE SYNOPSIS

The globally renowned Chief Certified Information Security Officer (C|CISO) program, spearheaded by EC-Council, has truly revolutionized the capabilities of senior information security professionals worldwide.

With unwavering dedication, EC-Council harnessed the collective wisdom of a select group of esteemed senior information security executives within our esteemed C|CISO Advisory Board. This exceptional panel of seasoned professionals meticulously crafted the program's bedrock, delineating the comprehensive content encapsulated in the C|CISO exam, the body of knowledge, and the training program.

Through their invaluable expertise, EC-Council has empowered countless CISOs to excel in the realm of information security.

Funding Support

The following information are relevant for candidates who are seeking SSG-funding support for the course:

Assessments

Candidates must pass all prescribed tests/assessments and attain 100% competency to be eligible for funding support.

Mode of Assessment: Written Assessment, Case Study Assessment.

Statement of Attainment (SOA) from SkillsFuture Singapore:

After passing the assessment(s), you'll receive a SkillsFuture Singapore Statement of Attainment (SOA) certifying that you have achieved the following Competency Standard(s):
SNA-4021-1.1 – Security Strategy-4 .

C|CISO Detailed Course Outline

1. Governance, Risk, Compliance

- ▲ Governance
- ▲ Risk Management
- ▲ Compliance

2. Information Security Controls and Audit Management

- ▲ Information Security Management Controls
- ▲ Audit Management

3. Security Program Management & Operations

- ▲ Security Program Management
- ▲ Security Program Operations

4. Information Security Core Competencies

- ▲ Access Control
- ▲ Social Engineering, Phishing Attacks, Identity Theft
- ▲ Physical Security
- ▲ Disaster Recovery and Business Continuity Planning
- ▲ Firewall,
- ▲ IDS/IPS and Network Defense Systems
- ▲ Wireless Security
- ▲ Virus, Trojans and Malware, and other Malicious Code Threats
- ▲ Secure Coding Best Practices and Securing Web Applications
- ▲ OS Hardening
- ▲ Encryption Technologies
- ▲ Vulnerability Assessment and Penetration Testing
- ▲ Threat Management
- ▲ Incident Response and Computer Forensics

5. Strategic Planning, Finance, Procurement, and Third-Party Management

- ▲ Strategic Planning
- ▲ Finance
- ▲ Third Party Management

Learning Through War Games

The training provides wargaming sessions in all live classes, providing interactive and engaging incident modeling. In the C|CISO wargaming session, candidates participate in instructor-led war games that mimic what happens during a security breach. All aspects of what students have learned in the C|CISO course are incorporated into the exercise, reinforcing their knowledge and skills.

Duration

5-Day Instructor-Led Training

Course Overview

- ▲ **Cutting-edge knowledge**
Gain insights into the latest trends in the security industry, leadership methodologies, and security technologies.
- ▲ **A focus on risk management**
CCISO aligns with all the popular risk management frameworks.
- ▲ **Emphasis on new developments**
Such as AI, augmented reality, autonomous security operations centers, and dynamic deception.
- ▲ **Learning through war games**
Build skills with interactive sessions that mimic what happens during a security breach.
- ▲ **Financial management proficiency**
Gain expertise in budgeting and cost optimization.
- ▲ **Master the boardroom language**
Build confidence in presenting cybersecurity strategies that align with executive priorities.

WHO SHOULD ATTEND

The C|CISO certification is designed for information security professionals who want to advance their careers as a CISO or other executive-level security career path.

Existing CISOs are also encouraged to participate in this program to strengthen their security program knowledge, understand current technology principles, and sharpen their business acumen.

Certification Exam Eligibility

To take the C|CISO examination, candidates must provide proof that they have 5 years of experience in at least 3 of the 5 domains.

Experience waivers are available for some industry-accepted credentials and higher education within the field of information security.

Certification

Upon passing the C|CISO exam, candidates will receive their C|CISO certificate and associated community privileges.

The C|CISO certification is valid for 3 years from the date of issuance. After 3 years, members must adhere to the certification renewal policy as outlined in the EC-Council Continuing Education (ECE) requirements

EXAMINATION FORMAT

- ▲ Scenario-based multiple-choice questions
- ▲ 150 questions
- ▲ 2.5 hours
- ▲ Through EC-Council Exam Portal
- ▲ 60–85%, depending on exam form

CONTACT US

📍 #02-01 243 Beach Road Singapore 189754 📞 +65 6729 2976

✉️ enquiries@sapience-consulting.com

🌐 www.sapience-consulting.com