CCISO – Certified Chief Information Security Officer (e-Learning)

EC-Council

Com certificação

- **Nível:** Avançado
- **Duração:** 14h

Sobre o curso

C|CISO Program has Certified Leading Information Security Profissional around the World

Develop executive-level cybersecurity leadership skills and align security strategy with business goals.

- Based on the official EC-Council CCISO framework
- Focus on governance, risk, and strategic leadership
- Designed for current and aspiring security leaders

The Certified Chief Information Security Officer (CCISO) program is designed to bridge the gap between technical knowledge and executive leadership in cybersecurity. This course prepares experienced professionals to lead, design, and manage an organization's information security program at a strategic level.

What makes this program unique

Unlike traditional cybersecurity certifications, CCISO focuses on leadership, governance, and decision-making at the executive level. The program is developed by seasoned CISOs and emphasizes real-world application of security within business environments.

- Designed by experienced CISOs
- Focus on business-driven security strategy
- Real-world, practical approach
- Globally recognized certification

The only certification that validates both security expertise and executive leadership.

- 5 domains of executive security leadership: Govern; Lead; Operate; Secure; Strategize

- AI-enhanced governance & risk management
- Board-level communication & strategy
- Budget, finance & vendor management

Destinatários

This course is ideal for experienced information security professionals, managers, and consultants who are looking to move into executive roles or strengthen their leadership capabilities in cybersecurity.

Objetivos

What you will master:

This program is structured around five key domains that define the role of a Chief Information Security Officer.

- Governance & Risk Management
- Controls, Compliance & Audit Management
- Security Program Management & Operations
- Information Security Core Competencies
- Strategic Planning, Finance & Vendor Management

What you will achieve:

By completing this program, you will be able to:

- Lead and manage enterprise-level cybersecurity programs
- Align security initiatives with organizational strategy
- Make informed, risk-based decisions at an executive level
- Communicate effectively with senior stakeholders and board members
- Drive security transformation across the organization

Condições

Cursos E-learning EC-Council não beneficiam de isenção de IVA. Ao valor apresentado acresce IVA.

O exame da EC-Council incluído no valor do curso é, por defeito, realizado em formato remoto (online), sem custos adicionais.

Caso o formando pretenda realizar o exame presencialmente num dos Centros de Exames GALILEU/Rumos, poderá solicitar a conversão do voucher, sendo aplicada uma taxa adicional de 109,50€ + IVA.

Mensalidades (apenas para particulares): Taxa de inscrição de 10% + pagamento do valor restante em prestações flexíveis, sem juros, à escolha do cliente, através do parceiro Cofidis Pay. (Sujeito a aprovação, consulta-nos para mais informações).

Pré-requisitos

Take the C|CISO Assessment

Minimum Requirements: In order to qualify to sit for the CCISO Exam without taking any training, candidates must have five years of experience in each of the 5 CCISO domains verified via the Exam Eligibility Application. To sit for the exam after taking training, candidates must have five years of experience in three of the five CCISO Domains verified via the Exam Eligibility Application.

Metodologia

About the Exam

There are three cognitive levels tested on the CCISO exam.

- **Level 1 – Knowledge:** This cognitive level of questions is used to recall memorized facts. This is the most basic cognitive level rarely accepted on certifications as it merely recognizes the candidate's ability to memorize information. It can be effectively used when asking for basic definitions, standards or any concrete fact.
- **Level 2 – Application:** This cognitive level of questions is used to identify the candidate's ability to understand the application of a given concept. It differs from Knowledge based questions in the sense that it requires the understanding and correct applicability of a given concept – not just the concept itself. This type of question often requires additional context before the actual question is provided in the stem.
- **Level 3 – Analysis:** This cognitive level of questions is used to identify the candidate's ability to identify and resolve a problem given a series of variables and context. Analysis questions differ greatly from Application based questions in the sense that they require not only the applicability of a concept but also how a concept, given certain constraints, can be used to solve a problem.

Passing Score

In order to maintain the high integrity of our certifications exams, EC-Council Exams are provided in multiple forms (i.e., different question banks). Each form is carefully analyzed through beta testing with an appropriate sample group under the purview of a committee of subject matter experts that ensure that each of our exams not only has academic rigor but also has "real world" applicability. We also have a process to determine the difficulty rating of each question. The individual rating then contributes to an overall "Cut Score" for each exam form. To ensure each form has equal assessment standards, cut scores are set on a "per exam form" basis. Depending on which exam form is challenged, cut scores can range from 60% to 78%.

Exam Details

The CCISO exam is delivered through the EC-Council Exam Portal and consists of multiple-choice questions designed to assess both strategic and practical knowledge across the five domains.

With CCISO v4 Certification

- Qualify for CISO, CSO, VP of Security roles
- Present ROI-driven security strategies to boards
- Recognized as an executive security leader
- Drive organizational cybersecurity strategy

Programa

- Information Security Governance and Strategy
- Risk Management, Compliance and GRC
- AI, Automation & Emerging Technologies
- Leadership, Ethics, and Executive Presence
- Financial Management and Vendor Governance
- Security Operations, SOC, and Incident Management
- Technical & Architecture Foundations
- Privacy, Awareness and Security Culture

Information Security Governance and Strategy

- Design and implement strategic security programs across enterprises
- Build and manage governance structure and hierarchy
- Enterprise-wide security programs and architectures
- Modern cybersecurity leadership with AI-driven innovation

Risk Management, Compliance and GRC

- Threat, vulnerability, and risk assessment frameworks (ISO 27005, NIST)
- Global compliance: GDPR, HIPAA, SOX, PCI DSS, EU AI Act
- Security frameworks: NIST CSF, ISO 27001, COBIT, MITRE ATT&CK, Zero Trust
- Establish and manage audit programs with AI-driven auditing

AI, Automation & Emerging Technologies

- Integrate AI into risk management and predictive modeling
- Embed fairness, accountability, and transparency in AI adoption
- AI-powered predictive budgeting and forecasting
- AI and NLP tools for automated contract analysis and vendor scoring

Leadership, Ethics, and Executive Presence

- Emotional, social, and cultural intelligence for global leadership
- Lead inclusive, cross-functional cybersecurity teams
- Succession planning, talent development, and mentoring
- AI ethics and governance board participation

Financial Management and Vendor Governance

- CAPEX vs. OPEX strategies and cost-benefit analysis
- Vendor management: SLA, MSA, and contract lifecycle management
- Third-party risk and AI-driven SLA breach detection
- Procurement strategies with AI-powered vendor scoring

Security Operations, SOC, and Incident Management

- Secure architecture for AI/ML pipelines, APIs, and SOC automation
- Integrate AI into SIEM/SOAR and SOC operations
- Incident response, digital forensics, and AI-driven threat intelligence
- Performance measurement with KPIs and security metrics

Technical & Architecture Foundations

- Secure SDLC, DevSecOps, and application security testing (SAST, DAST, IAST)
- Enterprise architecture frameworks (TOGAF, Zachman, SABSA, FEAF)
- AI-driven traceability and secure AI/ML pipeline architecture
- Cryptography, encryption, hashing, and PKI management

Privacy, Awareness and Security Culture

- Build effective crisis communication strategies
- AI-personalized security awareness campaigns
- Build organizational security culture and influence behaviors
- Privacy impact assessments and global data protection compliance