Rumos valorizamos profissionais!

Certified Chief Information Security Officer (CCISO)

- **Formato do curso:** E-learning
- **Preço:** 1751€

EC-Council's Certified Chief Information Security Officer (CCISO) Program has certified leading information security professionals around the world. A core group of high-level information security executives, the CCISO Advisory Board, formed the foundation of the program and outlined the content 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 instructors.

Each segment of the program was developed with the aspiring and sitting CISO in mind and looks to transfer the knowledge of seasoned executives to the next generation of leaders in the areas that are most critical in the development and maintenance of a successful information security program.

Exame:

There are three cognitive levels tested on the CCISO exam but only two tested on the EISM 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. This level appears on both the CCISO and EISM exam.
- 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 quires additional context before the actual question is provided in the stem. This level appears on both the CCISO and EISM exam.
- 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 constrain can be used to solve a problem. This level appears on the CCISO and not on the EISM exam

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%.

Details

- Number of Questions: 150
- Test Duration: 2.5 Hours
- Test Format: Multiple Choice
- Test Delivery: ECC Exam Portal

Think You’re Ready? Take the Quiz to test your readiness!

Este curso e-learning inclui

- Acesso durante 1 ano
- Certificado de participação
- Voucher de exame de certificação

Pré-requisitos

- **Minimum Requirements for Exam:**
  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.

Programa

Domain 1: Governance and Risk Management

- **Define, Implement, Manage, and Maintain an Information Security Governance Program**
  - 1. Form of Business Organization
  - 2. Industry
  - 3. Organizational Maturity
- **Information Security Drivers**
- **Establishing an information security management structure**

    - 1. Organizational Structure
    - 2. Where does the CISO fit within the organizational structure
    - 3. The Executive CISO
    - 4. Nonexecutive CISO
- **Laws/Regulations/Standards as drivers of Organizational Policy/Standards/Procedures**
- **Managing an enterprise information security compliance program**
    - 1. Security Policy
    - 1.1. Necessity of a Security Policy
    - 1.2. Security Policy Challenges
    - 2. Policy Content
    - 2.1. Types of Policies
    - 2.2. Policy Implementation
    - 3. Reporting Structure
    - 4. Standards and best practices
    - 5. Leadership and Ethics
    - 6. EC-Council Code of Ethics
- **Introduction to Risk Management**
    - 1. Organizational Structure
    - 2. Where does the CISO fit within the organizational structure
    - 3. The Executive CISO
    - 4. Nonexecutive CISO

Domain 2: Information Security Controls, Compliance, and Audit Management

- **Information Security Controls**
    - 1. Identifying the Organization’s Information Security Needs
    - 1.1. Identifying the Optimum Information Security Framework
    - 1.2. Designing Security Controls
    - 1.3. Control Lifecycle Management
    - 1.4. Control Classification
    - 1.5. Control Selection and Implementation
    - 1.6. Control Catalog
    - 1.7. Control Maturity
    - 1.8. Monitoring Security Controls
    - 1.9. Remediating Control Deficiencies
    - 1.10. Maintaining Security Controls
    - 1.11. Reporting Controls
    - 1.12. Information Security Service Catalog
- **Compliance Management**
    - 1. Acts, Laws, and Statutes
        - 1.1. FISMA
    - 2. Regulations
        - 2.1. GDPR
    - 3. Standards
        - 3.1. ASD—Information Security Manual

        - 3.2. Basel III
        - 3.3. FFIEC
        - 3.4. ISO 00 Family of Standards
        - 3.5. NERC-CIP
        - 3.6. PCI DSS
        - 3.7. NIST Special Publications
        - 3.8. Statement on Standards for Attestation Engagements No. 16 (SSAE 16)
- **Guidelines, Good and Best Practices**
    - 1. CIS
        - 1.1. OWASP
- **Audit Management**
    - 1. Audit Expectations and Outcomes
    - 2. IS Audit Practices
        - 2.1. ISO/IEC Audit Guidance
        - 2.2. Internal versus External Audits
        - 2.3. Partnering with the Audit Organization
        - 2.4. Audit Process
        - 2.5. General Audit Standards
        - 2.6. Compliance-Based Audits
        - 2.7. Risk-Based Audits
        - 2.8. Managing and Protecting Audit Documentation
        - 2.9. Performing an Audit
        - 2.10. Evaluating Audit Results and Report
        - 2.11. Remediating Audit Findings
        - 2.12. Leverage GRC Software to Support Audits
- **Summary**

Domain 3: Security Program Management & Operations

- **Program Management**
    - 1. Defining a Security Charter, Objectives, Requirements, Stakeholders, and Strategies
        - 1.1. Security Program Charter
        - 1.2. Security Program Objectives
        - 1.3. Security Program Requirements
        - 1.4. Security Program Stakeholders
        - 1.5. Security Program Strategy Development
    - 2. Executing an Information Security Program
    - 3. Defining and Developing, Managing and Monitoring the Information Security Program
        - 3.1. Defining an Information Security Program Budget
        - 3.2. Developing an Information Security Program Budget
        - 3.3. Managing an Information Security Program Budget
        - 3.4. Monitoring an Information Security Program Budget
    - 4. Defining and Developing Information Security Program Staffing Requirements
    - 5. Managing the People of a Security Program
        - 5.1. Resolving Personnel and Teamwork Issues

        - 5.2. Managing Training and Certification of Security Team Members
        - 5.3. Clearly Defined Career Path
        - 5.4. Designing and Implementing a User Awareness Program
    - 6. Managing the Architecture and Roadmap of the Security Program
        - 6.1. Information Security Program Architecture
        - 6.2. Information Security Program Roadmap
    - 7. Program Management and Governance
        - 7.1. Understanding Project Management Practices
        - 7.2. Identifying and Managing Project Stakeholders
        - 7.3. Measuring the Effectives of Projects
    - 8. Business Continuity Management (BCM) and Disaster Recovery Planning (DRP)
    - 9. Data Backup and Recovery
    - 10. Backup Strategy
    - 11. ISO BCM Standards
        - 11.1. Business Continuity Management (BCM)
        - 11.2. Disaster Recovery Planning (DRP)
    - 12. Continuity of Security Operations
        - 12.1. Integrating the Confidentiality, Integrity and Availability (CIA) Model
    - 13. BCM Plan Testing
    - 14. DRP Testing
    - 15. Contingency Planning, Operations, and Testing Programs to Mitigate Risk and Meet Service Level Agreements (SLAs)
    - 16. Computer Incident Response
        - 16.1. Incident Response Tools
        - 16.2. Incident Response Management
        - 16.3. Incident Response Communications
        - 16.4. Post-Incident Analysis
        - 16.5. Testing Incident Response Procedures
    - 17. Digital Forensics
        - 17.1. Crisis Management
        - 17.2. Digital Forensics Life Cycle
- **Operations Management**
    - 1. Establishing and Operating a Security Operations (SecOps) Capability
    - 2. Security Monitoring and Security Information and Event Management (SIEM)
    - 3. Event Management
    - 4. Incident Response Model
        - 4.1. Developing Specific Incident Response Scenarios
    - 5. Threat Management
    - 6. Threat Intelligence
        - 6.1. Information Sharing and Analysis Centers (ISAC)
    - 7. Vulnerability Management
        - 7.1. Vulnerability Assessments
        - 7.2. Vulnerability Management in Practice
        - 7.3. Penetration Testing

        - 7.4. Security Testing Teams
        - 7.5. Remediation
    - 8. Threat Hunting
- **Summary**

Domain 4: Information Security Core Competencies

- **Access Control**
    - 1. Authentication, Authorization, and Auditing
    - 2. Authentication
    - 3. Authorization
    - 4. Auditing
    - 5. User Access Control Restrictions
    - 6. User Access Behavior Management
    - 7. Types of Access Control Models
    - 8. Designing an Access Control Plan
    - 9. Access Administration
- **Physical Security**
    - 1. Designing, Implementing, and Managing Physical Security Program
        - 1.1. Physical Risk Assessment
    - 2. Physical Location Considerations
    - 3. Obstacles and Prevention
    - 4. Secure Facility Design
        - 4.1. Security Operations Center
        - 4.2. Sensitive Compartmented Information Facility
        - 4.3. Digital Forensics Lab
        - 4.4. Datacenter
    - 5. Preparing for Physical Security Audits
- **Network Security**
    - 1. Network Security Assessments and Planning
    - 2. Network Security Architecture Challenges
    - 3. Network Security Design
    - 4. Network Standards, Protocols, and Controls
        - 4.1. Network Security Standards
        - 4.2. Protocols
- **Certified Chief**
    - 1. Network Security Controls
    - 2. Wireless (Wi-Fi) Security
        - 2.1. Wireless Risks
        - 2.2. Wireless Controls
    - 3. Voice over IP Security
- **Endpoint Protection**
    - 1. Endpoint Threats
    - 2. Endpoint Vulnerabilities
    - 3. End User Security Awareness

    - 4. Endpoint Device Hardening
    - 5. Endpoint Device Logging
    - 6. Mobile Device Security
        - 6.1. Mobile Device Risks
        - 6.2. Mobile Device Security Controls
    - 7. Internet of Things Security (IoT)
        - 7.1. Protecting IoT Devices
- **Application Security**
    - 1. Secure SDLC Model
    - 2. Separation of Development, Test, and Production Environments
    - 3. Application Security Testing Approaches
    - 4. DevSecOps
    - 5. Waterfall Methodology and Security
    - 6. Agile Methodology and Security
    - 7. Other Application Development Approaches
    - 8. Application Hardening
    - 9. Application Security Technologies
    - 10. Version Control and Patch Management
    - 11. Database Security
    - 12. Database Hardening
    - 13. Secure Coding Practices
- **Encryption Technologies**
    - 1. Encryption and Decryption
    - 2. Cryptosystems
        - 2.1. Blockchain
        - 2.2. Digital Signatures and Certificates
        - 2.3. PKI
        - 2.4. Key Management
    - 3. Hashing
    - 4. Encryption Algorithms
    - 5. Encryption Strategy Development
        - 5.1. Determining Critical Data Location and Type
        - 5.2. Deciding What to Encrypt
        - 5.3. Determining Encryption Requirements
        - 5.4. Selecting, Integrating, and Managing Encryption Technologies
- **Virtualization Security**
    - 1. Virtualization Overview
    - 2. Virtualization Risks
    - 3. Virtualization Security Concerns
    - 4. Virtualization Security Controls
    - 5. Virtualization Security Reference Model
- **Cloud Computing Security**
    - 1. Overview of Cloud Computing
    - 2. Security and Resiliency Cloud Services

    - 3. Cloud Security Concerns
    - 4. Cloud Security Controls
    - 5. Cloud Computing Protection Considerations
- **Transformative Technologies**
    - 1. Artificial Intelligence
    - 2. Augmented Reality
    - 3. Autonomous SOC
    - 4. Dynamic Deception
    - 5. Software-Defined Cybersecurity
- **Summary**

Domain 5: Strategic Planning, Finance, Procurement and Vendor Management

- **Strategic Planning**
    - 1. Understanding the Organization
        - 1.1. Understanding the Business Structure
        - 1.2. Determining and Aligning Business and Information Security Goals
        - 1.3. Identifying Key Sponsors, Stakeholders, and Influencers
        - 1.4. Understanding Organizational Financials
    - 2. Creating an Information Security Strategic Plan
        - 2.1. Strategic Planning Basics
        - 2.2. Alignment to Organizational Strategy and Goals
        - 2.3. Defining Tactical Short, Medium, and Long-Term Information Security Goals
        - 2.4. Information Security Strategy Communication
        - 2.5. Creating a Culture of Security
- **Designing, Developing, and Maintaining an Enterprise Information Security Program**
    - 1. Ensuring a Sound Program Foundation
    - 2. Architectural Views
    - 3. Creating Measurements and Metrics
    - 4. Balanced Scorecard
    - 5. Continuous Monitoring and Reporting Outcomes
    - 6. Continuous Improvement
    - 7. Information Technology Infrastructure Library (ITIL) Continual Service Improvement (CSI)
- **Understanding the Enterprise Architecture (EA)**
    - 1. EA Types
        - 1.1. The Zachman Framework
        - 1.2. The Open Group Architecture Framework (TOGAF)
        - 1.3. Sherwood Applied Business Security Architecture (SABSA)
        - 1.4. Federal Enterprise Architecture Framework (FEAF)
- **Finance**
    - 1. Understanding Security Program Funding
    - 2. Analyzing, Forecasting, and Developing a Security Budget
        - 2.1. Resource Requirements
        - 2.2. Define Financial Metrics
        - 2.3. Technology Refresh

        - 2.4. New Project Funding
        - 2.5. Contingency Funding
    - 3. Managing the information Security Budget
        - 3.1. Obtain Financial Resources
        - 3.2. Allocate Financial Resources
        - 3.3. Monitor and Oversight of Information Security Budget
        - 3.4. Report Metrics to Sponsors and Stakeholders
        - 3.5. Balancing the Information Security Budget
- **Procurement**
    - 1. Procurement Program Terms and Concepts
        - 1.1. Statement of Objectives (SOO)
        - 1.2. Statement of Work (SOW)
        - 1.3. Total Cost of Ownership (TCO)
        - 1.4. Request for Information (RFI)
        - 1.5. Request for Proposal (RFP)
        - 1.6. Master Service Agreement (MSA)
        - 1.7. Service Level Agreement (SLA)
        - 1.8. Terms and Conditions (T&C)
    - 2. Understanding the Organization’s Procurement Program
        - 2.1. Internal Policies, Processes, and Requirements
        - 2.2. External or Regulatory Requirements
        - 2.3. Local Versus Global Requirements
    - 3. Procurement Risk Management
        - 3.1. Standard Contract Language
- **Vendor Management**
    - 1. Understanding the Organization’s Acquisition Policies and Procedures
        - 1.1. Procurement Life cycle
    - 2. Applying Cost-Benefit Analysis (CBA) During the Procurement Process5
    - 3. Vendor Management Policies
    - 4. Contract Administration Policies
        - 4.1. Service and Contract Delivery Metrics
        - 4.2. Contract Delivery Reporting
        - 4.3. Change Requests
        - 4.4. Contract Renewal
        - 4.5. Contract Closure
    - 5. Delivery Assurance
        - 5.1. Validation of Meeting Contractual Requirements
        - 5.2. Formal Delivery Audits
        - 5.3. Periodic Random Delivery Audits
        - 5.4. Third-Party Attestation Services (TPRM)
- **Summary**