EC-Council Certified Chief Information Security Officer (CCISO) + Voucher d'examen

Durée: 5 Jours Réf de cours: CCISO Version: 4 Méthodes d'apprentissage: Intra-entreprise & sur-mesure

Résumé:

CCISO builds your skills to lead where cybersecurity meets business strategy.
EC-Council's CCISO Program has certified leading information security professionals around the world. A core group of high-level information security executives, the CCISO Advisory Board, contributed by forming the foundation of the program and outlining the content that would be 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 trainers. Each segment of the program was developed with the aspiring CISO in mind and looks to transfer the knowledge of seasoned professionals to the next generation in the areas that are most critical in the development and maintenance of a successful information security program.
The CCISO program ensures participants gain not only a deep understanding of cybersecurity but also the leadership, financial, and strategic planning skills necessary to succeed in an executive role. CCISO prepares leaders to integrate AI into cybersecurity risk management, compliance, forecasting, and governance with accountability and transparency. Earning the CCISO credential demonstrates that you are equipped to align security strategies, AI security strategies with business goals, effectively manage enterprise risks, and communicate with boards and executive leadership.
CCISO v4 equips you to:
- Align cybersecurity with business objectives
- Lead AI governance, compliance, and risk strategy
- Communicate effectively with boards and executives
- Manage enterprise-wide security programs and budgets
Earning CCISO v4 proves you are ready for **C-suite and board-facing security leadership**.
The CCISO program is a first-of- its-kind training and certification course that aims to produce cybersecurity executives of the highest caliber and ethics. The CCISO curriculum, developed by seasoned CISOs for current and aspiring CISOs, takes an executive management viewpoint that incorporates both information security management principles and general technical knowledge.
Updated 3/2026

Formation intra-entreprise

Cette formation est délivrable en session intra-entreprise, dans vos locaux ou dans les nôtres. Son contenu peut être adapté sur-mesure pour répondre aux besoins de vos collaborateurs. Contactez votre conseiller formation Global Knowledge ou adressez votre demande à info@globalknowledge.fr.

Public visé:

CCISO is designed for experienced Security Professionals ready to lead at the executive level. Bridge technical expertise with business strategy and AI governance.
- C-Suite & Executive
CISOs, CIOs, CTOs, CEOs, Chief AI Officers, and Chief Digital Officers
- VP & Director Level
VP of Information Security, Director of Security, Director of Cloud Security, Directory of GRC
- Security Management
Security Managers, Security Auditors, Head of Security Architecture, Security Engineers
- Governance & Advisory

Objectifs pédagogiques:

- After this course participants should be able to:
- Leverage AI for governance, compliance, and security monitoring.
- Build skills in AI-enabled risk management, auditing, and strategic planning.
- Help leaders develop AI security strategies aligned with global standards and frameworks.
- Ensure AI is integrated securely into enterprise operations while
- Lead AI adoption securely and responsibly.
- Address emerging regulatory requirements for AI usage across multiple jurisdictions.
- Equip CISOs to balance innovation and risk while guiding AI adoption within the enterprise.
- Prepare leaders to communicate AI risks effectively to boards and executives, strengthening organizational trust.

maintaining business continuity.

Pré-requis:

Professional experience is required for entry into this certification program. Candidates must meet experience requirements in order to take the certification examination:

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. Exam Eligibility Application [SK1] .

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 [SK1]

Test et certification

Certified Chief Information Security Officer (CCISO) certification is an executive focused program designed to develop and validate leaders responsible for defining, managing, and driving an organization's cybersecurity strategy.

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

Exam Code: 712-50

Contenu:

Domain 1: Governance; Risk Management; Security, Compliance, and Privacy; and Audit Management

- Fundamentals of Information Security Governance
- Risk Management Foundations
- Security Controls and Implementation
- CISO Role in the AI Era
- Leveraging AI for Governance and Compliance
- Establishing Cybersecurity Governance for AI
- Risk Management for AI
- Tools and Technologies for AI-Driven GRC
- Compliance and Regulatory Framework
- Security Frameworks, Standards, Laws, Acts and Directives
- Audit and Assessment
- Foundations of Leadership
- Personal Leadership Development
- Leading Teams and People
- Organizational Leadership
- Responsible and Ethical AI Leadership
- Cross-Functional AI Innovation Leadership
- Strategic AI Alignment and Innovation Management
- Introduction and Program Management Fundamentals
- Financial and Resource Management
- Program Architecture and Operations
- Stakeholder Management and Project Assessment
- Security Controls and Risk Management
- Cloud Security and Program Wrap-up
- Secure AI/ML System Architecture
- AI in Cybersecurity Operations
- Roadmap for CISOs to Implement AI in Security Programs
- Identity and Access Management (IAM) Fundamentals
- Physical Security and Business Continuity
- Network Security and Infrastructure
- Cloud and Endpoint Security
- Application Security and Development
- AI System Lifecycle Security
- Encryption and Incident Response
- AI- Driven Incident and Threat Response Strategies
- Introduction
- Key Challenges for CISOs
- Strategic Planning
- Understanding the Organization
- Information Security Strategic Planning ; Execution
- Enterprise Security Program Management
- Enterprise Architecture and Frameworks
- Finance ; Budgeting
- Procurement ; Vendor Management
- Delivery Assurance Framework

Domain 3: Information Security Controls, Security Program Management and Operations

- Fundamentals of Information Security Governance
- Risk Management Foundations
- Security Controls and Implementation
- CISO Role in the AI Era
- Leveraging AI for Governance and Compliance
- Establishing Cybersecurity Governance for AI
- Risk Management for AI
- Tools and Technologies for AI-Driven GRC
- Compliance and Regulatory Framework
- Security Frameworks, Standards, Laws, Acts and Directives
- Audit and Assessment
- Foundations of Leadership
- Personal Leadership Development
- Leading Teams and People
- Organizational Leadership
- Responsible and Ethical AI Leadership
- Cross-Functional AI Innovation Leadership
- Strategic AI Alignment and Innovation Management
- Introduction and Program Management Fundamentals
- Financial and Resource Management
- Program Architecture and Operations
- Stakeholder Management and Project Assessment
- Security Controls and Risk Management
- Cloud Security and Program Wrap-up
- Secure AI/ML System Architecture
- AI in Cybersecurity Operations
- Roadmap for CISOs to Implement AI in Security Programs
- Identity and Access Management (IAM) Fundamentals
- Physical Security and Business Continuity
- Network Security and Infrastructure
- Cloud and Endpoint Security
- Application Security and Development
- AI System Lifecycle Security
- Encryption and Incident Response
- AI- Driven Incident and Threat Response Strategies
- Introduction
- Key Challenges for CISOs
- Strategic Planning
- Understanding the Organization
- Information Security Strategic Planning ; Execution
- Enterprise Security Program Management

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

- Fundamentals of Information Security Governance
- Risk Management Foundations
- Security Controls and Implementation
- CISO Role in the AI Era
- Leveraging AI for Governance and Compliance
- Establishing Cybersecurity Governance for AI
- Risk Management for AI
- Tools and Technologies for AI-Driven GRC
- Compliance and Regulatory Framework
- Security Frameworks, Standards, Laws, Acts and Directives
- Audit and Assessment
- Foundations of Leadership
- Personal Leadership Development
- Leading Teams and People
- Organizational Leadership
- Responsible and Ethical AI Leadership
- Cross-Functional AI Innovation Leadership
- Strategic AI Alignment and Innovation Management
- Introduction and Program Management Fundamentals
- Financial and Resource Management
- Program Architecture and Operations
- Stakeholder Management and Project Assessment
- Security Controls and Risk Management
- Cloud Security and Program Wrap-up
- Secure AI/ML System Architecture
- AI in Cybersecurity Operations
- Roadmap for CISOs to Implement AI in Security Programs
- Identity and Access Management (IAM) Fundamentals
- Physical Security and Business Continuity
- Network Security and Infrastructure
- Cloud and Endpoint Security
- Application Security and Development
- AI System Lifecycle Security
- Encryption and Incident Response
- AI- Driven Incident and Threat Response Strategies
- Introduction
- Key Challenges for CISOs
- Strategic Planning
- Understanding the Organization
- Information Security Strategic Planning ; Execution
- Enterprise Security Program Management
- Enterprise Architecture and Frameworks
- Finance ; Budgeting
- Procurement ; Vendor Management
- Delivery Assurance Framework

Domain 2: Organizational Executive Leadership

- Fundamentals of Information Security Governance
- Risk Management Foundations
- Security Controls and Implementation
- CISO Role in the AI Era
- Leveraging AI for Governance and Compliance
- Establishing Cybersecurity Governance for AI
- Risk Management for AI
- Tools and Technologies for AI-Driven GRC
- Compliance and Regulatory Framework
- Security Frameworks, Standards, Laws, Acts and Directives
- Audit and Assessment
- Foundations of Leadership
- Personal Leadership Development
- Leading Teams and People
- Organizational Leadership
- Responsible and Ethical AI Leadership
- Cross-Functional AI Innovation Leadership
- Strategic AI Alignment and Innovation Management
- Introduction and Program Management Fundamentals
- Financial and Resource Management
- Program Architecture and Operations
- Stakeholder Management and Project Assessment
- Security Controls and Risk Management
- Cloud Security and Program Wrap-up
- Secure AI/ML System Architecture
- AI in Cybersecurity Operations
- Roadmap for CISOs to Implement AI in Security Programs
- Identity and Access Management (IAM) Fundamentals
- Physical Security and Business Continuity
- Network Security and Infrastructure
- Cloud and Endpoint Security
- Application Security and Development
- AI System Lifecycle Security
- Encryption and Incident Response
- AI- Driven Incident and Threat Response Strategies
- Introduction
- Key Challenges for CISOs
- Strategic Planning
- Understanding the Organization
- Information Security Strategic Planning ; Execution
- Enterprise Security Program Management
- Enterprise Architecture and Frameworks
- Finance ; Budgeting
- Procurement ; Vendor Management
- Delivery Assurance Framework

- Enterprise Architecture and Frameworks
- Finance ; Budgeting
- Procurement ; Vendor Management
- Delivery Assurance Framework

Domain 4: Information Security Core Competencies

- Fundamentals of Information Security Governance
- Risk Management Foundations
- Security Controls and Implementation
- CISO Role in the AI Era
- Leveraging AI for Governance and Compliance
- Establishing Cybersecurity Governance for AI
- Risk Management for AI
- Tools and Technologies for AI-Driven GRC
- Compliance and Regulatory Framework
- Security Frameworks, Standards, Laws, Acts and Directives
- Audit and Assessment
- Foundations of Leadership
- Personal Leadership Development
- Leading Teams and People
- Organizational Leadership
- Responsible and Ethical AI Leadership
- Cross-Functional AI Innovation Leadership
- Strategic AI Alignment and Innovation Management
- Introduction and Program Management Fundamentals
- Financial and Resource Management
- Program Architecture and Operations
- Stakeholder Management and Project Assessment
- Security Controls and Risk Management
- Cloud Security and Program Wrap-up
- Secure AI/ML System Architecture
- AI in Cybersecurity Operations
- Roadmap for CISOs to Implement AI in Security Programs
- Identity and Access Management (IAM) Fundamentals
- Physical Security and Business Continuity
- Network Security and Infrastructure
- Cloud and Endpoint Security
- Application Security and Development
- AI System Lifecycle Security
- Encryption and Incident Response
- AI- Driven Incident and Threat Response Strategies
- Introduction
- Key Challenges for CISOs
- Strategic Planning
- Understanding the Organization
- Information Security Strategic Planning ; Execution

- Enterprise Security Program Management
- Enterprise Architecture and Frameworks
- Finance ; Budgeting
- Procurement ; Vendor Management
- Delivery Assurance Framework

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement