EC-Council
Building A Culture Of Security

C|CISO

Certified Chief Information Security Officer

The Gold Standard in C-Suite Security Leadership

Now supercharged with *AI capabilities*

Certified

C|CISO

builds your skills to lead where cybersecurity meets business strategy.

Why Does the Industry Need *Certified* CISO (C|CISO)?

Why CISOs Need Business Education & Business Skills

Board communication gap

83%

of CISOs present to boards, but only 29% of boards have cyber expertise - forcing CISOs to translate technical risk into business terms

Business framing challenge

66%

of CISOs say senior leaders don't fully understand their role, and 58% struggle to translate technical issues into business language

Finance misalignment

Only

46%

of security leaders say finance is aligned with their priorities, highlighting the need for stronger business and financial fluency

Cybersecurity Leadership Has also Changed

AI-driven threats, global regulations, and board accountability have reshaped the CISO role.

90%

of organizations lack maturity against AI-driven attacks

63%

of breached organizations had no AI governance policy

Only

36%

of leaders believe current security can keep pace with AI threats

AI security is no longer a tooling problem - **it's a leadership problem.**

"While my 23 years of a dynamic career reflects rich experiences and a successful journey, I realized it [was] time to move one step further and stay in power with the latest requirements for leaders in information security.

The C|CISO was an ideal choice for me, as it provided the necessary knowledge [of] required information security management, executive leadership, and risk management strategies to protect an organization."

Deryck Rodrigues
Vice President - Group CIO Regulatory, Risk & Control, Deutsche Bank

What is C|CISO?

Certified Chief Information Security Officer (C|CISO) is executive-focused, designed specifically to train and certify leaders who are responsible for developing and leading an organization's cybersecurity strategy.

The C|CISO 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.

C|CISO prepares leaders to integrate AI into cybersecurity risk management, compliance, forecasting, and governance with accountability and transparency.

Earning the C|CISO 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.

C|CISO **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 C|CISO proves you are ready for **C-suite and board-facing security leadership.**

The C|CISO program is a first-of- its-kind training and certification course that aims to produce cybersecurity executives of the highest caliber and ethics. The C|CISO 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.

C|CISO Domains / Course *Modules*

Domain 1:	Governance; Risk Management; Security, Compliance, and Privacy; and Audit Management
Domain 2:	Organizational Executive Leadership
Domain 3:	Information Security Controls, Security Program Management & Operations
Domain 4:	Information Security Core Competencies
Domain 5:	Strategic Planning, Finance, Procurement and Vendor Management

What you will *Learn*

Key Skills You'll Gain

1. **Information Security Governance & Strategy**
   - Understand the fundamentals of information security governance and its alignment with business goals
   - Learn how to design and implement strategic security programs across enterprises
   - Build and manage an effective governance structure and hierarchy within security organizations
   - Gain expertise in building and managing enterprise-wide security programs and architectures
   - Prepare for modern cybersecurity leadership challenges by blending technical expertise, executive strategy, and AI-driven innovation

2. **Risk Management, Compliance & GRC**
   - Develop skills in risk management fundamentals, including quantitative and qualitative analysis
   - Gain expertise in threat, vulnerability, and risk assessment frameworks (ISO 27005, NIST, etc.)
   - Understand global compliance and regulatory requirements (GDPR, HIPAA, SOX, PCI DSS, DPDP Act, EU AI Act)
   - Gain exposure to security frameworks and standards (NIST CSF, ISO 27001, COBIT, MITRE ATT&CK, Zero Trust, etc.)
   - Learn how to establish and manage audit programs, leveraging GRC tools and AI-driven auditing

3. **AI, Automation & Emerging Technologies**
    - Learn the evolving role of the CISO in the AI era and how to leverage AI responsibly
    - Understand how to integrate AI into risk management, predictive modeling, and compliance monitoring
    - Learn how to embed fairness, accountability, and transparency in AI adoption
    - Apply AI-powered predictive budgeting and forecasting for cybersecurity programs
    - Learn how to apply AI and NLP tools for automated contract analysis and vendor scoring

4. **Leadership, Ethics & Executive Presence**
    - Master leadership principles, including executive presence, board communication, and stakeholder management
    - Develop emotional, social, and cultural intelligence for effective leadership in global enterprises
    - Learn how to lead inclusive, cross-functional, and virtual cybersecurity teams
    - Gain insights into succession planning, talent development, and mentoring practices for cybersecurity leaders
    - Understand ethical and responsible leadership, including AI ethics and governance board participation
    - Develop resilience and adaptability as a cybersecurity leader in uncertain environments

5. **Financial Management & Vendor Governance**
    - Learn budgeting, financial planning, and ROI assessment of cybersecurity investments
    - Understand CAPEX vs. OPEX strategies and apply cost-benefit analysis methods to security initiatives
    - Develop strong vendor management and procurement strategies, including SLA, MSA, and T&C design
    - Manage third-party risks, contract lifecycles, and SLA breach detection using AI-driven alerts

6. **Security Operations, SOC & Incident Management**
    - Gain knowledge of security program operations, monitoring frameworks, and performance measurement
    - Understand secure architecture for AI/ML pipelines, APIs, and SOC automation
    - Learn how to integrate AI into SIEM/SOAR and SOC operations for real-time incident response
    - Learn incident response, digital forensics, and AI-driven threat intelligence and forensic strategies

7. **Technical & Architecture Foundations**
    - Build expertise in network, endpoint, cloud, and application security core competencies
    - Implement Secure SDLC, DevSecOps, and application security testing (SAST, DAST, IAST)
    - Master enterprise architecture frameworks (TOGAF, Zachman, SABSA, FEAF) with AI-driven traceability

8. **Privacy, Awareness & Security Culture**
    - Gain knowledge of data privacy concepts, privacy impact assessments, and global data protection laws
    - Build effective crisis communication and security awareness strategies using AI-personalized campaigns
    - Learn how to build organizational security culture and influence behaviors effectively

What's *Unique* About C|CISO?

01 Executive-focused certification

designed exclusively for current and aspiring CISOs, emphasizing business strategy, governance, and enterprise risk over technical implementation

02 Built by practicing CISOs,

delivering real-world insights, boardroom perspectives, and leadership scenarios grounded in executive experience

03 Strong business and financial orientation,

covering budgeting, ROI, investment justification, and cost optimization to enable informed executive decision-making

04 Board and stakeholder communication mastery,

enabling leaders to translate cyber risk into business impact and influence senior leadership effectively

05 End-to-end cybersecurity leadership coverage,

spanning governance, risk, culture, crisis management, AI cybersecurity and long-term organizational resilience

06 Human-centric leadership development,

focusing on ethics, emotional intelligence, talent growth, and succession planning - areas rarely addressed in other certifications

07 Major latest enhancements:

- AI-driven cybersecurity leadership & strategy
- Dedicated executive leadership & board influence module
- Expanded privacy laws and global regulations
- AI risk management aligned with NIST AI RMF & EU AI Act

08

Workforce Framework Alignment:

- Mapped to DoD Cyber Workforce Framework (DCWF)
- Mapped to NICE Cybersecurity Workforce Framework

09

Learning Through War Games

CISOs have a challenging role; they need to adapt to ever-changing business needs, new regulations and compliance policies, emerging threats, and rapidly changing technologies within cybersecurity. War games are a valuable training tool for improving decision-making abilities and building experience with handling incidents. War gaming is a response development technique used in the military and adopted by many businesses today. EC-Council's C|CISO 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.

Topics Covered in the C|CISO *Program*

The five C|CISO domains bring together the components required for a C-level information security position. The C|CISO curriculum combines security risk management, controls, audit management, security program management and operations, governance, information security core concepts, strategic planning, finance, and vendor management–all of which are vital for leading a highly successful information security program.

The five C|CISO domains align with the NICE Workforce Framework for Cybersecurity, a national resource that categorizes and describes cybersecurity work and roles, including common job duties and skills needed to perform specific tasks. In addition to outlining 33 specialty areas and 52 work roles, the NICE Framework defines seven highly important cybersecurity functions

- Analyze
- Collect And Operate
- Investigate
- Operate And Maintain
- Oversee And Govern
- Protect And Defend
- Securely Provision

Become a Certified Chief Information Security Officer

Get Trained in The Gold Standard in C-Suite Security Leadership

Now Enhanced with AI Skills

ENQUIRE NOW

Why Is the C|CISO a First-of-Its-Kind *Certification?*

01 Includes All Competencies Required for C-Level Cybersecurity Positions

The C|CISO program imparts the skills necessary to lead a successful information security program, including audit management, information security controls, resource management, governance, strategic program development, and financial expertise.

02 Redefining Cybersecurity Leadership for the AI Era

This first-of-its-kind certification empowers cybersecurity leaders to responsibly integrate AI across governance, risk, compliance, financial planning, and vendor management elevating the CISO role from reactive defense to predictive, intelligence-driven executive leadership.

03 Abstraction of Technical Knowledge

The C|CISO course material includes a high-level view of technical topics. It includes basic technical information and teaches information security executives how to apply that technical knowledge in their day-to-day work.

04 Bridges the gap between technical management and executive leadership

Traditionally, leadership skills are acquired on the job, which can result in knowledge gaps as practitioners move from middle to senior management and executive roles. The C|CISO program provides the critical knowledge that lies between the executive management skills required of CISOs and the technical expertise many aspiring CISOs already possess. The C|CISO training paves the way for a successful transition to the top levels of information security management.

05

Recognizes the Importance of Real-World Experience

CISOs and other cybersecurity executives need deep experience in order to fulfill the expectations of the C-suite leadership role. The C|CISO program includes extensive real- world examples and input from current CISOs around the world. The program teaches students how to develop security portfolios for companies in various industries, create and use metrics to communicate risk to all levels within an organization, and align security services with business goals.

06

Designed by Industry Experts

The C|CISO Advisory Board is comprised of current CISOs who have designed the program based on their day-to-day experiences and technical and management knowledge. The Board includes security leaders from Fortune 500 companies, leading universities, and global consulting firms, all of whom have contributed their vast knowledge to address the need for leadership training in information security.

07

Recommendations and Accreditations

- **National Initiative for Cybersecurity Education (NICE)**

  The five C|CISO domains are mapped to the NICE Workforce Framework for Cybersecurity.

- **ANAB National Accreditation Board (ANSI)**

  The C|CISO is independently accredited and designed to meet the rigorous ANAB standards.

- **U.S. Department of Defense (DoD)**

  The C|CISO certification is an approved baseline certification under DoD Directive 8570/8140.

- **U.S. Armed Forces**

  The C|CISO certification provides an excellent opportunity for advancement in the U.S. military and is recognized by the U.S. Army, Navy, Air Force, and Marine Corps.

- **Government Communications Headquarters (GCHQ) Certified Training**

  The C|CISO course is designed to meet the standards of the United Kingdom's GCHQ.

Who Should *Enroll?*

- Aspiring CISOs and security leaders
- Security managers and architects
- GRC, risk, and compliance professionals
- CTOs and technical leaders moving into executive roles
- Consultants preparing for board or advisory positions

"Despite having 20 years of experience in information technology, including 8 years in information security and 15 years leading multidisciplinary teams in infrastructure and cybersecurity, I have gained a better understanding of the five critical domains explained in EC-Council's C|CISO body of knowledge and through real-life examples that the instructor presented during the C|CISO certification program."

Leandro Ribeiro

Leader of Cyber Defense, United Health Group, Brazil

C|CISO 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. They can take the exam without additional training if they have 5 years of experience in 5 of the C|CISO domains. If they have less than 5 years in 5 domains, but 5 or more years in 3 domains, they are required to take the training to qualify for the exam.

Experience waivers are available for some industry-accepted credentials and higher education within the field of information security. Waivers can be used for a maximum of 3 years of experience for each domain.

Candidates who do not meet 5 years of experience in 3 of the C|CISO domains, but have 2 or more years of experience in at least 1 domain (or currently hold any one of the CISSP, CISM, CISA certifications) can participate in the Associate C|CISO program.

Candidates participating in the Associate C|CISO will have the opportunity to attend the same training as our C|CISO candidates, and learn the job requirements of a security executive so they can plan their careers to meet their career goals of security industry leadership.

C|CISO training is mandatory for all Associate C|CISO candidates prior to taking the Associate C|CISO examination.

C|CISO *Exam Details*

Exam Title	EC-Council Certified Chief Information Security Officer (C|CISO)
Exam Code	712-50
Test Format	Scenario-based multiple-choice questions
Number of Questions	150
Duration	2.5 hours
Availability	EC-Council Exam Portal
Passing Score	60–85%, depending on exam form

Associate C|CISO
Exam Details

Exam Title	EC-Council Associate C|CISO Certification
Number of Questions	150 multiple-choice questions
Duration	2 hours
Passing Score	70%

What are Certified CISOs Around the World Saying about the *Certification?*

Beatriz Silveira
Head of Tech Risk and Control

"Successfully developing a threat resilience is the most impactful achievement since earning the C|CISO certification."

Jason Wright
Chief Information Officer

"Achieving DoD Impact Level 4 operations for the organization's cloud environment and migrated assets, resources, and data to the IL4 cloud infrastructure would be the most impactful achievement post earning the C|CISO."

Joseph Stenaka
Chief Information Security Officer

"Being selected as the CISO for the Social Security Administration, one of the best cybersecurity jobs within the US government would be the most impactful achievement post earning the C|CISO."

Salvador Chio Guarino Jr.
Chief Information Security Officer

"The most impactful achievement I made when I received my C|CISO certification was to build and maintain the customer's trust in our information security program."

Jitendra Tripathi
Head Cyber Security Operations

"Post earning the C|CISO, I was able to improve the efficiency of the SOC, and aligned Security Operations with business goals."

Justen Dyche
Head of Information Security, BBC

"The most impactful achievement post earning the C|CISO was completing a transformative program fundamentally redesigning the approach to Cyber Security at the BBC."

Andrew Green
Chief Information Security Officer

"Winning the Cloud Security Influencer of the Year at the Cyber Security Awards is the most impactful achievement post earning the C|CISO."

Department for Business, Energy & Industrial Strategy

Why Students *Choose* C|CISO?

Designed for **leadership**, not just technical skills

Focus on **AI, governance, and executive decision-making**

Globally recognized and aligned to modern regulations

Builds credibility for **C-suite and board-level roles**

Why C|CISO Is the Gold Standard in C-Suite *Leadership Training*.

Certified CISOs Response About Leadership, Growth, and Influence

99% reported that the Certified CISO training program vastly improved their cybersecurity leadership skills.

99% reported that Certified CISO curricula aligns to the responsibilities of C-level cybersecurity positions.

99% would recommend Certified CISO to colleagues and peers.

90% gained confidence in their ability to align security strategies with organizational goals.

98% affirm that the Certified CISO program empowered them to improve their organization's cybersecurity stance.

76% experienced increase in compensation after obtaining Certified CISO.

100% contributed to the cybersecurity community in a meaningful way after becoming a Certified CISO

About EC-Council

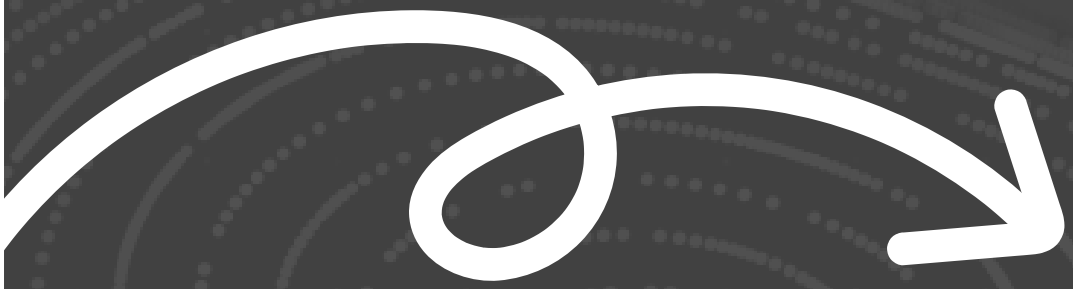
EC-Council's sole purpose is to build and redefine the cybersecurity profession globally.

We help individuals, organizations, educators, and governments address global workforce problems by developing and curating world-class cybersecurity education programs and their corresponding certifications. We also provide cybersecurity services to some of the largest businesses globally. Trusted by 7 of the Fortune 10, 47 of the Fortune 100, the Department of Defense, the intelligence community, NATO, and over 2,000 of the best universities, colleges, and training companies, our programs have certified people in over 140 countries, and set the bar in the field of cybersecurity education.

Best known for the Certified Ethical Hacker (C|EH^{AI}) program, we are dedicated to equipping over 380,000 information-age soldiers with the knowledge, skills, and abilities required to fight and win against cyber adversaries. EC-Council builds individual- and organization-wide cyber capabilities through our other programs as well, including Certified Secure Computer User (C|SCU), Computer Hacking Forensic Investigator (C|HFI), Certified Security Analyst, Certified Network Defender (C|ND), Certified SOC Analyst (C|SA), Certified Threat Intelligence Analyst (C|TIA), Certified Incident Handler (E|CIH), and the Certified Chief Information Security Officer (C|CISO). We are an ANAB ISO/IEC 17024 accredited organization and have earned recognition by the DoD under Directive 8140/8570 in the UK by the GCHQ, CREST, and various other authoritative bodies.

Founded in 2001, EC-Council employs over 400 individuals worldwide, with ten global offices in the U.S., UK, Malaysia, Singapore, India, and Indonesia. Our U.S. offices are in Albuquerque, NM, and Tampa, FL.

Learn more at **eccouncil.org.**



EC-Council

Building A Culture Of Security

CERTIFIED CHIEF INFORMATION SECURITY OFFICER

C|CISO

Certified | Chief Information Security Officer