EC-Council

Building A Culture Of Security

C|CISO

Certified | Chief Information Security Officer

Train for the **C-Suite**

Certified Chief Information Security Officer

www.ciso.eccouncil.org

ABOUT THE PROGRAM

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.

Members of the Board contributed as authors, exam writers, and instructors. They also provided continuous quality assurance through periodic materials reviews. Each segment of the C|CISO Program was developed in order to move a security professional's career into the realm of executive leadership.

Through the C|CISO program, EC-Council will transfer the knowledge of seasoned professionals to you, the next generation of leadership, by focusing on the most critical competencies required to develop and maintain a successful information security portfolio. 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.

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

"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*

The Five C|CISO Domains

C|CISOs exhibit their knowledge and experience within five core domains:

1. Governance and risk management (policy, legal, and compliance)
2. Information security controls, compliance, and audit management
3. Security program management and operations
4. Information security core competencies
5. Strategic planning, finance, procurement, and vendor management

Who Needs the C|CISO Program?

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. In the C|CISO program, cybersecurity leaders hone their knowledge and learn how to integrate information security initiatives with needs of the business, aligning to the critical goals and objectives of an organization. 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.

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. Please see the chart (below) for additional information.

DOMAIN	EXPERIENCE WAIVERS
Governance and risk management	PhD in information security (3 years)
	Master of Science in information security management or information security engineering (2 years)
	Bachelor of Science in information security (2 years)
Information security controls, compliance, and audit management	PhD in information security (3 years)
	Master of Science in information security management or information security engineering (2 years)
	Bachelor of Science in information security (2 years)
Security program management and operations	PhD in information security (3 years)
	Master of Science in information security or project management (2 years)
	Bachelor of Science in information security (2 years)
Information security core competencies	PhD in information security (3 years)
	Master of Science in information security (2 years)
	Bachelor of Science in information security (2 years)
Strategic planning, finance, procurement, and vendor management	Certified Public Accountant (CPA) license, Master of Business Administration, or Master of Science in finance (3 years)

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

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

(for details, please refer to https://cert.eccouncil.org/certified-chief-information-security-officer.html)

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%

"If you want to be the best, I strongly believe the C|CISO credential should be one of the first things you add to your professional profile."

*— **Rodney Gullatte, Jr.***
CEO, Firma IT Solutions and Services

What's New in the C|CISO Certification Program

- Updated information on the latest security industry trends, leadership methodology, and security technologies
- Increased focus on risk management frameworks, including the NIST RMF (SP 800-30/39/53), ISO 27005 and 31000, OCTAVE Allegro/Forte, COSO ERM, FAIR RM, COBIT ERM, and others.
- More robust contract management
- Heavier emphasis on vendor management
- Step-by-step advisement on how to build and mature a security program
- A CISO-level view of transformative technologies, including artificial intelligence, augmented reality, autonomous security operations centers, dynamic deception, and more
- In-depth coverage of strategic planning

Learning Through War Games

CISOs clearly 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. Wargaming 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.

Recommendations and Accreditations

- *National Initiative for Cybersecurity Education (NICE)*
  The five C|CISO domains are mapped to the NICE Workforce Framework for Cybersecurity.

- *American National Standards Institute (ANSI)*
  The C|CISO is independently accredited and designed to meet the rigorous ANSI standards.

- *U.S. Department of Defense (DoD)*
  The CCISO certification is an approved baseline certification under DoD Directive 8570/8140.

- *U.S. Armed Forces*
  The CCISO 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 CCISO course is designed to meet the standards of the United Kingdom's GCHQ.

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

100% mapping to NICE Workforce Framework for Cybersecurity

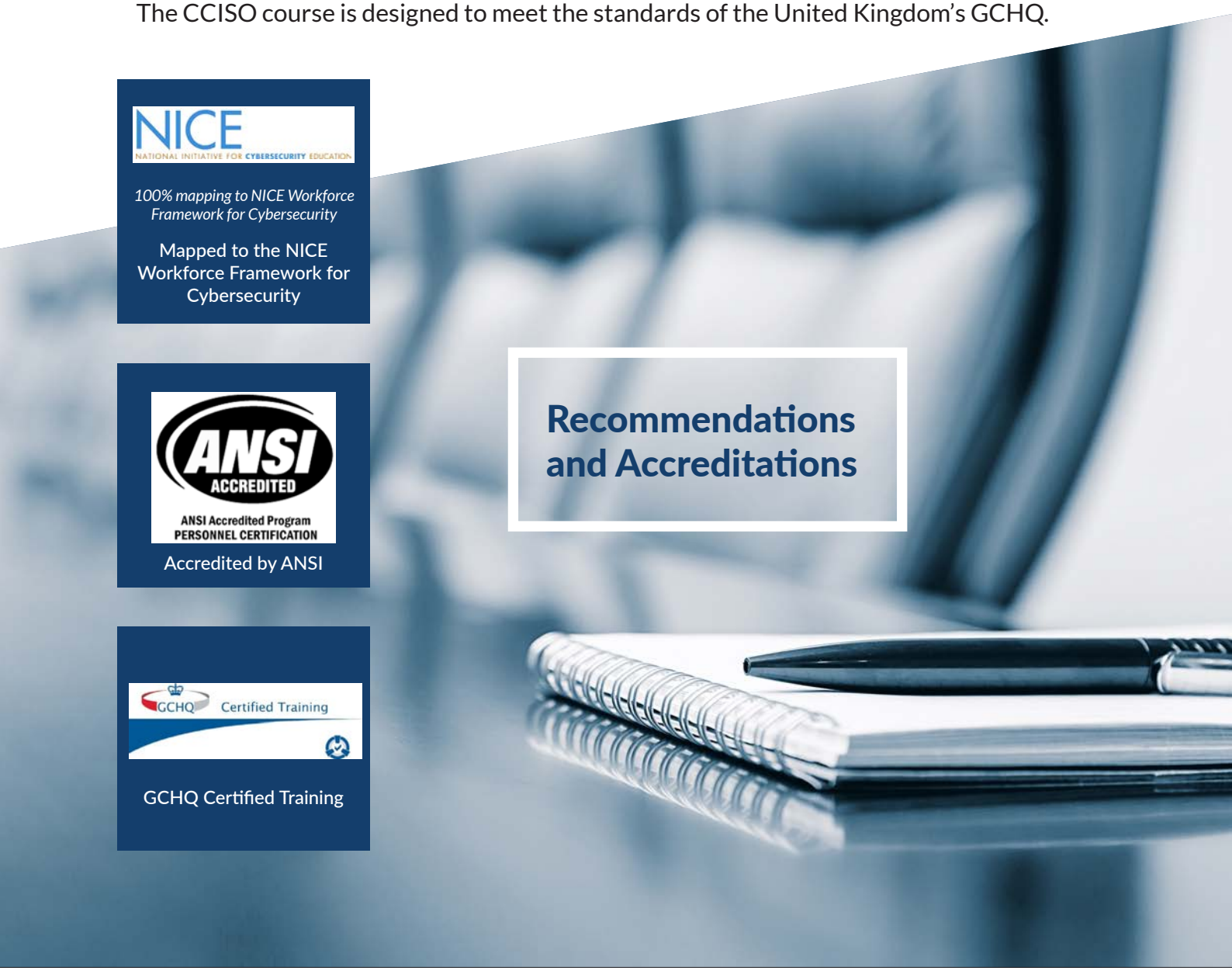
Mapped to the NICE Workforce Framework for Cybersecurity

ANSI ACCREDITED
ANSI Accredited Program
PERSONNEL CERTIFICATION

Accredited by ANSI

GCHQ Certified Training

GCHQ Certified Training



Recommendations and Accreditations

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		

The C|CISO program includes skill development courses in legal advice and advocacy, strategic planning and policy creation, information systems security operations, and security program leadership.

C|CISO Body of Knowledge

EC-Council's C|CISO body of knowledge provides in-depth coverage of all five C|CISO information security management domains. The C|CISO body of knowledge was created by knowledgeable and current CISOs for aspiring security executives.

"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 CCISO certification program."

— ***Leandro Ribeiro*** *Leader of Cyber Defense, United Health Group, Brazil*

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

Accredited by ANSI

EC-Council's C|CISO certification program is accredited by ANSI. EC-Council is one of the ew certification bodies with a primary specialization in information security to meet the ANSI/ ISO/IEC 17024 personnel certification accreditation standard.

Compliant with the NICE Framework

The five domains of the C|CISO program are mapped to the NICE Framework, a national resource that describes and categorizes key cybersecurity functions, common sets of responsibilities, and skills needed to perform specific tasks.

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.

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.

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 cprovides 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.

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.

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.

Join the Elite
Become a Member of the C|CISO Community

Members of the C|CISO community receive the following benefits:

- Complimentary access to one EC-Council CISO event per year (limited free passes available on a first-come, first-served basis), plus discounts for additional events
- First notice for speaking opportunities at conferences
- Opportunity to contribute articles to EC-Council's CISO resources page
- Assistance in marketing and publishing white papers
- Opportunity to deliver webinars to large audiences via EC-Council's security channel

EC-Council

Building A Culture Of Security

CERTIFIED CHIEF INFORMATION SECURITY OFFICER (C|CISO)

www.ciso.eccouncil.org