EC-Council

C|CISO

Certified Chief Information Security Officer

Train for the **C-Suite**

Certified Chief Information Security Officer

www.ciso.eccouncil.org

ABOUT THE PROGRAM

EC-Council's Chief Certified Information Security Officer (CCISO) program has empowered information security professionals across the globe. EC-Council developed the CCISO certification by leveraging the knowledge of a core group of deeply experienced information security executives within our CCISO Advisory Board. These seasoned professionals built the program's foundation and outlined the content covered in the CCISO exam, body of knowledge, and training program.

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 CCISO Program was developed in order to move a security professional's career into the realm of executive leadership.

Through the CCISO program, EC-Council will transfer the knowledge of experienced 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 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 security executives for current and aspiring executives—provides an upper management viewpoint that incorporates information security management principles, business acumen, and general technical knowledge.

Professional experience is required for entry into this certification program. Candidates must meet the basic CCISO 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 CCISO 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 CCISO Domains

CCISOs exhibit their knowledge and experience in the following 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 CCISO Program?

The CCISO 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 CCISO program, cybersecurity leaders hone their knowledge and learn how to integrate information security initiatives with needs of the business by 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 insight.

CCISO Certification Exam Eligibility

To take the CCISO examination, candidates must provide proof that they have 5 years of experience in at least 3 of the 5 domains. A training course is required if a candidate has 5 years of experience in 3 or 4 of the CCISO domains. If the candidate has 5 years of experience in all 5 domains the training course is not required.

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)

Upon passing the CCISO exam, candidates will receive their CCISO certificate and associated community privileges. The CCISO 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.

CCISO Certification Renewal

To maintain your CCISO credential after the initial 3-year period, you must earn 120 credits within 3 years and maintain annual dues. To submit credits, you simply update your ECE credit account in the EC-Council Aspen portal with details and verification of your earned credits. Please note that if you hold multiple EC-Council certifications, all credits you earn will be applied to all certifications.

If you do not renew your CCISO certification within 3 years, EC-Council will suspend your certification for 1 year. Your certification will be inactive until you earn 120 ECE credits. If you fail to meet these certification maintenance requirements during the suspension period, EC-Council will revoke your CCISO certification. If this occurs, you will be required to retake the CCISO certification exam to reinstate the CCISO credential.

Tips for Earning Credits

CCISOs can earn credits in a variety of ways, including attending conferences and webinars, writing research papers, presenting at conferences, reading materials on a related subject, and many others. We provide flexible options for making sure your professional efforts and participation count toward maintaining your certification.

CCISO Exam Details

Exam Title	EC-Council Certified Chief Information Security Officer (CCISO)
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)

"If you want to be the best, I strongly believe the CCISO 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 CCISO Certification Program

- New sections covering the General Data Protection Regulation (GDPR)
- Increased focus on risk management frameworks, including the NIST Risk Management Framework, COBIT, TARA, OCTAVE, FAIR, and ITIL
- 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 CCISO training provides wargaming sessions in all live classes, providing interactive and engaging incident modeling. In the CCISO 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 CCISO course are incorporated into the exercise, reinforcing their knowledge and skills.

Recommendations and Accreditations

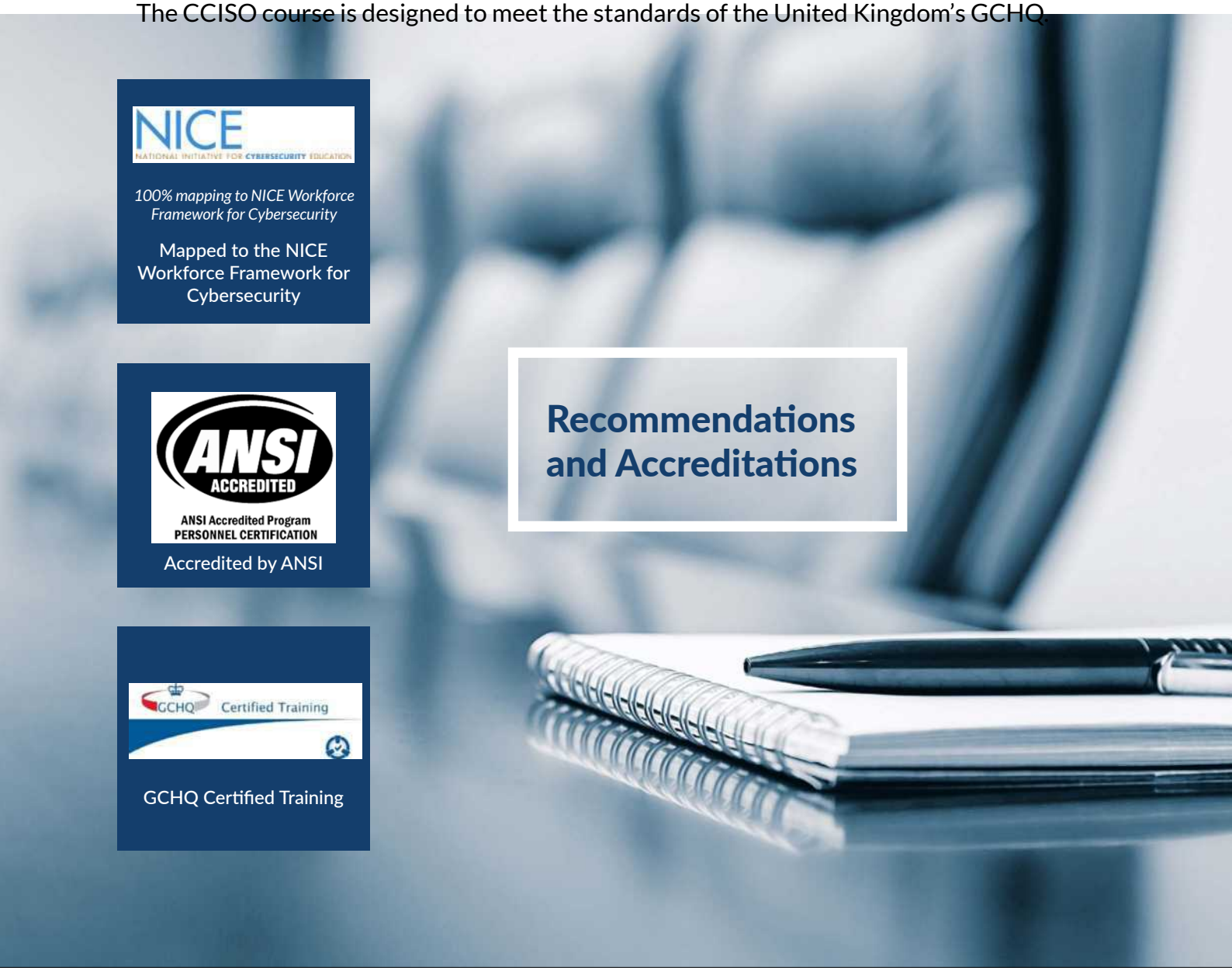
- *National Initiative for Cybersecurity Education (NICE)*
  The five CCISO domains are mapped to the NICE Workforce Framework for Cybersecurity.

- *American National Standards Institute (ANSI)*
  The CCISO 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.



Topics Covered in the CCISO Program

The five CCISO domains bring together all the components required for a C-level information security position. The CCISO 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 CCISO 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 CCISO program was established to align with the NICE Framework and includes skill development courses in legal advice and advocacy, strategic planning and policy creation, information systems security operations, and security program management.

CCISO Body of Knowledge

EC-Council's CCISO body of knowledge provides in-depth coverage of all five CCISO information security management domains. The CCISO 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 CCISO 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 CCISO a First-of-Its-Kind Certification?

Accredited by ANSI

EC-Council's CCISO certification program is accredited by ANSI. EC-Council is one of the few 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 CCISO 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 CCISO program imparts the skills necessary to lead a successful information security program including audit management, information security controls, human capital management, governance, strategic program development, and financial expertise.

Abstraction of Technical Knowledge

The CCISO course material includes a high-level understanding of technical topics, enabling executives to be familiar with technology principles and concepts. This empowers informed decisions and conceptual discussions.

Bridges Gaps Between Technical, Executive Management, and Financial Functions

Traditionally, leadership skills have been learned on the job, creating knowledge gaps as practitioners move from middle to senior management and executive roles. The CCISO program creates a bridge between the technical expertise many aspiring CISOs already possess and critical executive management skills. The CCISO training enables successful transition to the top levels of information security management.

Recognizes the Importance of Real-World Experience

Cybersecurity executives need deep experience in order create, lead, and enable security professionals. The CCISO program incorporates extensive real-world experience and input from current CISOs around the world. The CCISO Program transfers the knowledge, allowing our students to develop security portfolios that enable organizations to pursue their plans in the safest, most secure manner possible.

Designed by Industry Experts

The CCISO Advisory Board is comprised of practicing CISOs who have designed the program based on their operational experiences, technical knowledge, and management expertise. The Board includes security leaders from a wide range of industries and verticals, to include Amtrak, HP, the City of San Francisco, Lennar, the Centers for Disease Control, leading universities, and international consulting firms. They have contributed their vast knowledge to address the need for effective, efficient security leadership training.

Join the Elite
Become a Member of the CCISO Community

Members of the CCISO 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

CERTIFIED CHIEF INFORMATION SECURITY OFFICER (CCISO)

www.ciso.eccouncil.org

Behaviour Group

Behaviour Group Training Advisory Best Practices
ISO Standards, BCS, ISACA, APMG, AXELOS, PeopleCert, EC-Council

www.behaviour-group.com
training@behaviour-group.com