



GLACIER CYBER ALLIANCE

EC-Council

C | CISO

Certified Chief Information Security Officer



ciso.eccouncil.org

JOIN THE ELITE

**CERTIFIED CHIEF INFORMATION
SECURITY OFFICER V3**

Elements that make CCISO one of a kind

Accredited by ANSI

EC-Council has been accredited by the American National Standards Institute (ANSI) for its CCISO certification program. It is one of the few certification bodies whose primary specialization is information security in order to meet the ANSI/ISO/IEC 17024 Personnel Certification Accreditation standard.

Compliant to the NICE Framework

The five domains of the CCISO program are mapped to the NICE Cybersecurity Workforce Framework (NCWF), a national resource that categorizes and describes cybersecurity work, listing common sets of duties and skills needed to perform specific tasks.

It brings together all the components required for a C-Level position:

The CCISO program combines audit management, governance, IS controls, human capital management, strategic program development, and the financial expertise vital to leading a highly successful IS program.

Focuses on the application of technical knowledge:

Material in the CCISO Program assumes a high-level understanding of technical topics and doesn't spend much time on strictly technical information, but rather on the application of technical knowledge to an information security executive's day-to-day work.

Bridges the Gap between Technical Knowledge, Executive Management, and Financial Management

The CCISO aims to bridge the gap between the executive management knowledge that CISOs need and the technical knowledge that many aspiring CISOs have. This can be a crucial gap as a practitioner endeavors to move from mid-management to upper, executive management roles. Much of this is traditionally learned as on the job training, but the CCISO Training Program can be the key to a successful transition to the highest ranks of information security management.

Recognizes the Importance of Real-World Experience

To reach a C-Level position, an information security officer must have prior experience to gain a holistic idea of what to expect while in the field. With this in mind, the CCISO program consists of many real-world experiences faced by current CISOs around the world.

The CCISO exam also challenges students to develop a business continuity plan for a company in a given industry and situation, use metrics to communicate risk for different audiences, and describes how to align security programs with the goals of the business—among many other exercises.

Designed by the Experts

The CCISO Advisory board is comprised of practicing CISOs who designed the program based on their day-to-day experiences - based on both technical and management concerns. The board is made up of security leaders from Amtrak, HP, the City of San Francisco, Lennar, the Center for Disease Control, universities, and consulting firms who have contributed their vast knowledge to create this program to address the lack of leadership training in information security.

Are you ready to be a CISO?

- ✓ Do you feel comfortable defending your security risk analysis methodology to your board?
- ✓ What's your long-term security strategy?
- ✓ How mature is your security program?
- ✓ Are you compliant yet still at risk for a major, brand-damaging breach?

C|CISO™

**CERTIFIED CHIEF
INFORMATION
SECURITY OFFICER**

The Top 3 reasons you should consider attaining the Certified CISO (CCISO) Certification:

1

CCISO WAS DESIGNED BY CISOs

For CISOs and aspiring CISOs to create true leaders. The CCISO Advisory Board is made up of CISOs from government and private sectors spanning industries and areas of expertise. Security leaders from Amtrak, HP, the City of San Francisco, Lennar, the Center for Disease Control, universities, and consulting firms all contributed their vast knowledge to creating this program to address the lack of leadership training in information security.

2

CCISO IS NOT FOCUSED ON THE TECHNICAL ASPECTS OF THE CISO JOB ROLE

That material is covered by many other certifications on the market. The content of the CCISO Program is from the perspective of executive management. The training program is built around responding to scenarios written by our contributing CISOs drawing on their experiences leading some of the world's top organizations' security programs. During the CCISO workshop, students will be challenged to develop a business continuity plan for a company in a given industry and situation, use metrics to communicate risk for different audiences, and describe how to align a given security program with the goals of the business in which it resides, among many other exercises.

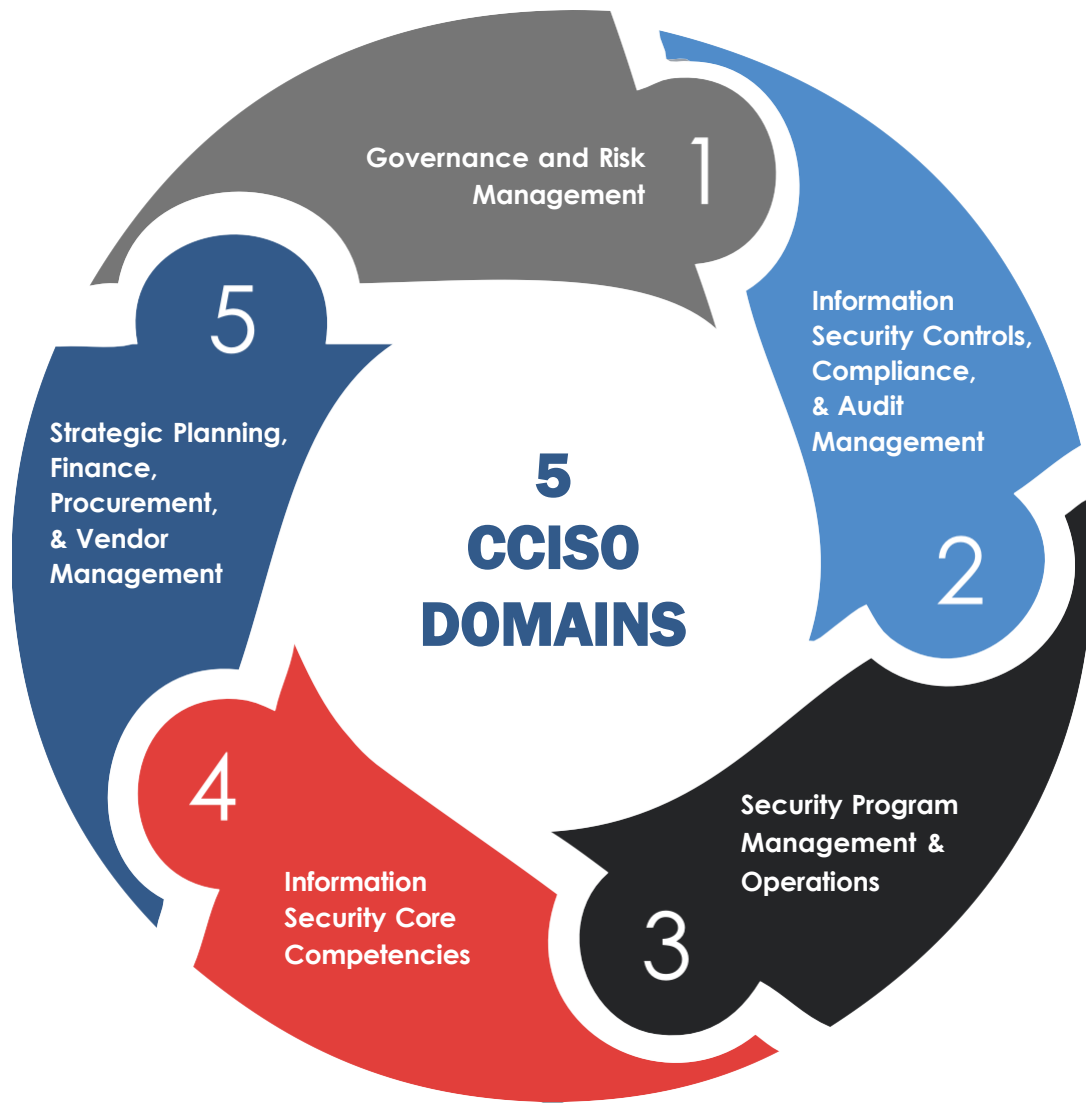
3

CCISO COVERS STRATEGIC AND FINANCIAL MANAGEMENT

Like no other program on the market. Recent surveys suggest that other C-Level executives do not view the CISO as a true peer. In order to become true leaders in their organizations, IS professionals are required to have a higher business acumen than has ever been required previously. The CCISO program dives deep into how security should be injected into the procurement process and how a CISO should manage budgets and assets – vital skills and knowledge that many in the profession lack.

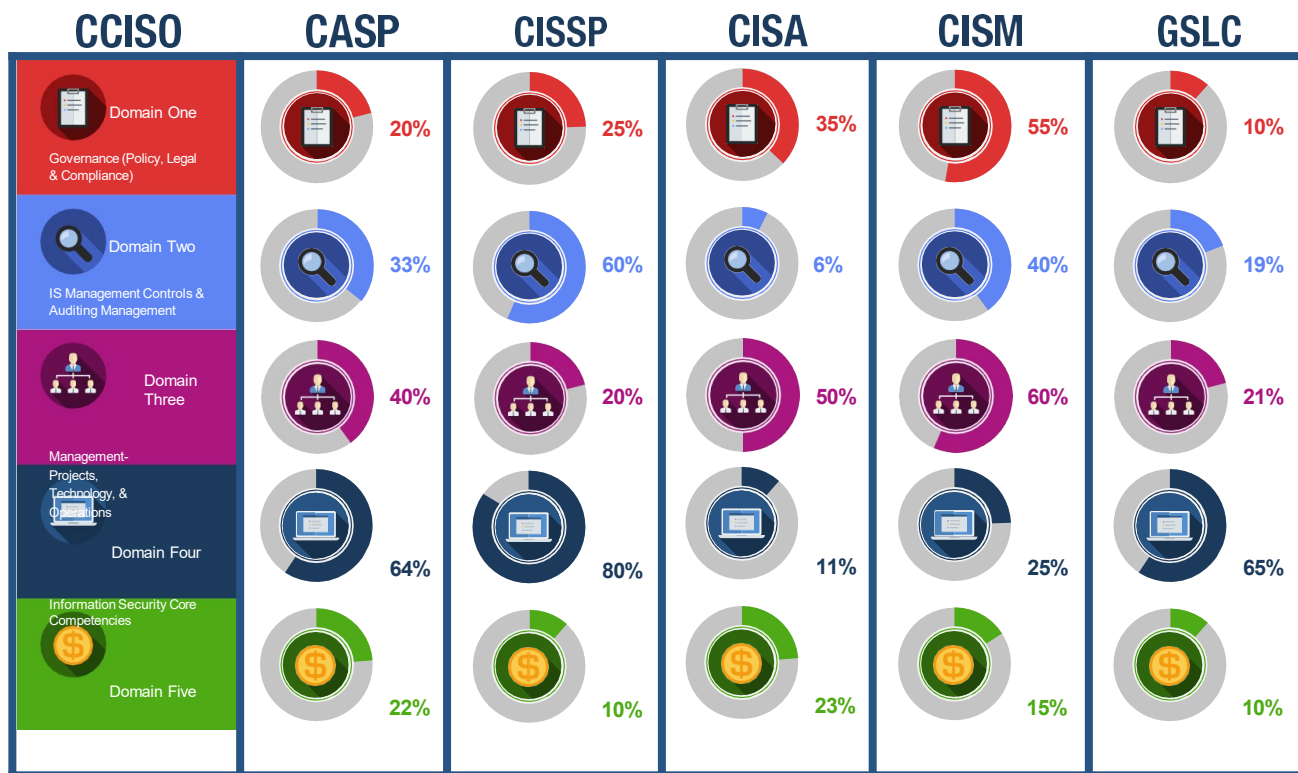
The Five CCISO Domains

CCISOs are certified in the knowledge of and experience in the following CCISO Domains:



There is a common misperception that CCISO is a competitor to CISSP —

This is simply not the case. CCISO is the step anyone interested in an executive career in information security should take after completing courses like CISSP, CISA, CISM, etc. The chart below describes how the content in each of these programs compares to CCISO.



The following is a summary of the learning objectives for each Domain:

Domain 1

Domain 1 covers Policy, Legal, and Compliance issues involved in the executive management of an Information Security Program.

Domain 2

Domain 2 is concerned with Audit and Risk Management, including understanding your organization's risk tolerance and managing accordingly.

Domain 3

Domain 3 covers many of the day-to-day aspects of the CISO job including project, technology, and operations management.

Domain 4

Domain 4 delves into the technology of the CISO's role but from an executive perspective.

Domain 5

Domain 5 covers Finance and Strategic management, some of the key skills that help CISOs rise to the level of their peer C-Level executives.

CCISO WAR GAMES



CCISO is now an interactive class



All instructors lead War Games, which mimic what happens during a breach



All aspects of what the student has learned are incorporated into the exercise, reinforcing the content

CCISO Recognition/ Endorsement/ Mapping



The National Initiative for Cybersecurity Education (NICE)



American National Standards Institute (ANSI)



GCHQ Certified Training (GCT)



United States Department of Defense (DoD)



United States Navy



United States Army



United States Marine Corps



United States Air Force

“ The program trained me to look at every security incident from a different perspective – not as a technical professional but someone who belongs to the managerial level.

*- Joshua William K.,
Head, IT Governance and Compliance at GCB Bank Limited.*

Certification:

To be approved to take the CCISO exam without first taking certified training, you will need to show evidence and present verifiers to show that you have 5 years of experience in each of the five CCISO domains. Experience waivers are available for some industry-accepted certifications and CCISO Exam Eligibility Application Form higher education. Between certification and training waivers, applicants can only waive 3 years of experience for each domain. If you have taken training, you must show 5 years of experience in 3 of the 5 domains in order to take the CCISO exam.

Applicants found not qualified for the CCISO Exam may choose to take the EC-Council Information Security Manager (EISM) exam instead. The EISM exam is less challenging than the CCISO exam and leads to the EISM certification, which has no experience requirements, but does require that you take CCISO training.

Candidates that successfully pass the exam will receive their C|CISO certificate and community privileges. Members are expected to adhere to recertification requirements through EC-Council's Continuing Education Requirements.

Target Audience:

The CCISO is for information security executives aspiring to be CISOs through refining their skills and learning to align information security programs with business goals and objectives. This program also encourages existing CISOs to improve their technical and management skills, as well as business procedures.

ATTAINING THE CCISO CREDENTIAL

- ◆ **Exam Title:** EC-Council Certified CISO
- ◆ **Exam Code:** 712-50
- ◆ **Number of Questions:** 150
- ◆ **Duration:** 2.5 Hours
- ◆ **Availability:** ECC Exam Portal
- ◆ **Test Format:** Scenario-based Multiple Choice
- ◆ **Passing Score:** Please refer to <https://cert.eccouncil.org/faq.html>

Information systems

Network


Protection





Hack


Join the Elite – Become a Member of the CCISO Community


As a member of the CCISO Community, you can gain access to:


- 

Free attendance at one EC-Council CISO Event per year (limited free passes available - first come, first served) and deep discounts if you would like to attend more than one event.
- 

First notice for speaking opportunities at conferences.
- 

Whitepaper assistance, marketing, and publishing.
- 

The opportunity to post articles to the CISO Resources Page.
- 

The opportunity to give webinars to large EC-Council audiences via our Security Channel.
- 

Free subscription to CISO Mag – EC-Council's online magazine for information security leaders! Normally \$79 per year.

How to Get Certified?

To get certified, you need to complete the following steps:

STEP ONE Have at least 2 years of experience in any one of the C|CISO domains or be currently certified in one of the following: CISA, CISM, or CISSP.

STEP TWO Candidates must complete their Associate C|CISO application and meet the minimum verified by EC Council, to take the exam as described in the Associate C|CISO Pre-Requisites section. The candidate then submits the application.

STEP THREE Complete the C|CISO training program that includes all 5 of the C|CISO Domains.

STEP FOUR Prepare for the Associate C|CISO exam. The exam is designed to test the applicant's basic security program knowledge and the ability to think critically.

This exam assesses candidates across two cognitive levels:

LEVEL ONE

Knowledge-based questions, which assess the applicant's ability to recall memorized facts. These questions are straightforward and often ask for basic definitions or standards.

LEVEL TWO

Application-based questions, which assess the applicant's ability to understand and apply a given concept. These questions require the applicant to demonstrate their understanding of a concept and how it can be applied in different scenarios.

STEP FIVE Pass the Associate C|CISO exam, which tests your knowledge & skills and is subject to the following conditions:

- 150 multiple-choice questions.
- 2-hour time limit.
- A minimum passing score of 70%.

Associate C|CISO Pre-requisites

To qualify for the Associate C|CISO Program, applicants must have at least 2 years of technical or management experience in any 1 of the 5 C|CISO domains.

OR

Currently hold the CISSP, CISM, or CISA certifications (any 1 of them).

Transition from Associate C|CISO to C|CISO

Below are the steps for becoming a C|CISO after achieving the Associate C|CISO certification

- To obtain full C|CISO status, candidates must meet the experience requirements by having a minimum of 5 years of experience in at least 3 of the 5 domains.
 - The required experience must be earned while the candidate remains current with the Associate C|CISO credential (annual fees and professional education credits).
 - After gaining the required experience, Associate C|CISO certification holders will have their experience verified by EC-Council before being approved to take the C|CISO exam.
 - Training prior to taking the C|CISO exam is optional, as the Associate C|CISO already completed the training earlier. If a long period of time has elapsed taking the training, we advise candidates to retake the C|CISO training due to potential changes in the security industry and C|CISO training materials.
 - If the candidate's Associate C|CISO certification has lapsed, they must reapply for the C|CISO program and follow the standard C|CISO application process from the beginning.
-

June 3rd Class Registration Open

- Class will be held both virtually and in Whitefish Montana
- Class Schedule
 - Monday – Thursday 8am to 4pm Mountain Time
 - Friday morning review with opportunity to test in the afternoon for those in person.

For more information, please reach out to Glacier Cyber Alliance at info@glaciercyberalliance.com