C|CISO Exam Eligibility Application Form

C|CISO is the first of its kind certification that recognizes an individual's accumulated skills in developing and executing an information security management strategy in alignment with organizational goals.

C|CISO equips information security leaders with the most effective toolset to defend organizations from cyber-attacks.

To rise to the role of the CISO, strong technical knowledge, and experience is more imperative now than ever before but it must be accompanied by the ability to communicate in business value. C|CISOs understand that their information security decisions often have a direct impact on their organization's operational cost, efficiency, and agility. As organizations introduce new technologies, C|CISOs will develop and communicate a strategy to avoid the potential risks stemming from their implementation to the organization's operations.

C|CISOs are certified in the knowledge of and experience in the following C|CISO Domains:

1. Governance and Risk Management (Policy, Legal, and Compliance)
2. Information Security Controls, Compliance, and Audit Management
3. Security Program Management & Operations
4. Information Security Core Competencies
5. Strategic Planning, Finance, Procurement, and Vendor Management

F.A.Q.

1. How do I sign up for the exam?

First, you must be approved to sit for the exam by filling out and returning this application to cciso@eccouncil.org. Once approved, you may purchase a voucher and instruction regarding where and how to do that will be sent to you with your approval.

2. What resources are available to help me prepare for the CCISO exam?

The CCISO Body of Knowledge courseware and the online training program are available for purchase here: https://iclass.eccouncil.org/.
For instructor-led, in-person classes, please check the EC-Council CISOP program website here: https://ciso.eccouncil.org/cciso-certification/cciso-training-study-options/.

3. What are the cost associated with the C|CISO application and exam?

The application fee for the eligibility application is $100. Once approved, the voucher for the exam can be purchased for $999. Instructions on where and how to purchase the exam voucher will be sent to you once you are approved. These costs do not apply to students who have purchased training packages.

4. What experience and skills do I need to possess in order to qualify to sit for the CCISO exam?

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 C|CISO Exam Eligibility Application Form higher education. Please see the chart below for more details on waivers. Experience Waivers are granted in certain domains in the case of industry accepted, professional certifications and higher degrees in information security as show below. 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.

DOMAIN	PROFESSIONAL CERTIFICATION WAIVERS	EDUCATION WAIVERS
1. Governance and Risk Management (Policy, Legal, and Compliance)	CGEIT, CRISC, HISP	Ph.D. Information Security – 3 years, MS Information Security Management, MS Information Security Engineering – 2 years, BS Information Security – 2 years
2. Information Security Controls, Compliance, and Audit Management	CISA, CISM, HISP	Ph.D. Information Security – 3 years, MS Information Security Management, MS Information Security Engineering – 2 years, BS Information Security – 2 years
3. Security Program Management & Operations	PMP, ITIL, PM in IT Security, HISP	Ph.D. Information Security – 3 years, MS Information Security or MS Project Management – 2 years, BS Information Security – 2 years
4. Information Security Core Competencies	CISSP, LPT, E|DRP, CIPP, MBCP – 2 years	Ph.D. Information Security – 3 years, MS Information Security – 2 years, BS Information Security – 2 years
5. Strategic Planning, Finance, Procurement, and Vendor Management	None	CPA, MBA, M. Fin. – 3 years

5. Can I be Grandfathered into the program?

No. Grandfathering for the CCISO program ended December 31, 2013. There are no exceptions.

6. Does the CCISO Program map to any US Government frameworks?

Yes, the CCISO program maps to the US Government's NICE framework. You can learn more here: http://ciso.eccouncil.org/wp-content/uploads/2013/09/NICE-IA-Framework-and-EC-Council-CertsEcosystem-Mapping-CCISO.pdf.

7. What if I am not qualified 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.

8. How do I know if C|CISO is for me?

C|CISO is the right choice for you and your career if you:
- Aspire to attain the highest regarded title within the information security profession – CISO
- Already serve as an official CISO
- Or perform CISO functions in their organization without the official title

9. How long is the CCISO certification valid?

Your C|CISO certification is valid for a period of one year.

10. What do I need to do to renew my certification?

To renew your certification you must satisfy the Continuing Education requirements and remit a renewal fee of $100.00 (USD).

11. I have more questions.

We are happy to answer your questions. Please email us at CCISO@eccouncil.org or call +1-505-341-3228 for more information.

EC-COUNCIL C|CISO Application Form

Section 1: Applicant Information

First Name:

Last Name:

Address:

City:

State:

Country:

Postal Code:

Business or Home Phone:

Business or Home E-mail:

Current Employer:

Current Title/Position:

Have you taken Accredited CCISO training?

☐ **Yes** ☐ **No**

If yes: Name of Training Center:
(if iLearn or direct EC-Council class, enter "ECC")

Name of Instructor:

Class Date:

If you have an EISM voucher, please enter the number here:

Section 2: Employment Information

For each employer, enter information that pertains to the Information Security and Management experience that you have gained during this employment period. Beginning with the most current position, enter each job title(s) held and the start and end dates of your employment (month/day/year). Place a check mark next to each of the domains that your employment covered. If you need to add more employers to show 5 years of experience in each of the 5 domains, please do so on an attachment that shows the same information that is requested on the application. Resumes cannot be accepted in lieu of the information on the application.

The 5 C|CISO Domains are:

1. Governance (Policy, Legal & Compliance)
2. IS Management Controls and Auditing Management (Projects, Technology & Operations)
3. Management – Projects and Operations
4. Information Security Core Competencies
5. Strategic Planning and Finance

Employer 1 Name:

Job Title:

Employment Start Date:

Employment End Date:

Please check the domains that this employment covered:

- ☐ **Domain 1**
- ☐ **Domain 2**
- ☐ **Domain 3**
- ☐ **Domain 4**
- ☐ **Domain 5**

Employer 2 Name:

Job Title:

Employment Start Date:

Employment End Date:

Please check the domains that this employment covered:

- ☐ **Domain 1**
- ☐ **Domain 2**
- ☐ **Domain 3**
- ☐ **Domain 4**
- ☐ **Domain 5**

Employer 3 Name:

Job Title:

Employment Start Date:

Employment End Date:

Please check the domains that this employment covered:

- ☐ **Domain 1**
- ☐ **Domain 2**
- ☐ **Domain 3**
- ☐ **Domain 4**
- ☐ **Domain 5**

Employer 4 Name:

Job Title:

Employment Start Date:

Employment End Date:

Please check the domains that this employment covered:

- ☐ **Domain 1**
- ☐ **Domain 2**
- ☐ **Domain 3**
- ☐ **Domain 4**
- ☐ **Domain 5**

Employer 5 Name:

Job Title:

Employment Start Date:

Employment End Date:

Please check the domains that this employment covered:

- ☐ **Domain 1**
- ☐ **Domain 2**
- ☐ **Domain 3**
- ☐ **Domain 4**
- ☐ **Domain 5**

Section 3: Experience Information Summary

Summarize your employment and C|CISO domain work experience from all employers listed above by listing the number of years of experience you have gained in each domain. Keep mind that experience can be earned in more than one domain at the same time. Most high-level information security jobs require work in all five domains at the same time, so even though you may list 5 years in each domain, that does not imply that you have (or that this program requires) 25 years of experience. The number in each box for each domain should correspond to the total years of experience you listed in the Employment sections (Section 2.a-e above) (sum of each job listed).

Domain 1	**Domain 2**	**Domain 3**	**Domain 4**	**Domain 5**
Section 3.a	Section 3.b	Section 3.c	Section 3.d	Section 3.e

Section 4: Waivers (optional)

If you have the required years of experience (5 years in each domain for candidates not taking training and 5 years in 3 of the 5 domains for students taking training), skip to Section 5. This section is only required if you are lacking in experience and are requesting waivers in order to qualify for the CCISO exam.

Summarize the waivers you are submitted for acceptance below. For more information regarding ECCouncil's waiver policy, please see the table on page 2 of this document. If you are submitting professional certifications, please include a scan of the certificate as well as the certificate number (if not visible on the certificate). If you are submitting education for a waiver, please make sure to send your unofficial transcript along with your application. Please list the certifications or waivers you are submitting for each domain below. Between certification and training waivers, applicants can only waive 3 years of experience for each domain. Only three years will be waived for each domain regardless of how many waivers you qualify for in each domain.

Please remember: If you have the required years of experience, this section is not required and will not be evaluated.

1. Domain 1 (list certifications/degrees):

Section 4.a

Number of Years Waived:

2. Domain 2 (list certifications/degrees):

Section 4.a

Number of Years Waived:

3. Domain 3 (list certifications/degrees):

Section 4.a

Number of Years Waived:

4. Domain 4 (list certifications/degrees):

Section 4.a

Number of Years Waived:

5. Domain 5 (list certifications/degrees):

Section 4.a

Number of Years Waived:

Section 5: Experience & Waiver Totals

In the boxes below, please put the total number of years experience plus years requested for waivers for each domain:

Domain 1

Section 3 a plus Section 4.a:

Domain 2

Section 3 b plus Section 4.b:

Domain 3

Section 4 c plus Section 5 c:

Domain 4

Section 4 d plus Section 5.d:

Domain 5

Section 4 e plus Section 5.e:

Section 6: Employment and C|ISO Domain Work Experience Verification

Please identify up to five individuals qualified to verify your work experience in each of the five CCISO Domains. Please submit as many verifiers as is necessary. All CCISO applicants must be verified, regardless of waivers or experience level. EC-Council will independently reach out to the verifiers listed to confirm your experience in the domains you indicate below:

Verifier 1

Name:

Job Title:

Company Name:

Business Phone:

Email Address:

Domains to be Verified:

- **Domain 1**
- **Domain 2**
- **Domain 3**
- **Domain 4**
- **Domain 5**

Verifier 2

Name:

Job Title:

Company Name:

Business Phone:

Email Address:

Domains to be Verified:

- [ ] **Domain 1**
- [ ] **Domain 2**
- [ ] **Domain 3**
- [ ] **Domain 4**
- [ ] **Domain 5**

Verifier 3

Name:

Job Title:

Company Name:

Business Phone:

Email Address:

Domains to be Verified:

- [ ] **Domain 1**
- [ ] **Domain 2**
- [ ] **Domain 3**
- [ ] **Domain 4**
- [ ] **Domain 5**

Verifier 4

Name:

Job Title:

Company Name:

Business Phone:

Email Address:

Domains to be Verified:

- ☐ **Domain 1**
- ☐ **Domain 2**
- ☐ **Domain 3**
- ☐ **Domain 4**
- ☐ **Domain 5**

Verifier 5

Name:

Job Title:

Company Name:

Business Phone:

Email Address:

Domains to be Verified:

- ☐ **Domain 1**
- ☐ **Domain 2**
- ☐ **Domain 3**
- ☐ **Domain 4**
- ☐ **Domain 5**

I hereby submit my application for EC-Council's C|CISO certification. I certify that the information provided by me is true and accurate. In the event that any statements or information provided by me in this application is false and/or if I violate any of the rules and regulations governing C|CISO certification, I agree to denial of certification. I agree to adhere to the EC-Council's Code of Professional Ethics and the Continuing Education Policy. I authorize EC-Council to disclose my certification status. Contact my verifiers (Listed above), employers, and/or suitable parties in order to verify the authenticity of my claims. Information may be used by EC-Council to contact me and to send me information about products and services that may be of interest to me, including marketing and promotional materials. I understand that the decision to grant me access to the C|CISO exam rests solely and exclusively with EC-Council and that EC-Council's decision is final. I agree to hold EC-Council, its officers, directors and employees harmless from any complaint or damage arising out of any action or omission by any of them in connection with this application, the application process or the failure to issue me C|CISO certification.

By submitting this form to EC-Council, I agree to indemnify and hold EC-Council, its corporate affiliates, and their respective officers, directors and shareholders harmless from and against any and all liabilities arising from my submission of Personally Identifiable Information (such as passport, government ID, social security number etc.) to EC-Council. I understand that should EC-Council receive any Personally Identifiable Information attached to this application, this application will be rejected.

Signature:

Date: **Typed Name:**

Note: We do accept electronic signatures as long as the signature can be validated by standard Adobe Reader software. If you use a digital signature that cannot be recognized by the Application Processing Team, a standard signature will be requested.

Strictly Confidential

EC-Council DECLARATION OF NO CRIMINAL CONVICTION
To: The President International Council of E-Commerce
Consultants 6330 Riverside Plaza Ln NW Suite 210
Albuquerque, NM
87120 United States
of America

Sir, IN CONSIDERATION of being granted the Certified Chief Information Security Officer (C|CISO) credential, I HEREBY DECLARE that:

1. I have not been convicted of any felony; I do not have a criminal background whatsoever and do not intend to use the certification for any purpose other than what it is intended.

2. International Council of E-Commerce Consultants (EC-Council) has the right to revoke or reject my certification status or application package if I am found to have been involved in criminal activity pre or post certification.

3. EC-Council has the right to revoke the C|CISO credential if I fail to pay fees due and/or fail to maintain the required points under EC-Council's Continuing Education system. EC-Council has the right to request a criminal background/police verification report to prove that I have not committed any crimes as a basis for licensure renewal.

4. All information contained in my C|CISO Application package are true and correct.

5. I will not make any derogatory remarks against EC-Council or its certifications.

6. I will not use the C|CISO credential for fraud, deception, theft, sabotage or other malicious or unethical activities.

7. EC-Council shall not be held liable or responsible for the lack of knowledge, experience, or quality of work as a Certified Chief Information Security Officer.

8. I will adhere to the C|CISO Code of Ethics.

9. I will comply with all the obligations and requirements of the C|CISO credential.

10. I indemnify EC-Council against any claims that arise against EC-Council due to my negligence, inaptitude or for any other reason whatsoever in the execution of my duties as a Certified Chief Information Security Officer or the revocation of my license.

11. I declare under the penalties of perjury that all information provided by myself to EC-Council is true and correct.

Signature:

Date: **Typed Name:**

Note: We do accept electronic signatures as long as the signature can be validated by standard Adobe Reader software. If you use a digital signature that cannot be recognized by the Application Processing Team, a standard signature will be requested.

C|CISO Professional Code of Conduct v1.0

Preamble The C|CISO Professional Code of Conduct ("Code") has been established to act as a guide for C| CISO Professionals. C|CISO Professionals are advised to refer to the Code when faced with ethical or moral dilemmas. All C|CISO Professionals must abide by and enforce the Code. Any violation of the Code will be subject to review by EC-Council and may lead to suspension or revocation of the C|CISO Professional certification.

By adhering to this Code, C|CISO Professionals agree to uphold their responsibilities to society, the profession, their employers, and their clients at all times.

Code of Conduct
The Code is divided into four main principles:

1. To act within legal limits
2. To act with honesty and integrity
3. To uphold professionalism
4. To maintain privacy and confidentiality

1. To act within legal limits

- C|CISO Professionals shall respect and abide by all local, state, federal and international laws pertaining to their course of work.
- C|CISO Professionals shall ensure that they do not engage in any unlawful activities.
- C|CISO Professionals shall report to the proper authorities all and any unlawful acts known to them.
- C|CISO Professionals shall honor the work agreement signed between himself and the client organization and stay within the limits of the agreement.

2. To act with honesty and integrity

- C|CISO Professionals shall act with full honesty, integrity and responsibility at all times.
- C|CISO Professionals shall not partake in any deceptive or manipulative activities.
- C|CISO Professionals shall not partake in activities which have a negative outcome on society.
- C|CISO Professionals shall avoid real or perceived conflicts of interest whenever possible and disclose them to affected parties when they do exist.
- C|CISO Professionals shall carry out their duties in an ethical manner without harm to the client organization.

3. C|CISO Professionals shall not partake in any malicious activity towards the client organization and protect the systems of the client organization to the best of his ability in the course of his duties.

4. To uphold professionalism

- C|CISO Professionals shall demonstrate high standards and professional care in their course of work.
- C|CISO Professionals shall promote an objective and fair work environment.
- C|CISO Professionals shall render service for which they are competent and not claim knowledge on areas for which they are incompetent.
- C|CISO Professionals shall respect and not tarnish the reputation of certifications by other organizations or establishments.

5. To maintain privacy and confidentiality

- C|CISO Professionals shall maintain the privacy and confidentiality of all information encountered in their course of work unless required by a legal authority.
- C|CISO Professionals shall not disclose or misuse any information encountered for personal benefit.

Signature:

Date: **Typed Name:**

Note: We do accept electronic signatures as long as the signature can be validated by standard Adobe Reader software. If you use a digital signature that cannot be recognized by the Application Processing Team, a standard signature will be requested.