

Issue Date: July 1<sup>st</sup>, 2020

**EC-Council**



# C|CISO Candidate Handbook v4

# Table of Contents

1. Objective of CCISO Candidate Handbook.....	1
2. About EC-Council.....	2
3. What is the CCISO credential?.....	3
4. CCISO Testimonials.....	4
5. Steps to Earn the ANSI accredited CCISO credential.....	5
6. To Attempt the CCISO Exam.....	6
7. Retakes & Extensions.....	23
8. EC-Council Special Accommodation Policy.....	24
9. EC-Council Exam Development & Exam Item Challenge.....	29
10. EC-Council Certification Exam Policy.....	33
11. CCISO Credential Renewal .....	38
12. EC- Council Continuing Education (ECE) Policy.....	39
13. CCISO Career Path.....	42
14. Code of Ethics.....	43
15. Ethics Violation .....	45
16. Appeal Process .....	47
17. Change in Certification Scope.....	52
18. Logo Guidelines.....	53
19. FAQ .....	58
Appendix A .....	62
Appendix B .....	80

## Objective of C|CISO Candidate Handbook

The C|CISO Candidate Handbook outlines the following:

- a. Impartiality and objectivity is maintained in all matters regarding certification.
- b. Fair and equitable treatment of all persons in certification process.
- c. Provide directions for making decisions regarding granting, maintaining, renewing, expanding and reducing EC-Council certification/s
- d. Understand boundaries/limitations and restrictions of certifications.

# About EC-Council

The International Council of E-Commerce Consultants (EC-Council) is a member-based organization that certifies individuals in various e-business and information security skills. It is the owner and creator of the world famous Certified Ethical Hacker (CEH), Computer Hacking Forensics Investigator (CHFI), EC-Council Certified Security Analyst (ECSA), License Penetration Tester (LPT) certifications and as well as many other certifications that are offered in over 194 countries globally.

The EC-Council mission is “to validate information security professionals who are equipped with the necessary skills and knowledge required in a specialized information security domain that will help them avert a cyber conflict, should the need ever arise.” EC-Council is committed to uphold the highest level of impartiality and objectivity in its practices, decision making, and authority in all matters related to certification.

As of June 30, 2020, EC-Council has over 268567 certifications granted to those who successfully earned the standards required to hold an EC-Council title. Individuals who have achieved EC-Council certifications include those from some of the finest organizations around the world such as the US Army, the FBI, Microsoft, IBM and the United Nations.

Many of these certifications are recognized worldwide and have received endorsements from various government agencies including the US Federal Government via the Montgomery GI Bill, National Security Agency (NSA) and the Committee on National Security Systems (CNSS). Moreover, the United States Department of Defense has included the CEH program into its Directive 8570, making it as one of the mandatory standards to be achieved by Computer Network Defenders Service Providers (CND-SP).

EC-Council has also been featured in internationally acclaimed publications and media including Fox Business News, CNN, The Herald Tribune, The Wall Street Journal, The Gazette and The Economic Times as well as in online publications such as the ABC News, USA Today, The Christian Science Monitor, Boston and Gulf News.

For more information about EC-Council | Certification, please visit <https://cert.eccouncil.org/>



# What is the CCISO credential?

The CCISO certification is an industry-leading program that recognizes the real-world experience necessary to succeed at the highest executive levels of information security.

Bringing together all the components required for a C-Level positions, 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. 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. 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.

A core group of high-level information security executives, the CCISO Advisory Board, contributed by forming the foundation of the program and outlining the content that would be covered by the exam, body of knowledge, and training. Each segment of the program was developed with the aspiring CISO in mind and looks to transfer the knowledge of seasoned professionals to the next generation in the areas that are most critical in the development and maintenance of a successful information security program.



The Certified CISO (CCISO) program is the first of its kind training and certification program aimed at producing top-level information security executives. The CCISO does not focus solely on technical knowledge but on the application of information security management principles from an executive management point of view. The program was developed by sitting CISOs for current and aspiring CISOs.

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

Domain 1: Governance (Policy, Legal & Compliance)

Domain 2: IS Management Controls and Auditing Management (Projects, Technology & Operations)

Domain 3: Management – Projects and Operations

Domain 4; Information Security Core Competencies

Domain 5: Strategic Planning and Finance

# CCISO Testimonials

“ Testimonial / Your feedback: Conducting the CISO course with EC-Council's brought a broadened view of the importance of developing an Information Governance model together with senior management.

With acquired knowledge it is possible to establish guidelines and premises that enable the board to evaluate the area of information security as an ally of the business.

Another relevant point in training and the quality of the content and its clarity in the management model.

I strongly recommend this training to all those who seek professional improvement, a holistic view of the area of information security integrated with corporate strategy.

**Full Name: ALEX GOMES GALHO**  
**Designation: CISO**  
**Organisation/Institution: FGC CREDIT GUARANTEE FUND**

“ Testimonial / Your feedback: Cyber Security become a necessity, we should keep our organization far from the bad guys, so what can we do? How can we go forward with all these new threats?

I think Ec-council helps us to move forward and protect our organization, I did in the past the training Certified Ethical Hacker, and now I did the Certified Chief information security officer.

The CCISO help us to have a different view to help our business to become more safe and grow.

I would like to say thank you very much, I think this was the best training Course I did in My Life.

**Full Name: Leandro Ribeiro**  
**Designation: Leader of Cyber Defense**  
**Organisation/Institution: UnitedHealth Group Brazil**

“ Testimonial / Your feedback: “I don't have any doubt: C|CISO is a best training I've made in this year (maybe in my life). The EC-Council partner, the instructor, the material, the colleagues and the shared knowledge are invaluable. Highly recommendable, of course!”

**Full Name: Sergio Antonio Pohlmann**  
**Designation: CISO**  
**Organisation/Institution: A.F. Electrical Industries - Panambi, Brazil**

“ Testimonial / Your feedback: The C|CISO classroom environment was one of engagement and learning of the CISO body of knowledge fundamentals. The course pushed for table top scenario responses in the form of teams, which allowed each attendee to provide their insight and experience, but also allowed the ability to learn from others. This course and certification is more than just a check in the box, it helps reinforce and grow the fundamentals a senior cyber security professional already has skill and knowledge wise.

**Full Name: Heath Cory Renfrow**  
**Designation: CISO**  
**Organisation/Institution: Army Medicine**

“ Testimonial / Your feedback: I am already performing the functions of CISO so the CCISO program gave me the necessary training to carry out the tasks correctly. My goal is to apply all the knowledge gained. I think the instructor, material and facilities for the course are excellent, I think it was 5 days where I really enjoyed the program.

**Full Name: Carlos Alberto Blanco**  
**Designation: Chief Information Security**  
**Organisation/Institution: Grant Thornton México**

For latest CCISO Testimonials, please visit <https://cert.eccouncil.org/cciso-testimonials.html>

# Steps to Earn the ANSI accredited CCISO credential

Candidates will be granted the Certified Chief Information Security Officer credential by passing a proctored CCISO exam.

The exam consists of 150 multiple-choice questions administered over a two-and-a-half-hour period.

The ANSI accredited CCISO exam is available at EC-Council Test Centers. Please contact [https://eccouncil.zendesk.com/anonymous\\_requests/new](https://eccouncil.zendesk.com/anonymous_requests/new) to provide you with the locations of the nearest test centers that proctor the ANSI accredited CCISO exam.

You will be tested in the following task and knowledge domains of CCISO:

- ◆ **Governance (Policy, Legal & Compliance)**
- ◆ **IS Management Controls and Auditing Management (Projects, Technology & Operations)**
- ◆ **Management – Projects and Operations**
- ◆ **Information Security Core Competencies**
- ◆ **Strategic Planning and Finance**

If you are interested in knowing the objectives of the ANSI accredited CCISO exam, or the minimum competencies required to pass the ANSI accredited CCISO exam, please refer to Appendix A: CCISO Exam Blueprint.

Upon successfully passing the exam you will receive your digital ANSI accredited CCISO certificate within 7 working days.

The CCISO credential is valid for 3 year periods but can be renewed each period by successfully earning EC-Council Continued Education (ECE) credits. Certified members will have to achieve a total of 120 credits (per certification) within a period of three years. An annual fee of \$100 is applicable.

All EC-Council related correspondence will be sent to the email address provided during exam registration. If your email address changes notify EC-Council by contacting us at [https://eccouncil.zendesk.com/anonymous\\_requests/new](https://eccouncil.zendesk.com/anonymous_requests/new); failing which you will not be able to receive critical updates from EC-Council.

# To Attempt the CCISO Exam

In order to be eligible to attempt the CCISO certification examination, you may:

## Completed Official Training

Candidates who have completed the official training must show experience in three out of the five CCISO Domains via the application process to take the CCISO Exam and earn the certification.

Prior to attempting the exam, you are required to AGREE to:

- a. EC-Council Non-Disclosure Agreement terms
- b. EC-Council Candidate Certification Agreement terms

You should NOT attempt the exam unless you have read, understood and accepted the terms and conditions in full. BY ATTEMPTING THE EXAM, YOU SIGNIFY THE ACCEPTANCE OF THE ABOVE MENTIONED AGREEMENTS available on Appendix B. In the event that you do not accept the terms of the agreements, you are not authorized by EC-Council to attempt any of its certification exams.



## B. Attempt Exam without Official Training

Candidates who do not attend official training must show experience in all five CCISO Domains via the application process to take the CCISO Exam and earn the certification. Credit toward experience is granted in certain domains in the case of industry-accepted, professional certifications and higher degrees in information security as shown below. Between certification and training waivers, applicants can only waive 3 years of experience for each domain.

Waivers for the CCISO are available to Self-Study Candidates

Domain	Professional Certification Waivers	Education Waivers
1. Governance (Policy, Legal & 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. IS Management Controls and Auditing Management (Projects, Technology & Operations)	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. Management – Projects and 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 and Finance	None	CPA, MBA, M. Fin. – 3 years

Candidates must have five years of experience in each of the 5 CCISO domains verified via the Exam Eligibility Application.



## Eligibility Process:

- The CCISO program requires the applicant to have five years of work experience in the Information Security domain in each of the five CCISO domains and should be able to provide a proof of the same as validated through the application process unless the candidate attends official training. For more information on the five CCISO domains please visit <https://ciso.eccouncil.org/cciso-certification/cciso-domain-details/>
- The application process can take up to six weeks depending on how quickly the verifier(s) listed on the application take to respond.
- Applications, questions about the application process, and inquiries regarding where an application is in the process should be sent to [cciso@eccouncil.org](mailto:cciso@eccouncil.org) for US applicants and [ccisoapp@eccouncil.org](mailto:ccisoapp@eccouncil.org) for International applicants.
- On the application, there is a section for the applicant to list verifiers for each domain.
- Each domain for which the applicant is claiming experience needs to be verified by a supervisor, client, peer, or other individual in the position to respond regarding the applicant's experience and expertise.
- More than one domain may be verified by each verifier, so it is possible to list one verifier to verify all domains.
- If the application is approved, the applicant will be sent instructions on purchasing a voucher from EC-Council directly.
- EC-Council will then send the candidate the voucher code which candidate can use to register and schedule the test.
- If application is not approved, the application fee of USD 100 will not be refunded.
- The approved application is valid for 3 months from the date of approval so the candidate must purchase a voucher within 3 months. After the voucher code is released, the applicant has one year to use the code.
- Should you require the exam voucher validity to be extended, kindly contact [certmanager@eccouncil.org](mailto:certmanager@eccouncil.org) before the voucher expires. Only valid vouchers can be extended once.
- An application extension request will require the approval of the Director of Certification.

## C. Take the EC-Council Information Security Manager (EISM) Exam

Candidates who take CCISO training and who either do not qualify for the CCISO exam or who do not want to go through the application process can take the EISM exam and earn that certification. EISMs can reapply to the CCISO program and purchase a voucher for 50% off when they accrue the required experience.

# EC-Council Exam Eligibility Application Form v3

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 (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

**Confidentiality Of Information:** We treat personal information securely and confidentially. EC-Council adheres to strict US privacy laws and will not disclose the submitted information to any third party with the exception of your Boss / Supervisor / Department head. (As stated above, verification is required.)

**Disclaimer:** EC-Council reserves the right to deny certification to any candidate who attempts to sit for this exam without qualifying as per the mentioned eligibility criteria. Should the audit team discover that a certification was granted to a candidate who sat for the exam and did not qualify as per the eligibility criteria, EC-Council also reserves the right to revoke the candidate's certification.

**Retention Of Documentation:** EC-Council will not retain any supporting documents related to the application beyond a period of 2 years from date of receipt.

**Special Accommodation:** Should you have a special accommodation request, you can write to us at [certmanager@eccouncil.org](mailto:certmanager@eccouncil.org), for more information on our special accommodation policy please refer to <https://cert.eccouncil.org/special-accommodation-policy.html>

## 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 [ccisoapp@eccouncil.org](mailto:ccisoapp@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/ciso-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 (Policy, Legal, & Compliance)	CGEIT, CRISC	Ph.D. Information Security, MS Security Management, MS Information Security Engineering (3 years), BS Information Security (2 Years)
2. IS Management Controls & Auditing Management	CGEIT, CRISC	Ph.D. Information Security, MS Security Management, MS Information Security Engineering (3 years), BS Information Security (2 Years)
3. Leadership – Projects and Operations	PMP, ITL, PM in IT Security,	Ph.D. Information Security, MS Security Management, MS Information Security Engineering (3 years), BS Information Security (2 Years)
4. Information Security Core Concepts	CISSP, LPT, EDRP, CIPP, MBCP, CEH, CHFI	Ph.D. Information Security, MS Security Management, MS Information Security Engineering (3 years), BS Information Security (2 Years)
5. Strategic Planning & Finance	None	Ph.D. Information Security, MS Security Management, MS Information Security Engineering, (3 years); CPA, MBA, M. Fin. (2 years)

## 5. 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: <https://ciso.eccouncil.org/wp-content/uploads/2013/09/NICE-IA-Framework-and-EC-Council-Certs-Ecosystem-Mapping-CCISO.pdf>

## 6. 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.

## 7. 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

## 8. 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).

## 9. I have more questions.

We are happy to answer your questions. Please email us at [ccisoapp@eccouncil.org](mailto:ccisoapp@eccouncil.org)

# 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 4**

**Domain 2**

**Domain 5**

**Domain 3**

---

**Employer 2 Name:**

**Job Title:**

**Employment Start Date:**

**Employment End Date:**

**Please check the domains that this employment covered:**

**Domain 1**

**Domain 4**

**Domain 2**

**Domain 5**

**Domain 3**

---

**Employer 3 Name:**

**Job Title:**

**Employment Start Date:**

**Employment End Date:**

**Please check the domains that this employment covered:**

**Domain 1**

**Domain 4**

**Domain 2**

**Domain 5**

**Domain 3**

Employer 4 Name:

Job Title:

Employment Start Date:

Employment End Date:

Please check the domains that this employment covered:

Domain 1

Domain 4

Domain 2

Domain 5

Domain 3

Employer 5 Name:

Job Title:

Employment Start Date:

Employment End Date:

Please check the domains that this employment covered:

Domain 1

Domain 4

Domain 2

Domain 5

Domain 3

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 101C Sun Ave NE  
Albuquerque, NM 87109

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.



# Retakes & Extensions

## EC-Council Exam Retake Policy

If a candidate does not successfully pass an EC-Council exam, he/she can purchase ECC Exam center voucher to retake the exam at a discounted price.

- a. If a candidate is not able to pass the exam on the first attempt, no cooling or waiting period is required to attempt the exam for the second time (1st retake).
- b. If a candidate is not able to pass the second attempt (1st retake), a waiting period of 14 days is required prior to attempting the exam for the third time (2nd retake).
- c. If a candidate is not able to pass the third attempt (2nd retake), a waiting period of 14 days is required prior to attempting the exam for the fourth time (3rd retake).
- d. If a candidate is not able to pass the fourth attempt (3rd retake), a waiting period of 14 days is required prior to attempting the exam for the fifth time (4thd retake).
- e. A candidate is not allowed to take a given exam more than five times in a 12 month (1 year) period and a waiting period of 12 months will be imposed before being allowed to attempt the exam for the sixth time (5th retake).
- f. Candidates who pass the exam are not allowed to attempt the same version of the exam for the second time.

EC-Council strongly advises candidate who fail the exam for the third time (2nd retake) to attend official hands-on training that covers the certification objectives. This is not applicable for LPT (Master) Exam.

EC-Council reserves the right to revoke the certification status of candidates who attempt the exam without abiding to EC-Council retake policy as stated above.

## Extension Policy

EC-Council exam vouchers are valid for a maximum period of one year from the date of purchase. A candidate may opt to extend his/her EC-Council exam vouchers for an additional 3 months for \$35 if the voucher is valid (not used and not expired). Vouchers can only be extended once.

## Voucher Policy

Once purchased, EC-Council vouchers (new, retake, or extended) are non-refundable, nontransferable, and non-exchangeable. EC-Council reserves the right to revoke the certification status of candidates who attempt the exam without abiding to any of the above EC-Council voucher policies.

# EC-Council Special Accommodation Policy

A candidate with disabilities is defined as a person who has a physical, sensory, physiological, cognitive and/or developmental impairment that makes it difficult or impossible to attempt EC-Council certification exams using the standard testing equipment or within the standard exam duration.

In line with EC-Council's commitment to comply with the Americans with Disabilities Act (ADA, 1991), EC-Council will accommodate reasonable requests by candidates with disabilities who would like to attempt any EC-Council certification exams. Such requests will fairly equate disabled candidates with other candidates and enable them to denote their skills and knowledge in EC-Council's exams.

The special accommodation request is evaluated based on the candidate's particular accommodation request, nature of disability, and reasonableness of the request. The request form requires a legally approved expert, practitioner, or professional in the fields of physical or mental healthcare to confirm the need for special accommodation. The request form has 2 sections:

Section 1 should be filled and signed by the candidate, and Section 2 is to be filled and signed by a legally approved professional, expert or practitioner to support the candidate's special accommodation request. The information requested by EC-Council will be held in strict confidence and will not be released without the candidate's permission.

Candidates are required to submit their special accommodation requests to EC-Council at least 30 days prior to registering for an exam. EC-Council will respond with its decision within 14 days and provide the contact details of testing center/s that have the infrastructure to accommodate the candidate's special needs.

**For any details or clarification, please email to [certmanager@eccouncil.org](mailto:certmanager@eccouncil.org)**

# EC-Council

## Special Accommodation Request Form

Please submit the completed form to EC-Council as following:

E-mail Procedure	Send the form to <a href="mailto:certmanager@eccouncil.org">certmanager@eccouncil.org</a> Please attach the form as a scanned document that includes the certifying authority's signature.
------------------	---

### Section1:APPLICANTINFORMATION

Name : .....

Address (including city, state, and postal code) : .....

.....

.....

PhoneNumber: .....

Email Address: .....

EC-Council Voucher Number (if available): .....

Please list all examinations and versions for which you are requesting accommodations:

.....

.....

.....

.....

Signature: ..... Date: .....

# EC-Council

## Special Accommodation Request Form

### Section 2: DOCUMENTATION OF ACCESSIBILITY NEEDS

I have known..... since .....  
(Examination applicant name) (Date)

in my capacity as a .....  
(Professional title)

I have read the accompanying description of potential accessibility barriers and understand the nature of the examination(s) to be administered, and I certify that I have documentation on record supporting the need for accommodation. I believe that this applicant should be provided the following accommodations (identify relevant accommodations):

- ☐ Accessible testing site (for example, ramp for wheelchairs)
- ☐ Amanuensis (recorder of answers)
- ☐ Extended exam time—one and one-half times the usual allotment
- ☐ Extended exam time—twice the usual allotment
- ☐ Extra time for breaks (specify frequency and duration): .....
- ☐ Reader (person to read the exam items aloud)
- ☐ Separate testing room
- ☐ Special chair (specify type): .....
- ☐ Special input device, such as a trackball mouse (specify type): .....
- ☐ Special output device, such as a larger monitor (specify type): .....
- ☐ Written instruction of exam procedures
- ☐ Other (please describe in the space below):  
.....  
.....  
.....  
.....

# EC-Council

## Special Accommodation Request Form

Justification for accommodation (include description of condition):

.....

.....

.....

.....

.....

.....

Contact information for professional certifying accommodation needs:

Professional's Name:.....

Professional's Title :.....

License Number  
and Type (if applicable): .....

Phone Number :.....

Email Address : .....

Signature:..... Date: .....

# EC-Council

## Special Accommodation Request Form

### POTENTIAL ACCESSIBILITY BARRIERS

Standard format for EC-Council certification exams present the following potential accessibility barriers.

#### Manual

Examinees must use a mouse to point-and-click, click-and-drag, navigate from one question to the next by clicking, and perform tasks in a simulated or emulated software environment. Exam question formats include multiple choice questions in which the candidate answers by clicking on the selected response(s).

#### Optical

**Reading text:** Exam questions are written at a reading level appropriate to the content. The electronic exams must be read on a 15-inch or larger monitor with at least 1024 × 768 resolution. The font can be as small as 9 pt. in graphics and 11 pt. in text. Graphics will be displayed on the monitor (possibly in color).

#### Physical Stamina

Exams last for 2.5 hours (standard)

If you need more information in order to decide what accommodations are necessary, please contact the EC-Council Certification Division at [certmanager@eccouncil.org](mailto:certmanager@eccouncil.org)

# ANSI ACCREDITED CCISO EXAM DEVELOPMENT & EXAM ITEM CHALLENGE

Exam development is a pivotal process that emphasizes on the technical, structural, semantic, and linguistic quality of exam items. Exam quality checks are done by a team of independent experts and professionals to ensure that the exam items are clear, error-free, unbiased and/or unambiguous.

## Development Process

An invaluable input from industry experts was considered in the ANSI accredited CCISO exam development, especially on how the CCISO qualifications and credentials are exercised worldwide. The CCISO exam is meant to meticulously and unsparingly transcend ordinary knowledge to reflectively gauge the necessary knowledge and skill required by experts in Information Security.

## Development phases

The CCISO exam development process is comprised of 9 phases that cogently focus on optimizing the exam to reflect qualities of relevance, validity and reliability.

### ◆ Objective domain definition

Subject matter experts (SMEs) highlight the significant job functions of a CISO.

### ◆ Job analysis

The job analysis identifies the tasks and knowledge important to the work performed by professionals in the field of IT Security; and, creates test specifications that may be used to develop the ANSI accredited CCISO exam. The result of a job analysis is a certification exam blueprint.

The tasks and knowledge statements are transmuted into a survey that experts would use to rate, measure, and assess the skills and knowledge required. These ratings are used to rank the statements and determine the number of questions to stem from each exam statement.

### ◆ Scheme Committee Approval

EC-Council Scheme Committee, a group of experts, inspects and validates the objective domain and the approach used in the job analysis prior to the authoring or writing of the exams.

### ◆ Exam writing

SMEs write the exam items to measure the objectives stated in the exam blueprint. The exact number of exam items that they write is dependent on the feedback of the job analysis phase. The approved items are those that are technically, grammatically, and semantically clear, unbiased, and relevant.

### ◆ Standard setting

A panel of experts other than those who write the items will answer and rate all items to deduce a minimum passing or cut score. Scores vary from one exam to another due to the score dependence on the items pool difficulty.

### ◆ **Final Scheme Committee Approval**

The EC-Council Scheme Committee give their final approval of the whole process prior to the beta exam publication.

### ◆ **Beta exam**

Once the Scheme Committee approves the scheme a beta exam is published. Candidates are to sit for the beta exam under identical conditions to the real exam. The distribution of the beta exam scores enables EC-Council to assess and calibrate the actual exam for better quality.

### ◆ **Final evaluation**

The number and quality of items in the real live exam is determined by the scores and results of the beta exam. The analysis of the beta exam includes difficulty of items, capability of distinguishing level of candidates' competencies, reliability, and feedback from participants. EC-Council works closely with experts to continuously inspect the technical correctness of the questions and decide the pool of items that will be utilized for the live exam.

### ◆ **Final Exam Launch**

ECC operate and oversee the administration of EC-Council certification exams in their centers around the world.

If the candidate believes that a specific part of the CCISO exam is incorrect, he/she can challenge or request evaluation of the part in question via the steps enumerated below. This should be done within three calendar days of the exam day. Such a process is necessary to identify areas of weakness or flaws in the questions but the exam itself cannot be re-scored. Nevertheless, all possible efforts are not spared to assure the candidate's satisfaction. The candidate's feedback is paramount to EC-Council certification exams.

## **Steps for challenging exam items**

1. Fill and sign EC-Council Exam Feedback Form as detailed as possible. The detailed and clear description of the challenge will accelerate the review process. No candidate's exam item challenge of the exam's items will be considered without completing the form.
2. The form should be submitted within 3 calendar days from exam date to [tocertmanager@eccouncil.org](mailto:tocertmanager@eccouncil.org) with the subject line typed "Exam Item Evaluation". Only requests received within 3 working days from taking the exams will be reviewed.
3. The candidate must fill a separate form for each exam item he/she is challenging.
4. EC-Council will acknowledge receipt of the request by email. This may include a conclusive result of the evaluation, or an estimated time for the evaluation process to be completed and results to be shared with the candidate.



# EC-Council Exam Feedback Form

Use this form to describe in detail the specific reasons you are challenging an EC-Council Certification exam item. Include your contact information, registration ID, the number and name of the exam, the date you took the exam, and the location of the testing center. Please provide as much detail as possible about the item to expedite review. Your challenge will not be accepted for evaluation unless this form is complete.

Within three calendar days of taking the exam, submit this form by e-mail to [certmanager@eccouncil.org](mailto:certmanager@eccouncil.org) with "Exam Item Evaluation" in the subject line. You must submit a separate form for each exam item you are challenging.

Your submittal will be acknowledged through e-mail. At that time, you will receive either the result of the evaluation or, if more time is needed for evaluation, an estimate of when you can expect a decision.

Full Name : .....

Email Address : .....

Phone Number : .....

Mailing Address: : .....  
(including city, state,  
and postal code)

.....  
.....

Exam Portal : .....  
(VUE/ ECC Exam  
Center)

Exam Voucher No : .....

Exam No & Name : .....

Exam Date : .....  
(MM/DD/YYYY)  
(When did you take  
the exam?)

Test Center Location : .....  
(Where did you take  
the exam?)

Test Center Name : .....

Street Address : .....

City, State/ : .....

Province : .....

Zip/Postal Code : .....

Country : .....

# EC-Council Exam Feedback Form

Item Description  
(Describe the exam item in detail. Explain why you believe the item is not valid.)

.....

.....

.....

.....

.....  
Signature

.....  
Date

# EC-Council Certification Exam Policy

EC-Council has several exam policies to protect its certification program, including:

- a. Non-Disclosure Agreement (NDA)
- b. Candidate Certification Agreement (CCA)
- c. Security and Integrity Policy

## Non-Disclosure Agreement (NDA)

Prior to attempting an EC-Council exam, candidates are required to agree to EC-Council NDA terms. Candidates should not attempt the exam unless they have read, understood and accepted the terms and conditions in full. By attempting the exam, the candidates signify the acceptance of the NDA terms. In the event that the candidate does not accept the terms of the agreement, he/she is not authorized by EC-Council to attempt any of its certification exams.

The NDA mandates that candidates not to disclose exam content to any third party and do not use the content for any purpose that will negatively undermine the integrity and security of the certification exam. All content and wording of the exam questions is copyrighted by EC-Council under the protection of intellectual property laws.

Action will be taken against violators of their signed NDAs. EC-Council reserves the right to revoke the candidate's certification status, publish the infraction, and/or take the necessary legal action against the candidate.

[Please refer to Appendix B for EC-Council NDA.](#)

## Candidate Certification Agreement (CCA)

Prior to attempting an EC-Council exam, candidates are required to agree to EC-Council CCA terms. Candidates should not attempt the exam unless they have read, understood and accepted the terms and conditions in full. By attempting the exam, the candidates signify the acceptance of the CCA terms. In the event that the candidate does not accept the terms of the agreement, he/she is not authorized by EC-Council to attempt any of its certification exams. Through passing the certification exam, successful candidates are governed through EC-Council CCA. They are authorized to provide corresponding services and to use EC-Council marks, titles and benefits pertaining to the certification program(s) that the candidate has completed. Action will be taken against violators of their signed CCAs. EC-Council reserves the right to ban candidates from attempting EC-Council exams, revoke the candidate's certification status, publish the infraction, and/or take the necessary legal action against the candidate.

[Please refer to Appendix B for EC-Council CCA.](#)



## Security and Integrity

EC-Council is committed to communicating clearly what may or may not represent unethical, fraudulent, or cheating practices. We exert every effort to raise the necessary awareness among our candidates about this.

### Security Policies

The policies developed and maintained by EC-Council are meant to guard the integrity, confidentiality, and value of EC-Council exams and intellectual property.

#### a. Candidate bans

In the case of any infringement to any rules or policies in the NDA or any misdemeanor or misuse that harms certification program in whatever way, EC-Council reserves the right to bar the candidate from any future EC-Council certification exams by EC-Council. This may also be accompanied by EC-Council decertification. Below are some examples:

- The transference, distribution, creation, trading, or selling of any derived content of the exam through means like but not limited to copying, reverse-engineering, downloading or uploading, or any other form of distribution whether electronically, verbally, or via any other conventional or unconventional means for any purpose.
- Infringing EC-Council intellectual property.
- Utilizing the exam or any of its content in any way that may break the law.
- Not adhering to the exam retake policy
- Forgery of exam scores report or any manipulation with its content.
- Any sort of cheating during the exam including communicating with or peeking on other candidates answers.
- The sending or receiving of any information that can be a source of any assistance not in accordance with accepted rules or standards, especially of morality or honesty.
- The use of disallowed or unauthorized materials such as cheat sheets, notes, books, or electronic devices such as tablets or mobile phones.
- The use of certain materials that have been memorized re-created to provide an almost or close exact replica of the exam, widely known as “brain dump”.
- Identity impersonation when sitting for the exam.
- Not adhering to EC-Council NDA.
- Not adhering to EC-Council CPA.
- Not adhering to EC-Council exam guidelines.



## **b. Candidate Appeal Process**

- Banned candidates have the right to appeal to EC-Council. The candidate should fill the EC-Council Appeal form in full, attach his/her exam transcript and submit it to the certification department by raising a ticket at [https://eccouncil.zendesk.com/anonymous\\_requests/new](https://eccouncil.zendesk.com/anonymous_requests/new) within 90 days from the EC-Council ban date.
- EC-Council will complete its thorough investigation in a maximum 15 working days and will contact the candidate with the final decision.
- If the candidate is not satisfied by EC-Council's decision, he/she has the right to refer his/her case to the Scheme Committee. The Scheme Committee decision is final. Please refer to the Appeal Process section for more details.

## **c. Exam Retake Policy**

- If a candidate is not able to pass the exam on the first attempt, no cooling or waiting period is required to attempt the exam for the second time (1st retake).
- If a candidate is not able to pass the second attempt (1st retake), a waiting period of 14 days is required prior to attempting the exam for the third time (2nd retake).
- If a candidate is not able to pass the third attempt (2nd retake), a waiting period of 14 days is required prior to attempting the exam for the fourth time (3rd retake).
- If a candidate is not able to pass the fourth attempt (3rd retake), a waiting period of 14 days is required prior to attempting the exam for the fifth time (4thd retake).
- A candidate is not allowed to take a given exam more than five times in a 12 months (1 year) period and a waiting period of 12 month will be imposed before being allowed to attempt the exam for the sixth time (5th retake).
- Candidates who pass the exam are not allowed to attempt the same version of the exam for the second time.
- EC-Council strongly advises candidate who fail the exam for the third time (2nd retake) to attend official hands-on training that covers the certification objectives. This is not applicable for LPT (Master) Exam.
- EC-Council reserves the right to revoke the certification status of candidates who attempt the exam without abiding to EC-Council retake policy as stated above.



**d. EC-Council Test Center (ETC) Closures Due to Security or Integrity Reasons**

If there is a security or integrity issue with a certain testing center EC-Council may decide to suspend testing there until an investigation is complete or terminate the ETC status. EC-Council will provide affected candidates with a list of alternative test centers where they may attempt the EC-Council certification exam.

**e. Candidate Retesting at Request of EC-Council**

- In case of any suspicious patterns or trends on either the side of the candidate or the testing center EC-Council reserves the right to demand the candidate(s) to re-sit for the exam and/or assessment test. Candidate is to agree to the retest, failing which EC-Council will not award the certification to the candidate. Candidate will be given one chance to take the Candidate Retesting Audit (CRA) exam. Should candidate fail to pass the CRA exam, candidate will be given one chance to take the full exam again. Should candidate fail to pass the full exam, candidate will be temporarily barred from taking the exam.
- EC-Council has the right to ask for additional information pertaining to the experience and education background of the candidate on the grounds of verification.

**f. Revoking Certifications**

The infringement of any exam policies, rules, NDA, certification agreement or the involvement in misdemeanor that may harm the integrity and image of EC-Council certification program, may result in the candidate's temporary or permanent ban, at EC-Council's discretion, from taking any future EC-Council certification exams, revocation or decertification of current certifications. Such infringements include but are not limited to:

- The publication of any exam contents or parts with any person without a prior written approval from EC-Council.
- The recreation, imitation, or replication of any exam content through any means including memory recalling whether free or paid through any media including Web forums, instant messaging, study guides, etc.
- Harnessing any materials or devices not explicitly authorized by EC-Council during the exam.
- Taking out any materials that hold any exam contents outside the exam room, using for example, scratch paper, notebooks, etc.
- The impersonation of a candidate.



- Meddling with the exam equipment in an unauthorized way.
- Giving or being receptive of any assistance unauthorized by EC-Council.
- Acting in an uncivil, disturbing, mobbish, or unprofessional manner that may disregard or disrespect other candidates or exam officials during the exam.
- Communicating by whatever verbal or non-verbal means with other candidates in the exam room.
- Not adhering to EC-Council Exam Retake Policy and other candidate agreements.
- Not adhering to EC-Council Code of Ethics.
- Felony conviction in the court of law.

**g. Beta Exam**

- Sitting for a beta exam is only by invitation.
- Beta tests are focused on collecting data on the exam itself and are not focused on certifying you.

**h. Right of Exclusion**

EC-Council reserves the right of exclusion of any test centers, countries, or regions from EC-Council administering EC-Council certification exam/s.

# CCISO Credential Renewal

Your CCISO credential is valid for 3 years.

To renew your credential for another 3-year period you need to update your EC-Council Continuing Education (ECE) credit account in the EC-Council Aspen portal and submit proof of your earned credits. To maintain your certification you must earn a total of 120 credits within 3 years of ECE cycle period. An annual fee of \$100 is applicable.

The credits can be earned in many ways including attending conferences, writing research papers, preparing for training classes in a related domain (for instructors), reading materials on related subject matters, taking an exam of a newer version of the certification, attending webinars, and many others.

If you fail to meet the certification maintenance requirements within the 3-year time frame EC-Council will suspend your certification. Your certification will be suspended for a period of 1 year unless you earn the required 120 ECE credits to maintain/renew your certification.

If you fail to meet certification maintenance requirements during the suspension period your certification will be revoked. You will need to take and pass the certification exam again to earn the certification.

If you hold multiple EC-Council certifications, credits earned will be applied to all active certifications.

For full details regarding the ECE Policy please refer to the next section.





# EC-Council Continuing Education (ECE) Policy

## 1. REASONS FOR INTRODUCTION OF ECE SCHEME

All legitimate and credible certifications have a re-certification program. In fact, ANSI/ISO/IEC 17024, a quality accreditation body requires credible certification providers to have their own re-certification program. Requirement 6.5.1 states, "The certification body shall define recertification requirements according to the competence standard and other relevant documents, to ensure that the certified person continues to comply with the current certification requirements."

Continued competency can be demonstrated through many methodologies such as continuing professional education, examination (often not re-taking the original exam but an exam that would be at a higher level), or portfolios (when there is a product involved). The fact is there needs to be a time limit for the certification to ensure the consumers that the person has up-to-date knowledge.

This is why several governmental agencies are mandating accreditation of certifications in fields such as IT, Crane Operators, and Selling of Securities to the elderly.

Certification's main purpose is to "protect the public/consumers" NOT to protect the profession. When health, safety and security are at risk, certification is needed and it cannot be given for a "lifetime". It is generally noted that, if professionals are not required to maintain their knowledge and skills in their profession, they won't. Today, credible organizations within professional domains require their members to provide evidence of a continuous learning as a basis for maintaining their license.

### Differentiation

The ECE will brand, differentiate and distinguish a certified member as dedicated IT Security professional if he/she is willing to continuously learn and share knowledge to keep abreast of the latest changes in technology that affects the way security is viewed, deployed and managed. This is a key requirement of employers internationally and EC-Council being a major certification organization supports it.

## How does it work?

Once a candidate becomes certified by EC-Council, the relationship between EC-Council and candidate will always be governed by the EC-Council Candidate Certification Agreement which candidate must agree to prior from receiving your certification. This agreement is also provided at <https://cert.eccouncil.org/images/doc/EC-Council-Certification-Agreement-5.0.pdf>

If a certified member earned certification/s that are included under the ECE scheme, he/she will have to achieve a total of 120 credits (per certification) within a period of three years. If a member holds multiple certifications, credits earned will be applied across all the certifications. However, effective January 1st 2013, each certification will have its own ECE recertification requirements within its respective 3-year ECE window.

The credits can be earned in many ways including attending conferences, writing research papers, preparing for training classes in a related domain (for instructors), reading materials on related subject matters, taking an exam of a newer version of the certification, attending webinars, and many others. Qualified ECE activities must have been completed within ECE program's 3-year window and must be submitted in only one ECE 3-year window.

## 2. RECERTIFICATION

Effective January 1st, 2009, all EC-Council certifications will be valid for three years from the date of certification. During the three-year period, the certification must be renewed by participating in EC-Council Continuing Education (ECE) Program.

For members who were certified prior to 2009, their ECE period will be from January 1st 2009 until December 31st 2011. For their first ECE Scheme Period (2009-2011), they are only required to meet a total of 120 ECE credits By March 31st 2013.

Upon completion of the 3 year ECE program and meeting the requirements, the member's certification validity will be extended for another three years from the month of expiry.

EC-Council has introduced in 2017 its new American National Standards Institute (ANSI) accredited version of its CCISO certification program.

## 3. SUSPENSION, REVOCATION & APPEAL

### SUSPENSION

If the certified member fails to meet certification requirements within the 3-year time frame, EC-Council will suspend his/her certification.

Suspended members will not be allowed to use the certification logos and related EC-Council membership benefits.

Suspended members must remediate their suspension within a maximum period of 12 months from the date of the expiry of the 3 year time frame. Failing which, the member's certification and status will be revoked and the member will need to challenge and pass the certification exam again to achieve certification.

Suspended members that subsequently meet the 120 ECE credit requirements within the specified 12 months deadline from the date of the expiry of the 3 year time frame will be reinstated as a member in good standing and can enjoy the use of their certification logo and related EC-Council benefits. However, the reinstated member will have only a reduced period to achieve another 120 ECE credits for their next recertification window. "Reduced period" refers to a time frame of 3 years less the suspension period.

## **REVOCATIONS**

If member fails to meet certification requirements during the suspension period, he/she will have the certification revoked and will no longer be allowed to continue usage of the certification logo and related benefits. Members whose certification is revoked will be required to retake and pass the respective new exam to regain their certification.

## **APPEALS**

Members whose certification has been suspended or revoked due to non-compliance of certification requirements may send in an appeal in writing to EC-Council. This appeal letter must be received by EC-Council within ninety (90) days of the suspension/ revocation notice, providing details of the appeal and reason(s) for non-compliance.

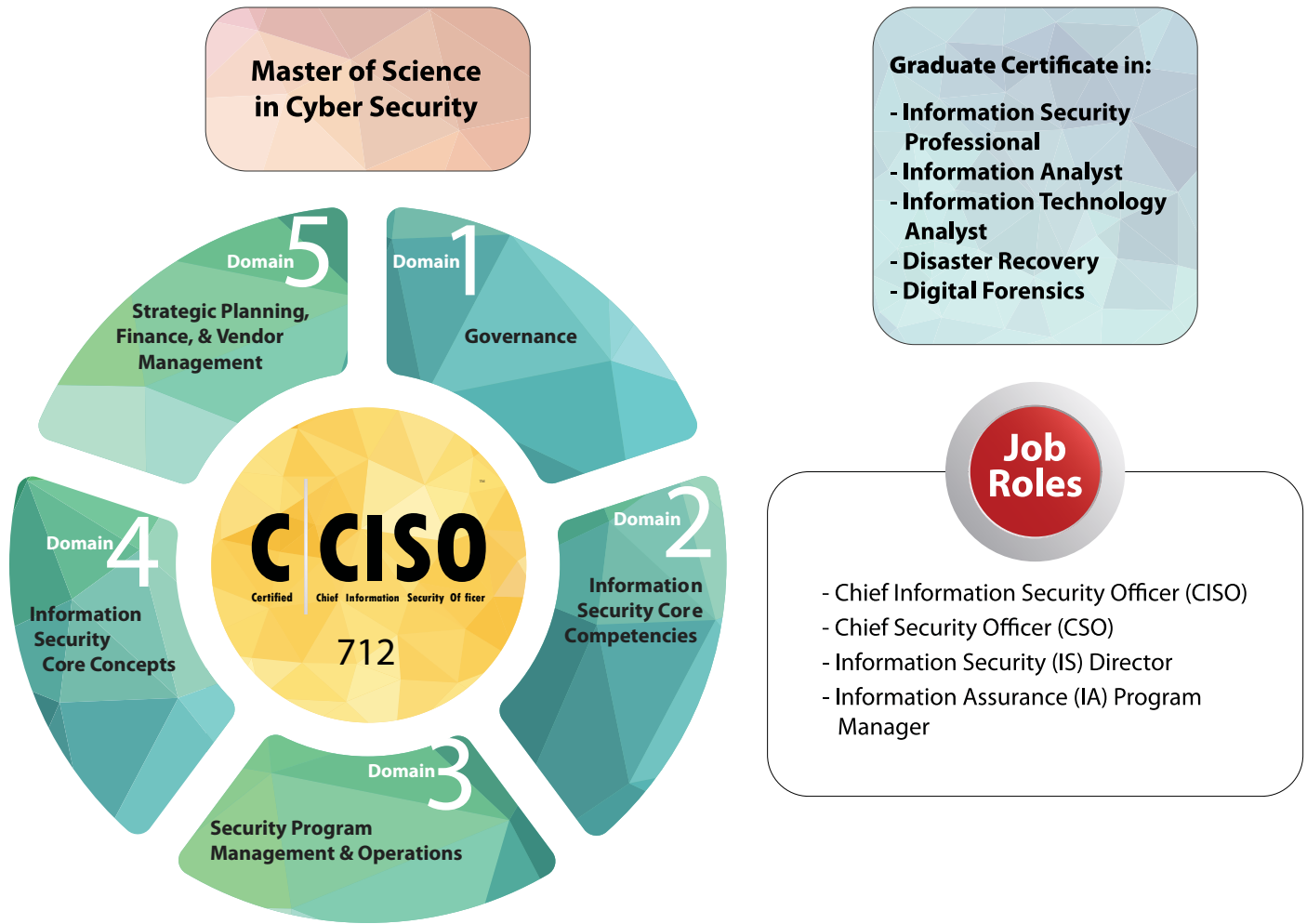
## **4. Audit Requirements**

Certified members are required to maintain sufficient evidence to show your involvement in activities that earns you ECE credits. There is no requirement to submit evidence until it is requested for specifically by EC-Council.

## **5. Important Notice**

Please note that the above is subject to change from time to time without prior notice. EC-Council reserves the right to make changes as required in order to maintain the reputation and recognition of its certifications and credentials. However, best effort will be used in informing members of changes via the website.

# C|CISO CAREER PATH



## This Track Maps to NICE's Specialty Areas:

1. Securely Provision (SP)
  - b. Risk Management (RM)
  - c. Technology R&D (RD)
  - d. Systems Requirements Planning (RP)
2. Oversee and Govern (OV)
  - a. Legal Advice and Advocacy (LG)
  - b. Training, Education, and Awareness (ED)
  - c. Cybersecurity Management (MG)
3. Collect and Operate (CO)
  - a. Cyber Operational Planning (PL)
- d. Strategic Planning and Policy (PL)
- e. Executive Cybersecurity Leadership (EX)
- f. Acquisition and Program/Project Management (PM)

# Code of Ethics

1. Keep private and confidential information gained in own professional work, (in particular if it pertains to your client lists and client's personal information). Not collect, give, sell, or transfer any personal information (such as name, e-mail address, Social Security number, or other unique identifier) to a third party without your client's prior consent.
2. Protect and respect the intellectual property of others by relying on your own innovation and efforts, thus ensuring that all benefits vest with its originator. Disclose and report to appropriate persons or authorities' potential dangers to any e-commerce clients, the Internet community, or the public, as applicable.
3. Provide service in own areas of competence. You should be honest and forthright about any limitations of own experience and education. Ensure that the Certified Member is qualified for any project by an appropriate combination of education, training, and experience.
4. Never knowingly use software or process that is obtained or retained either illegally or unethically.
5. Not to engage in deceptive financial practices such as bribery, double billing, or other improper financial practices. Use and protect the property of your clients or employers only in ways which are properly authorized, and with the owner's knowledge and consent.
6. Avoid any conflict of interest. Disclose to all concerned parties, including (without limitation) your clients, employers, EC-Council any actual or potential conflicts of interest that cannot reasonably be avoided or escaped. For the purpose of clarity, if you have participated in Item writing for any of the EC-Council certification examinations, you will not be allowed to sit for the same certification examination. Further, if you wish to be EC-Council's Consultant, you must disclose your association with EC-Council's other products and/or services and/or your association with competing products and/or services.
7. Ensure good management for any project as a Certified Member.
8. Add to the knowledge of the e-commerce profession by constant study, share the lessons of own experience with fellow EC-Council members, and promote public awareness of benefits of electronic commerce.
9. Conduct oneself in the most ethical and competent manner when soliciting professional service or seeking employment, thus meriting confidence in the Certified Member's knowledge and integrity.
10. Ensure ethical conduct and professional care at all times on all professional assignments without prejudice.
11. Not to associate with malicious hackers or engage in any malicious activities.
12. Not to purposefully compromise or allow the client's or organization's systems to be compromised in the course of the Certified Member's professional dealings. Ensure all penetration testing activities are authorized and within legal limits.
13. Not to take part in any black hat activity or be associated with any black hat community that serves to endanger networks.

14. Not to be part of any underground hacking community for purposes of preaching and expanding black hat activities.
15. Not to make inappropriate reference to the certification or misleading use of certificates, marks or logos in publications, catalogues, documents or speeches.
16. Not to be in violation of any law of the land or have any previous conviction.
17. Make claims regarding certification only with respect to the scope for which the certification has been granted.
18. Not to use the certification in a manner as to bring EC-Council into disrepute.
19. Not to make misleading and/or unauthorized statement regarding the certification or EC-Council.
20. Discontinue the use of all trademarks as regard to the certification which contains any reference to EC-Council and/or EC-Council trademark or logo or insignia upon suspension/withdrawal of the said certification.
21. Return any certificates issued by EC-Council upon suspension/withdrawal of the certification.
22. Refrain from further promoting the certification in the event of the said certification is withdrawn or suspended.
23. Inform EC-Council without any undue delay of any physical or mental condition which renders the Certified Member incapable to fulfill the continuing certification requirements.
24. Maintain the certification by completing, within the time frame specified by EC-Council, all continuing certification requirements (if any) that correspond with Certified member's particular certification.
25. To not to participate in any cheating incident, breach of security, misconduct or any other behavior that could be considered a compromise of the integrity or confidentiality of any EC-Council certification examination.

# ETHICS VIOLATIONS

EC-Council commitment towards ethics is the mainspring that holds all its programs, services, people and operations together. EC-Council regards ethics in earnest and from stem to stern. Corollary, EC-Council mandates and stipulates all its certified professionals, candidates, and prospective candidates to conduct themselves with the law, spirit of the law, and ethical practices that would reflect positively on clients, corporates, industries, and the society at large. The EC-Council Code of Ethics tops EC-Council mandatory standards and is a requisite and indeed a pillar of its strength.

EC-Council has an objective and fair process of evaluating cases of ethics violation. Any person/s may report an EC-Council certified professional by filling EC-Council Violation of Ethics Report form, describing clearly the facts and circumstance of the violation, and obtaining the confirmation of two verifiers who confirm that the report is true and correct. The Director of Certification has the authority to temporarily suspend a member that is suspected of violating EC-Council's Code of Ethics while the case is being brought before the EC-Council Scheme Committee.

The form will be submitted to EC-Council Scheme Committee for their review and resolution. The Committee will rule in light of substantial and sufficient evidence of ethics violation. Possible resolutions or penalties may include decertification, reprimand, warning, suspension of certification, publication of infraction and/or penalty, and lastly any possible litigation.

EC-Council will be formally notified of the Scheme Committee resolution in writing and with full details. EC-Council will notify the member/s, persons or parties concerned by email or registered mail of the Scheme Committee resolution. The Committee resolution is considered as final.

# EC-Council Ethics Violation Report Form

## Complaint lodged by:

Name :.....

Email Address :.....

Title/Company :.....

Country :.....

Phone :.....

EC-Council Cert ID :.....  
(if applicable)

## Complaint lodged against:

Name :.....

EC-Council Cert ID :.....  
(if applicable)

Section of EC-Council Code of Ethics Violated:

.....

.....

A detailed description of the facts known and circumstances relevant to the complaint:

.....

.....

.....

## Verified by

### Contact 1

Name :.....

Email Address :.....

Title/Company :.....

Country :.....

Phone :.....

**The information contained in this form is true  
and correct to the best of my knowledge.**

.....

Signature/Date

### Contact 2

Name :.....

Email Address :.....

Title/Company :.....

Country :.....

Phone :.....

**The information contained in this form is true  
and correct to the best of my knowledge.**

.....

Signature/Date



# Appeal Form v2



**EC-Council**





EC-Council adapts the term appeal as a reference to the mechanism by which a candidate/member can request the reconsideration of an EC-Council decision or exam. The appeal applicants should fill EC-Council Appeal Form and attach all supporting evidence. For instance, if the applicant is seeking EC-Council's decision in relation to the exam, for example its equipment, materials, content, scheduling, registration, or proctoring, he/should submit EC-Council Appeal Form, EC-Council Exam Feedback form and exam transcript.

The appeal will only be put forward to the adjudication of a subcommittee of the EC-Council Honorary Council, which will comprise of no less than 3 members; if the applicant is not satisfied with the Scheme Committee final decision. The request should be submitted to <https://eccouncil.zendesk.com/hc/en-us/requests/new> within thirty days from the date of the Scheme Committee written decision. Appeals received beyond the 30-days timeframe would not be reviewed.

### **The appeal process is comprised of three primary stages:**

#### **Stage 1: EC-Council**

EC-Council will inspect and scrutinize closely and thoroughly the candidate's appeal before providing a final decision. Technical issues like power outages, system crash, exam items will be forwarded to the testing companies (VUE or ECC) to advise whether there is valid grounds for appeal. EC-Council will provide the candidate with the appeal results within 30 days from receipt of candidate's appeal request.



## Stage 2: Scheme Committee

While EC-Council would exert every effort to resolve all matters in a fair and objective manner, EC-Council gives the applicant the right to appeal to EC-Council Scheme Committee Board if he/she is not satisfied with EC-Council's decision. The Scheme Committee will verify the intactness of all events and processes and provide EC-Council with its final decision, and EC-Council would communicate the decision to the candidate.

The Scheme Committee meets once every quarter. Only appeal requests received at least 30 days before the meeting will be reviewed at that session. Appeals received less than 30 days from the Scheme Committee meeting will be reviewed in the subsequent meeting.

## Stage 3: Honorary Council

The appeal will only be put forward to the adjudication of a subcommittee of the EC-Council Honorary Council, which will comprise of no less than 3 members; if the applicant is not satisfied with the Scheme Committee final decision. The request should be submitted at <https://eccouncil.zendesk.com/hc/en-us/requests/new> within thirty days from the date of the Scheme Committee written decision. Appeals received beyond the 30-days timeframe would not be reviewed.

The Honorary Council meets once every year. Only requests received at least 30 days prior to the Honorary Council meeting will be reviewed at that session. Appeals received less than 30 days from the Honorary Council meeting will be reviewed in the subsequent meeting. The decision concluded by the Honorary Council is irrefutable and is obligatory to all parties involved in the appeal.

# EC-Council Appeal Form

If the appeal is related to an EC-Council exam, the appeal request must be submitted to [certmanager@eccouncil.org](mailto:certmanager@eccouncil.org) within seven (7) calendar days from exam date. All other appeals must be submitted to [certmanager@eccouncil.org](mailto:certmanager@eccouncil.org) within sixty (60) calendar days from EC-Council's written decision. Appeals received beyond the above-mentioned timeframe would not be reviewed.

Kindly submit your appeal form to [certmanager@eccouncil.org](mailto:certmanager@eccouncil.org)

## SECTION A

Name Details : .....  
(Name given when enrolled)

Address : .....  
(including city, state, and postal code)

Phone Number : .....

Email Address : .....  
.....  
.....

Are you a certified EC-Council member? If yes, please complete section B with one of your certification details.

## SECTION B

EC-Council Cert ID : ..... Cert Award Date : .....

Title of Certification : ..... Cert Expiry Date : .....

Are you appealing against an EC-Council Exam? If yes, please complete Section C. If no, kindly proceed to Section D.

## SECTION C

Test Centre Name : ..... Exam Title : .....

Test Centre Location : ..... Exam Version : .....

EC-Council Proctor : ..... Date Tested : .....  
Name (if known)

Exam Voucher No. : .....

# EC-Council Appeal Form

## SECTION D

Details of your appeal

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....  
Candidate's Signature

\*Please attach a copy of score transcript/certificate, exam item or any other documents that may support your appeal.

## Change in Certification Scope

EC-Council shall, where applicable, give due notice to interested parties and certified members on changes in scope of certifications, rationale behind change, and effective dates of change. Such changes will be published on the EC-Council Certification website (<https://cert.eccouncil.org>).

EC-Council shall verify that each certified member complies with the changed requirements within such a period of time as is seen as reasonable for EC-Council. For instance, old versions of certification exams are retired six months from the date of official announcement of the launch of the new version of the exam. These changes will only be done after taking into consideration EC-Council Scheme Committee views.

EC-Council's Scheme Committee is a member based network of volunteers that are recognized by EC-Council as experts in the field of information security. They are carefully selected from the industry and are committed to the information security community. More importantly, they remain an independent voice for the industry and are responsible to advise EC-Council in the development and the maintenance of key certification-related matters.

Changes may be suggested by any stakeholder of EC-Council, but changes will be verified with documented psychometric analysis conducted by experts. Psychometric analysis would be conducted to determine the certification scope every three years or sooner; whereas evaluation would be conducted every year to ensure if amendment in scope of certification is required.



**EC-Council**



**EC-Council**  
**Logo Usage**

# EC-Council Logo Usage Guidelines

To use any of EC-Council's logos, candidate must be an EC-Council Certified Professional, EC-Council Test Center, EC-Council Accredited Training Center, or a Licensed Penetration Tester. A list of certifications can be found at <https://cert.eccouncil.org/certifications.html>

In this context, logo shall mean and include all logos provided by EC-Council. The logo is a trademark of EC-Council.

## 1. GENERAL

- a. Certified Member can only to use the logo in its original form as provided by EC-Council.
- b. Certified Member must state the certification version number next to the logo such as v1. Certified Member may not alter, change or remove elements of the logo in any other way.
- c. "Only ANSI accredited certifications carry the ANSI logo", the Certified Chief Information Security Officer – ANSI accredited version does not carry a version number.
- d. Certified Member may not alter, change or remove elements of the logo in any other way.
- e. Certified Member may not translate any part of the logo.
- f. Certified Member may not use elements of the logo to be part of the design of other materials or incorporate other designs into the logo.
- g. Certified Member may not incorporate the logo or parts of the logo into Certified Member company name, company logo, website domain, trademark, product name and design, or slogan.
- h. Certified Member may not use the logo to show any form of endorsement by EC-Council.

## 2. INDIVIDUALS

- a. Certified Member may use the logo on his/her business cards, business letters, resume, Websites, emails, and marketing materials for individual service.
- b. Certified Member may only use the logo of the credential he/she is awarded.
- c. Certified Member may not use the logo if certification has been revoked or suspended
- d. Certified Member may not use the logo if certification term has expired/lapsed and not renewed.
- e. Certified Member may not display the logo to be larger or more prominent than candidate's name or company name and logo.
- f. Candidates who hold EC-Council 'Retired Status' may not use the logo unless the logo is used with the word 'retired'.
- g. Candidate may not use the logo if he/she is not certified.
- h. Candidate may not use the logo if he/she is still in the midst of a program and have not passed the certification exam.
- i. Candidate may not use the logo to show affiliation with EC-Council in any way.

## 3. EC-Council Test Centers (ETCs) and EC-Council Accredited Training Partners (ATPs)

- a. ETCs and ATP's may use the logo on their marketing materials related to EC-Council programs and certifications. ETCs and ATP's may not use the logo on any material not related to EC-Council certifications or programs.
- b. ETCs may not use the logo to signify any relationship or affiliation with EC-Council other than as an ETC.
- c. ATPs may not use the logo to signify any relationship or affiliation with EC-Council other than as an ATP.



# EC-Council Logo Usage Guidelines

## 4. COMPLIANCE

- a. EC-Council may occasionally conduct surveillance audits for materials bearing the logos. Candidates are to abide by the guidelines stated above. Certified Member may be subject to sanction if he/she does not adhere to these guidelines and may have his/her certification credential suspended or revoked.
- b. Certified Member must immediately cease to display, advertise or use the logo upon the suspension or revocation of certification credential.

## 5. LOGO DETAILS

### a) Color

#### Full Color

The colors used for the logos are red, yellow, black and white. The color codes are:

#### Color- Red

RGB R: 255, G: 0, B: 0

#### Color- Yellow

RGB R: 255, G: 255, B: 0

#### Black and White

The logo can also be printed in black and white due to budget restrictions. For this, the color for the wordings and background of the logo must always be reversed. That is, the wordings are in black and the background is white or the wordings are in white and the background is black.



### b) Size

The logo can be of any size but it must maintain all the elements of the logo without any distortions. All elements of the logo must remain legible.



# EC-Council Logo Usage Guidelines

## c) Spacing

The logo must not be overlapped and be fully prominent. There must be sufficient space between the logo and any other text or object. We recommend a minimum spacing of 0.3 centimeters.



## d) Elements

All elements must remain in its original form. All elements of the logo must not be distorted or altered. Certified Member must ensure that the aspect ratio is maintained at all times.



## e) Orientation

The logo must be presented in its upright form and not be displayed at other angles other than its horizontal layout.



## f) Multiple Credentials

Individuals who attain multiple EC-Council certification credentials may display any of the logos for which certification has been achieved. Certified Member may not however, create a logo which displays a combination of all the credentials achieved. All logos must stand alone in its own right.



# EC-Council Logo Usage Guidelines

## 6. USAGE EXAMPLES

These are examples on the usage of the logo. The usage guidelines must be strictly adhered to

- a. **Business Cards:** We recommend displaying the logo on the lower left or lower right hand side of Certified Member business card.
- a. **Business Letters:** We recommend displaying the logo on the lower left or lower right hand side of the letterhead page of Certified Member business letter.
- a. **Resume:** We recommend displaying the logo on the lower left or lower right hand side of Certified Member resume.
- a. **Website:** We recommend displaying the logo at an appropriate location on Certified Member website.
- a. **Email:** We recommend displaying the logo at the bottom of Certified Member email signature.
- a. **Marketing Materials:** We recommend displaying the logo at an appropriate but prominent place in Certified Member marketing materials.

# FREQUENTLY ASKED QUESTIONS

## What is the CCISO program?

The Certified Chief Information Security Officer program 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.

---

## How do I apply for the CCISO exam?

In order to qualify to take the CCISO Exam, applicants must fill out the CCISO Exam Eligibility Application found **here**. Applications should be emailed to [cciso@eccouncil.org](mailto:cciso@eccouncil.org). If the applicant is attempting the exam without taking EC-Council Authorized Training, five years of experience in each of the five CCISO Domains is required (experience can be overlapping) and a \$100 application fee is due with the application. If an applicant has purchased EC-Council Authorized Training, there is no application fee due and only five years of experience in three of the five domains is required. For more information, please see <http://ciso.eccouncil.org/cciso-certification/>

---

## How long does it take to process the CCISO Exam Eligibility Application?

Application processing time varies due to the fact that part of the process involves reaching out to verifiers indicated by the applicants as able to verify their experience. In order to speed up this process, applicants can assist the application processing team by reaching out to their verifiers to ensure they have received the required forms from EC-Council and understand what is required. Applications from students in EC-Council Authorized Training are prioritized and expedited in order to ensure testing can occur at the time of the class if the student desires.

---

## Is the \$100 application fee refundable?

No, the \$100 application fee is not refundable.

---

## What are the five CCISO Domains?

The five CCISO Domains are:

Domain 1 : Governance (Policy, Legal & Compliance)

Domain 2 : IS Management Controls and Auditing Management (Projects, Technology & Operations)

Domain 3 : Management – Projects and Operations

Domain 4 : Information Security Core Competencies

Domain 5 : Strategic Planning and Finance

**Five years of experience is required in each of the five CCISO Domains (self-study). Does that mean 25 years of experience is required?**

No! In most high-level information security management jobs, each of the 5 CCISO Domains is part of each day. The five years can and usually do overlap.

---

**What if I don't have five years of experience in three of the five CCISO domains? Does that mean I can't take the CCISO training?**

No! If you do not meet the minimum requirements for the CCISO Exam, that doesn't mean you can't take training. Anyone can take the CCISO course, but only those who qualify to take the CCISO Exam will be issued an exam voucher. Students who do not have the years required can take the EC-Council Information Security Manager (EISM) exam after CCISO training.

---

**What is the EC-Council Information Security Manager (EISM) program?**

The EISM program allows students who are not yet qualified to sit for the CCISO exam to take the training course and attain an EC-Council certification. EISMs may apply for the CCISO Exam once they have acquired the years of experience. The eligibility application fee is waived and EISMs will receive a 50% discount from the normal CCISO Exam price.

---

**What is the EC-Council Information Security Manager (EISM) program?**

The EISM program allows students who are not yet qualified to sit for the CCISO exam to take the training course and attain an EC-Council certification. EISMs may apply for the CCISO Exam once they have acquired the years of experience. The eligibility application fee is waived and EISMs will receive a 50% discount from the normal CCISO Exam price.

---

**What are the EC-Council Authorized Training options?**

CCISO training is available at:

In-person training is available at EC-Council events ([www.hackerhalted.com](http://www.hackerhalted.com) and [www.takedowncon.com](http://www.takedowncon.com)) and others listed under the training section of this page: <https://ciso.eccouncil.org/cciso-certification/>

Online via our iClass program. Options for self-paced and live online are available. [Click here for more information!](#)

In-person training via our Accredited Training Center network! Fill out the form found here to find a training center in your area: <https://www.eccouncil.org/Training>

---

**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

### **I am an HR manager. Why should I hire a C|CISO?**

C|CISO will give you assurance that the certified professional possesses the necessary skills to identify factors that pose risk to the successful operation of your organization and develop and implement technical, operational, and procedural safeguards to manage those risk factors. C|CISOs are the leadership force that will protect your organization from unwanted and costly security breaches by designing information security programs and leading a team of information security professionals.

---

### **For how long is the exam voucher code valid for?**

The exam voucher code is valid for 1 year from the date of receipt.

---

### **How long is the CCISO certification valid?**

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

---

### **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).

---

### **I have more questions.**

We would love to help! Contact us at [cciso@eccouncil.org](mailto:cciso@eccouncil.org) or +1-505-341-3228 for answers!

---

### **Are there any annual fees payable?**

Effective January 1st, 2016. Any member certified or recertified requires to pay an annual membership of USD100 if he/she holds a minimum of one certificate under the ECE policy and USD20 if he/she holds certificates that are not under the ECE policy.

More details about the membership fee, cycle and due date can be found at <https://cert.eccouncil.org/membership.html>

---

### **How do I register my ECE credit?**

Please log on to the Aspen Portal (<https://aspen.eccouncil.org>) to register your ECE credits.

---

### **How do I register my ECE credit?**

Please log on to the Aspen Portal (<https://aspen.eccouncil.org>) to register your ECE credits.

### **ECE Qualifying Activities**

Only IT security related events are qualified for ECE scheme such as IT seminars, reading IT security books, publishing a paper on IT Security related topics and anything that updates your knowledge on IT Security not only from EC-Council.

## ECE Qualifying Events

- Volunteering in public sector - 1 credit per hour
- Association/Organization Chapter Meeting (per Meeting) - 1 credit per hour
- Author Article/Book Chapter/White Paper - 20 credits
- Authoring Course/Module - 40 credits
- Author Tool - 40 credits
- Authoring Book - 100 credits
- Contribution to the exam development: 40 credits - 100 credits
- Certification/ Examination - 40 credits
- EC-Council Examination (ECE) - 120 credits
- EC-Council Survey - 20 credits
- Education Course - 1 credit per hour
- Education Seminar/Conference/Event - 1 credit per hour
- Higher Education - 15 credits per semester hour
- Identify New Vulnerability - 10 credits
- Presentation - 3 credits per hour
- Reading an Information Security Book/Article Review/Book Review/Case Study - 5 credits
- Teach New - 21 credits per day
- Teach Upgrade - 11 credits per day
- Review Board - 80 credits

---

### What certifications from EC-Council are included in the ECE system?

EC-Council Examinations (CEH, CEH (Practical), ECSA, ECSA (Practical), LPT, LPT (Master), CHFI, EISM, CCISO, CND, ECIH, EDRP, CASE, CSA, CBP, CPM, CTIA, ECES, ECSS, CEI, CAST, CIMP and CDM) : 120 credits.

---

### Can a member holding any of the abovementioned certification be exempted from the ECE scheme?

No.

---

### Who can I speak to if I need more help?

If the particular event or activity is not listed on the Aspen portal, you can contact the Administrator at [delta@eccouncil.org](mailto:delta@eccouncil.org) for assistance.

---

### Can I use the certification name and logo after I pass my exams?

Yes, you can use the respective logos and labels of the certifications that you hold.

---

### Where do I go to download the logos and guidelines?

You can download logos and usage guidelines from  
<https://cert.eccouncil.org/images/doc/ec-council-logo-usage-v3.0.pdf>



# CCISO

Blueprint v1





Domains	Objectives	Weightage	Number of Questions
1. <b>Governance (Policy, Legal &amp; Compliance)</b>	<ul style="list-style-type: none"> <li>Define, implement, manage and maintain an information security governance program that includes leadership, organizational structures and processes.</li> <li>Align information security governance framework with organizational goals and governance, i.e., leadership style, philosophy, values, standards and policies.</li> <li>Establish information security management structure.</li> <li>Establish a framework for information security governance monitoring (considering cost/benefits analyses of controls and ROI).</li> <li>Understand standards, procedures, directives, policies, regulations, and legal issues that affect the information security program.</li> <li>Understand the enterprise information security compliance program and manage the compliance team.</li> <li>Analyze all the external laws, regulations, standards, and best practices applicable to the organization.</li> <li>Understand the various provisions of the laws that affect the organizational security such as Gramm-Leach-Bliley Act, Family Educational Rights and Privacy Act, Health Insurance Portability and Accountability Act [HIPAA], Federal Information Security Management Act [FISMA], Clinger-Cohen Act, Privacy Act, Sarbanes-Oxley, etc.</li> </ul>	16%	24

	<ul style="list-style-type: none"> <li>• Be familiar with the different standards such as ISO 27000 series, Federal Information Processing Standards [FIPS]</li> <li>• Understand the federal and organization specific published documents to manage operations in a computing environment</li> <li>• Assess the major enterprise risk factors for compliance</li> <li>• Coordinate the application of information security strategies, plans, policies, and procedures to reduce regulatory risk</li> <li>• Understand the importance of regulatory information security organizations and appropriate industry groups, forums, and stakeholders</li> <li>• Understand the information security changes, trends, and best practices</li> <li>• Manage enterprise compliance program controls</li> <li>• Understand the information security compliance process and procedures</li> <li>• Compile, analyze, and report compliance programs</li> <li>• Understand the compliance auditing and certification programs</li> <li>• Follow organizational ethics</li> </ul>		
<b>2. IS Management Controls and Auditing Management (Projects, Technology &amp; Operations)</b>	<ul style="list-style-type: none"> <li>• Information Security Management Controls               <ul style="list-style-type: none"> <li>• Identify the organization's operational process and objectives as well as risk tolerance level</li> </ul> </li> </ul>	18%	29

	<ul style="list-style-type: none"> <li>• Design information systems controls in alignment with the operational needs and goals and conduct testing prior to implementation to ensure effectiveness and efficiency</li> <li>• Identify and select the resources required to effectively implement and maintain information systems controls. Such resources can include human capital, information, infrastructure, and architecture (e.g., platforms, operating systems, networks, databases, applications)</li> <li>• Identify and select the resources required to effectively implement and maintain information systems controls. Such resources can include human capital, information, infrastructure, and architecture (e.g., platforms, operating systems, networks, databases, applications)</li> <li>• Design and implement information systems controls to mitigate risk. Monitor and document the information systems control performance in meeting organizational objectives by identifying and measuring metrics and key performance indicators</li> <li>• Design and conduct testing of information security controls to ensure effectiveness, discover deficiencies and ensure alignment with organization's policies, standards and procedures</li> <li>• Design and implement processes to appropriately remediate deficiencies and evaluate problem</li> </ul>		
--	--	--	--

	<ul style="list-style-type: none"> <li>• management practices to ensure that errors are recorded, analyzed and resolved in a timely manner</li> <li>• Assess and implement tools and techniques to automate information systems control processes.</li> <li>• Produce information systems control status reports to ensure that the processes for information systems operations, maintenance and support meet the organization's strategies and objectives, and share with relevant stakeholders to support executive decision-making</li> <li>• Auditing Management <ul style="list-style-type: none"> <li>• Understand the IT audit process and be familiar with IT audit standards</li> <li>• Apply information systems audit principles, skills and techniques in reviewing and testing information systems technology and applications to design and implement a thorough risk-based IT audit strategy</li> <li>• Execute the audit process in accordance with established standards and interpret results against defined criteria to ensure that the information systems are protected, controlled and effective in supporting organization's objectives</li> <li>• Effectively evaluate audit results, weighing the relevancy, accuracy, and perspective of conclusions against the accumulated audit evidence</li> </ul> </li> </ul>		
--	--	--	--

	<ul style="list-style-type: none"> <li>• Assess the exposures resulting from ineffective or missing control practices and formulate a practical and cost-effective plan to improve those areas</li> <li>• Develop an IT audit documentation process and share reports with relevant stakeholders as the basis for decision-making</li> <li>• Ensure that the necessary changes based on the audit findings are effectively implemented in a timely manner</li> </ul>		
<b>3. Management - Projects and Operations</b>	<ul style="list-style-type: none"> <li>• For each information systems project develop a clear project scope statement in alignment with organizational objectives</li> <li>• Define activities needed to successfully execute the information systems program, estimate activity duration, and develop a schedule and staffing plan</li> <li>• Develop, manage and monitor the information systems program budget, estimate and control costs of individual projects</li> <li>• Identify, negotiate, acquire and manage the resources needed for successful design and implementation of the information systems program (e.g., people, infrastructure, and architecture)</li> <li>• Acquire, develop and manage information security project team</li> <li>• Assign clear information security personnel job functions and provide continuous training to ensure effective performance and accountability</li> </ul>	22%	34

	<ul style="list-style-type: none"> <li>• Direct information security personnel and establish communications, and team activities, between the information systems team and other security-related personnel (e.g., technical support, incident management, security engineering)</li> <li>• Resolve personnel and teamwork issues within time, cost, and quality constraints</li> <li>• Identify, negotiate and manage vendor agreement and community</li> <li>• Participate with vendors and stakeholders to review/assess recommended solutions; identify incompatibilities, challenges, or issues with proposed solutions</li> <li>• Evaluate the project management practices and controls to determine whether business requirements are achieved in a cost-effective manner while managing risks to the organization</li> <li>• Develop a plan to continuously measure the effectiveness of the information systems projects to ensure optimal system performance</li> <li>• Identify stakeholders, manage stakeholders' expectations and communicate effectively to report progress and performance</li> <li>• Ensure that necessary changes and improvements to the information systems processes are implemented as required</li> </ul>		
--	--	--	--

<b>4. Information Security Core Competencies</b>	<ul style="list-style-type: none"> <li>• Access Control <ul style="list-style-type: none"> <li>• Identify the criteria for mandatory and discretionary access control, understand the different factors that help in implementation of access controls and design an access control plan</li> <li>• Implement and manage an access control plan in alignment with the basic principles that govern the access control systems such as need-to-know</li> <li>• Identify different access control systems such as ID cards and biometrics</li> <li>• Understand the importance of warning banners for implementing access rules</li> <li>• Develop procedures to ensure system users are aware of their IA responsibilities before granting access to the information systems</li> </ul> </li> <li>• Social Engineering, Phishing Attacks, Identity Theft <ul style="list-style-type: none"> <li>• Understand various social engineering concepts and their role in insider attacks and develop best practices to counter social engineering attacks</li> <li>• Design a response plan to identity theft incidences</li> <li>• Identify and design a plan to overcome phishing attacks</li> </ul> </li> <li>• Physical Security <ul style="list-style-type: none"> <li>• Identify standards, procedures, directives, policies, regulations and laws for physical security</li> <li>• Determine the value of physical assets and the impact if unavailable</li> </ul> </li> </ul>	25%	37
--	--	-----	----

	<ul style="list-style-type: none"> <li>• Identify resources needed to effectively implement a physical security plan</li> <li>• Design, implement and manage a coherent, coordinated, and holistic physical security plan to ensure overall organizational security</li> <li>• Establish objectives for personnel security to ensure alignment with overall security goals for the enterprise</li> <li>• Design and manage the physical security audit and update issues</li> <li>• Establish a physical security performance measurement system</li> <li>• Risk Management <ul style="list-style-type: none"> <li>• Identify the risk mitigation and risk treatment processes and understand the concept of acceptable risk</li> <li>• Identify resource requirements for risk management plan implementation</li> <li>• Design a systematic and structured risk assessment process and establish, in coordination with stakeholders, an IT security risk management program based on standards and procedures and ensure alignment with organizational goals and objectives</li> <li>• Develop, coordinate and manage risk management teams</li> </ul> </li> </ul>		
--	--	--	--



	<ul style="list-style-type: none"> <li>• Establish relationships between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies, vendors, and public relations professionals)</li> <li>• Develop an incident management measurement program and manage the risk management tools and techniques</li> <li>• Understand the residual risk in the information infrastructure</li> <li>• Assess threats and vulnerabilities to identify security risks, and regularly update applicable security controls</li> <li>• Identify changes to risk management policies and processes and ensure the risk management program remains current with the emerging risk and threat environment and in alignment with the organizational goals and objectives</li> <li>• Determine if security controls and processes are adequately integrated into the investment planning process based on IT portfolio and security reporting</li> <li>• Disaster Recovery and Business Continuity Planning <ul style="list-style-type: none"> <li>• Develop, implement and monitor business continuity plans in case of disruptive events and ensure alignment with organizational goals and objectives</li> </ul> </li> </ul>		

	<ul style="list-style-type: none"> <li>• Define the scope of the enterprise continuity of operations program to address business continuity, business recovery, contingency planning, and disaster recovery/related activities</li> <li>• Identify the resources and roles of different stakeholders in business continuity programs</li> <li>• Identify and prioritize critical business functions and consequently design emergency delegations of authority, orders of succession for key positions, the enterprise continuity of operations organizational structure and staffing model</li> <li>• Direct contingency planning, operations, and programs to manage risk</li> <li>• Understand the importance of lessons learned from test, training and exercise, and crisis events</li> <li>• Design documentation process as part of the continuity of operations program</li> <li>• Design and execute a testing and updating plan for the continuity of operations program</li> <li>• Understand the importance of integration of IA requirements into the Continuity of Operations Plan (COOP).</li> <li>• Identify the measures to increase the level of emergency preparedness such as backup and recovery solutions and design standard operating procedures for implementation during disasters</li> </ul>		
--	---	--	--

	<ul style="list-style-type: none"> <li>• Firewall, IDS/IPS and Network Defense Systems <ul style="list-style-type: none"> <li>• Identify the appropriate intrusion detection and prevention systems for organizational information security</li> <li>• Design and develop a program to monitor firewalls and identify firewall configuration issues</li> <li>• Understand perimeter defense systems such as grid sensors and access control lists on routers, firewalls, and other network devices</li> <li>• Identify the basic network architecture, models, protocols and components such as routers and hubs that play a role in network security</li> <li>• Understand the concept of network segmentation</li> <li>• Manage DMZs, VPN and telecommunication technologies such as PBX and VoIP</li> <li>• Identify network vulnerabilities and explore network security controls such as use of SSL and TLS for transmission security</li> <li>• Support, monitor, test, and troubleshoot issues with hardware and software</li> <li>• Manage accounts, network rights, and access to systems and equipment</li> </ul> </li> <li>• Wireless Security <ul style="list-style-type: none"> <li>• Identify vulnerability and attacks associated with wireless networks and manage different wireless network security tools</li> </ul> </li> </ul>		
--	---	--	--

	<ul style="list-style-type: none"> <li>• Virus, Trojans and Malware Threats <ul style="list-style-type: none"> <li>• Assess the threat of virus, Trojan and malware to organizational security and identify sources and mediums of malware infection</li> <li>• Deploy and manage anti-virus systems</li> <li>• Develop process to counter virus, Trojan, and malware threats</li> </ul> </li> <li>• Secure Coding Best Practices and Securing Web Applications <ul style="list-style-type: none"> <li>• Develop and maintain software assurance programs in alignment with the secure coding principles and each phase of System Development Life Cycle (SDLC)</li> <li>• Understand various system-engineering practices</li> <li>• Configure and run tools that help in developing secure programs</li> <li>• Understand the software vulnerability analysis techniques</li> <li>• Install and operate the IT systems in a test configuration manner that does not alter the program code or compromise security safeguards</li> <li>• Identify web application vulnerabilities and attacks and web application security tools to counter attacks</li> </ul> </li> </ul>		
--	---	--	--

	<ul style="list-style-type: none"> <li>• Hardening OS <ul style="list-style-type: none"> <li>• Identify various OS vulnerabilities and attacks and develop a plan for hardening OS systems</li> <li>• Understand system logs, patch management process and configuration management for information system security</li> </ul> </li> <li>• Encryption Technologies <ul style="list-style-type: none"> <li>• Understand the concept of encryption and decryption, digital certificates, public key infrastructure and the key differences between cryptography and steganography</li> <li>• Identify the different components of a cryptosystem</li> <li>• Develop a plan for information security encryption techniques</li> </ul> </li> <li>• Vulnerability Assessment And Penetration Testing <ul style="list-style-type: none"> <li>• Design, develop and implement a penetration testing program based on penetration testing methodology to ensure organizational security</li> <li>• Identify different vulnerabilities associated with information systems and legal issues involved in penetration testing</li> <li>• Develop pre and post testing procedures</li> <li>• Develop a plan for pen test reporting and implementation of technical vulnerability corrections</li> <li>• Develop vulnerability management systems</li> </ul> </li> </ul>		
--	---	--	--

	<ul style="list-style-type: none"> <li>• Computer Forensics and Incident Response           <ul style="list-style-type: none"> <li>• Develop a plan to identify a potential security violation and take appropriate action to report the incident</li> <li>• Comply with system termination procedures and incident reporting requirements related to potential security incidents or actual breaches</li> <li>• Assess potential security violations to determine if the network security policies have been breached, assess the impact, and preserve evidence</li> <li>• Diagnose and resolve IA problems in response to reported incidents</li> <li>• Design incident response procedures</li> <li>• Develop guidelines to determine whether a security incident is indicative of a violation of law that requires specific legal action</li> <li>• Identify the volatile and persistent system information</li> <li>• Set up and manage forensic labs and programs</li> <li>• Understand various digital media devices, e-discovery principles and practices and different file systems</li> <li>• Develop and manage an organizational digital forensic program</li> <li>• Establish, develop and manage forensic investigation teams</li> </ul> </li> </ul>		
--	--	--	--



	<ul style="list-style-type: none"> <li>• Design investigation processes such as evidence collection, imaging, data acquisition, and analysis</li> <li>• Identify the best practices to acquire, store and process digital evidence</li> <li>• Configure and use various forensic investigation tools</li> <li>• Design anti-forensic techniques</li> </ul>		
<b>5. Strategic Planning and Finance</b>	<ul style="list-style-type: none"> <li>• Strategic Planning <ul style="list-style-type: none"> <li>• Design, develop and maintain enterprise information security architecture (EISA) by aligning business processes, IT software and hardware, local and wide area networks, people, operations, and projects with the organization's overall security strategy</li> <li>• Perform external analysis of the organization (e.g., analysis of customers, competitors, markets and industry environment) and internal analysis (risk management, organizational capabilities, performance measurement etc.) and utilize them to align information security program with organization's objectives</li> <li>• Identify and consult with key stakeholders to ensure understanding of organization's objectives</li> <li>• Define a forward-looking, visionary and innovative strategic plan for the role of the information security program with clear goals, objectives and targets that support the operational needs of the organization</li> </ul> </li> </ul>	19%	26

	<ul style="list-style-type: none"> <li>• Define key performance indicators and measure effectiveness on continuous basis</li> <li>• Assess and adjust IT investments to ensure they are on track to support organization's strategic objectives</li> <li>• Monitor and update activities to ensure accountability and progress</li> <li>• Finance <ul style="list-style-type: none"> <li>• Analyze, forecast and develop the operational budget of the IT department</li> <li>• Acquire and manage the necessary resources for implementation and management of information security plan</li> <li>• Allocate financial resources to projects, processes and units within information security program</li> <li>• Monitor and oversee cost management of information security projects, return on investment (ROI) of key purchases related to IT infrastructure and security and ensure alignment with the strategic plan</li> <li>• Identify and report financial metrics to stakeholders</li> <li>• Balance the IT security investment portfolio based on EISA considerations and enterprise security priorities</li> <li>• Understand the acquisition life cycle and determine the importance of procurement by performing Business Impact Analysis</li> <li>• Identify different procurement</li> </ul> </li> </ul>		
--	--	--	--

	<ul style="list-style-type: none"> <li>• strategies and understand the importance of cost-benefit analysis during procurement of an information system</li> <li>• Understand the basic procurement concepts such as Statement of Objectives (SOO), Statement of Work (SOW), and Total Cost of Ownership (TCO)</li> <li>• Collaborate with various stakeholders (which may include internal client, lawyers, IT security professionals, privacy professionals, security engineers, suppliers, and others) on the procurement of IT security products and services</li> <li>• Ensure the inclusion of risk-based IT security requirements in acquisition plans, cost estimates, statements of work, contracts, and evaluation factors for award, service level agreements, and other pertinent procurement documents</li> <li>• Design vendor selection process and management policy</li> <li>• Develop contract administration policies that direct the evaluation and acceptance of delivered IT security products and services under a contract, as well as the security evaluation of IT and software being procured</li> <li>• Develop measures and reporting standards to measure and report on key objectives in procurements aligned with IT security policies and procedures</li> <li>• Understand the IA security requirements to be included in statements of work and other appropriate procurement documents</li> </ul>		
--	---	--	--



# AGREEMENTS

## Appendix B





# **NON-DISCLOSURE AGREEMENT**

**EC-Council**



# EC-Council NON-DISCLOSURE AGREEMENT

EC-Council and/or its Affiliate ("Disclosing Party") intends to make available or have made available to you ("Receiving Party" or "You") certain proprietary and confidential information including but not limited to exam items, materials, any notes or calculations, questions, exam methodologies, exam content and/or exam standards (together referred to as "Exam Materials") in connection with EC-Council certification ("Purpose"), in accordance with the terms of this Confidentiality and Non-Disclosure Agreement ("Agreement"). Disclosing Party either on its own or via its appointed representative spends substantial sums of time and money in developing and administering its Exam Materials which are the Intellectual Property of EC-Council. Such information related to Exam Materials so provided to You whether provided before or after the date hereof and whether written or oral, together with all manuals, documents, memoranda, notes, analyses, forecasts and other materials are strictly confidential and prohibited to be produced in any form whether written or oral, in any medium whether now known or to be developed later, in English or in any language, whatsoever, which contain or reflect, or are generated from, such Exam Material shall be collectively referred to herein as the "Confidential Information." For the purpose of clarity, "Affiliate" shall mean with respect to EC-Council at a given time, any entity whether incorporated or not, which is either controlled by or under common control with, or controls, the other entity, either directly or indirectly.

The Receiving Party now agrees as set forth below.

You shall hold Disclosing Party's Confidential Information in strict confidence and shall not disclose such Confidential Information to any third party or use it for any purpose other than to further the Purpose. You further agree not to create or engage in activities, either alone or jointly with others for the purpose of publishing any brain dump and/or any other unauthorized material that contains Exam Materials and any portion of the Confidential Information without the prior written consent of Disclosing Party. Further, You shall not copy or attempt to make copies (written, photocopied, or otherwise) of any Exam Material, including, without limitation, any exam questions or answers.

The Exam Materials including any questions and answers of the Exam are the exclusive and confidential property of the Disclosing Party and are protected by Disclosing Party's intellectual property rights, including but not limited to all patent, copyright, trademark, design and other proprietary rights and interests therein. You acknowledge and agree that nothing contained in this Agreement shall be construed as (i) granting any rights or license (either expressly or impliedly) in or to any Confidential Information or (ii) obligating either party to enter into an agreement regarding the Confidential Information, unless otherwise agreed to in writing. Neither this Agreement nor any right granted hereunder shall be assignable or otherwise transferable by You.

CONFIDENTIAL INFORMATION IS PROVIDED "AS IS" AND DISCLOSING PARTY MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR OTHERWISE, REGARDING CONFIDENTIAL INFORMATION, INCLUDING AS TO ITS ACCURACY. DISCLOSING PARTY ACCEPTS NO RESPONSIBILITY FOR ANY EXPENSES, LOSSES OR ACTION INCURRED OR UNDERTAKEN YOU AS A RESULT OF YOUR RECEIPT OR USE OF ANY INFORMATION PROVIDED HEREUNDER.

Any Confidential Information disclosed hereunder and any copies thereof (including, without limitation, all documents, memoranda, notes, analyses, forecasts and other materials prepared by the Disclosing Party, and all electronically stored copies or physically stored) will be returned or destroyed.

Your obligations under this Agreement shall survive the termination of the Agreement. This Agreement shall be governed by and construed in accordance with the laws of the State of New Mexico, without regard to its conflict of law principles.

You hereby acknowledge and agree that violation of any of these provisions will cause irreparable harm to the Disclosing Party for which monetary remedies may be inadequate, and that the Disclosing Party shall be entitled, without waiving any other rights or remedies, to take all appropriate actions to remedy or prevent such disclosure or misuse, including obtaining an immediate injunction.

This Agreement may not be modified except by writing by Disclosing Party. If any provision of this Agreement or any portion thereof shall be held invalid, illegal or unenforceable by a court of competent jurisdiction, the remaining provisions of this Agreement shall remain in full force and effect, and the affected provisions or portion thereof shall be replaced by a mutually acceptable provision, which comes closest to the economic effect and intention of the parties hereto. This Agreement may be executed in counterparts, all of which shall constitute one agreement.

DO NOT attempt an EC-Council certification exam unless you have read, understood and accepted the terms and conditions in full. By attempting an exam, you signify the acceptance of those terms. Please note that in the event that you do not accept the terms and conditions of the Agreement, you are not authorized by EC-Council to attempt any of its certification exams. EC-Council reserves the right to revoke your certification status, publish the infraction, and/or take the necessary legal action against you, if you fail to comply with the above terms and conditions.





## **EC-Council Certification Agreement v5.0**

w.e.f. June 1<sup>st</sup>, 2020

**EC-Council**

# EC-Council CERTIFICATION AGREEMENT v5.0

Candidate Application Agreement and Candidate Certification Agreement (Hereinafter referred to as "Certification Agreement" v5.0)

**READ THE FOLLOWING TERMS AND CONDITIONS CAREFULLY. EXAMINATION SHALL NOT BE ATTEMPTED UNLESS ALL THE TERMS AND CONDITIONS OF THE AGREEMENT HAS BEEN DULY READ, UNDERSTOOD AND ACCEPTED IN FULL.**

This EC-Council Certification Agreement (the "Agreement") is entered into between you and International Council of E-Commerce Consultant ("EC-Council") as of the date of the acceptance of the agreement.

## 1. DEFINITIONS

For purposes this Agreement, the terms defined in this Section shall have the meanings set forth below:

- 1.1 "Candidate"** means an individual who attempts the certification examination but is not conferred the said certification unless he fulfils all the requirements such as the Passing Criteria. When it is evidenced that the candidate is conferred a certification status, the Candidate shall referred to as a **"Certified Member"**.
- 1.2 "Program"** shall mean one of the certification programs offered by EC-Council.
- 1.3 "Examination Materials"** shall mean EC-Council certification examination(s) and any questions, instructions, responses, answers, worksheets, drawings and/or diagrams related to such examination(s) and any accompanying materials. The list is inclusive of all related EC-Council Training Materials.
- 1.4 "Marks"** means, as the case may be, any and all EC-Council titles, trademarks, service marks and/or logos which EC-Council may from time to time expressly designate for use corresponding to the EC-Council certification that a candidate attempts or a Certified Member have achieved.
- 1.5** Passing Criteria shall mean passing criteria for an EC-Council certification exam which may vary from exam to exam. The passing criteria for an EC-Council exam can be found at <https://cert.eccouncil.org/faq.html>.

## 2. OBLIGATIONS

- 2.1** At all times, you shall agree to adhere to the certification/candidate policies of EC-Council including but not limited to:
  - 2.1.1** Certification Exam Policy (<https://cert.eccouncil.org/certification-exam-policy.html>);
  - 2.1.2** Exam Retake Policy (<https://cert.eccouncil.org/exam-retake-policy.html>);
  - 2.1.3** Eligibility Policy (<https://cert.eccouncil.org/application-process-eligibility.html>);
  - 2.1.4** EC-Council Non-Disclosure Agreement (<https://cert.eccouncil.org/images/doc/NDA-Non-Disclosure-Agreement-v2.0.pdf>);
  - 2.1.5** Special Accommodation Policy (<https://cert.eccouncil.org/special-accommodation-policy.html>);
  - 2.1.6** Appeal Procedure (<https://cert.eccouncil.org/appeal-procedure.html>);
  - 2.1.7** Voucher Extension Policy (<https://cert.eccouncil.org/exam-voucher-extension-policy.html>)

# EC-Council CERTIFICATION AGREEMENT v5.0

EC-Council reserves the right to add, edit, amend or delete the abovementioned policies at any time with or without notice.

2.2 At all times, you shall, either in the capacity of being a Candidate and/or a Certified Member, as applicable, agree to adhere to the Code of Ethics of EC-Council including but not limited to:-

- Keep private and confidential information gained in own professional work, (in particular if it pertains to your client lists and client's personal information). Not collect, give, sell, or transfer any personal information (such as name, e-mail address, Social Security number, or other unique identifier) to a third party without your client's prior consent.
- Protect and respect the intellectual property of others by relying on your own innovation and efforts, thus ensuring that all benefits vest with its originator. Disclose and report to appropriate persons or authorities' potential dangers to any e-commerce clients, the Internet community, or the public, as applicable.
- Provide service in own areas of competence. You should be honest and forthright about any limitations of own experience and education. Ensure that the Certified Member is qualified for any project by an appropriate combination of education, training, and experience.
- Never knowingly use software or process that is obtained or retained either illegally or unethically.
- Not to engage in deceptive financial practices such as bribery, double billing, or other improper financial practices.
- Use and protect the property of your clients or employers only in ways which are properly authorized, and with the owner's knowledge and consent.
- Avoid any conflict of interest. Disclose to all concerned parties, including (without limitation) your clients, employers, EC-Council any actual or potential conflicts of interest that cannot reasonably be avoided or escaped. For the purpose of clarity, if you have participated in Item writing for any of the EC-Council certification examinations, you will not be allowed to sit for the same certification examination. Further, if you wish to be EC-Council's Consultant, you must disclose your association with EC-Council's other products and/or services and/or your association with competing products and/or services.
- Ensure good management for any project as a Certified Member.
- Add to the knowledge of the e-commerce profession by constant study, share the lessons of own experience with fellow EC-Council members, and promote public awareness of benefits of electronic commerce.
- Conduct oneself in the most ethical and competent manner when soliciting professional service or seeking employment, thus meriting confidence in the Certified Member's knowledge and integrity.
- Ensure ethical conduct and professional care at all times on all professional assignments without prejudice.
- Not to associate with malicious hackers or engage in any malicious activities.
- Not to purposefully compromise or allow the client's or organization's systems to be compromised in the course of the Certified Member's professional dealings. EC-Council Certification Agreement v5.0 04
- Ensure all penetration testing activities are authorized and within legal limits.

# EC-Council CERTIFICATION AGREEMENT v5.0

- Not to take part in any black hat activity or be associated with any black hat community that serves to endanger networks.
- Not to be part of any underground hacking community for purposes of preaching and expanding black hat activities.
- Not to make inappropriate reference to the certification or misleading use of certificates, marks or logos in publications, catalogues, documents or speeches.
- Not to be in violation of any law of the land or have any previous conviction.
- Make claims regarding certification only with respect to the scope for which the certification has been granted.
- Not to use the certification in a manner as to bring EC-Council into disrepute.
- Not to make misleading and/or unauthorized statement regarding the certification or EC-Council.
- Discontinue the use of all trademarks as regard to the certification which contains any reference to EC-Council and/or EC-Council trademark or logo or insignia upon suspension/withdrawal of the said certification.
- Return any certificates issued by EC-Council upon suspension/withdrawal of the certification.
- Refrain from further promoting the certification in the event of the said certification is withdrawn or suspended.
- Inform EC-Council without any undue delay of any physical or mental condition which renders the Certified Member incapable to fulfill the continuing certification requirements.
- Maintain the certification by completing, within the time frame specified by EC-Council, all continuing certification requirements (if any) that correspond with Certified member's particular certification.
- To not to participate in any cheating incident, breach of security, misconduct or any other behavior that could be considered a compromise of the integrity or confidentiality of any EC-Council certification examination.

2.2.1 Code of Ethics of EC-Council is subject to change from time to time in order to remain compliant with any applicable laws, rules and regulations and the same shall be updated and located at <https://cert.eccouncil.org/code-of-ethics.html>. It is your responsibility to always refer to such link for any updates.

2.2.2 Upon being a Certified member, you shall adhere to the EC-Council Education (ECE) policy (<https://cert.eccouncil.org/ece-policy.html>).

## 3. CERTIFICATION

3.1 You shall be conferred a certification only upon a successful completion of the required certification examination and your compliance with the requirements described in the current corresponding program brochure. You agree that EC-Council has the right to modify any examination, certification scheme, test objectives or the requirements for obtaining or maintaining any EC-Council certification at any time.



# EC-Council CERTIFICATION AGREEMENT v5.0

- 3.2 Notwithstanding anything in this agreement to the contrary, EC-Council has the sole discretion to withdraw, suspend, or refuse to renew and/or grant you the certification if EC-Council in good faith determines that your certification or use of the corresponding Marks will adversely affect EC-Council or the community at large or consumers.
- 3.3 Upon being conferred the certification, you are expected to notify EC-Council of any changes to your contact information to retain your certification. You may withdraw your contact information at any time in which case, EC-Council shall not have any obligation to keep your certification updated.
- 3.4 Once you are certified, you are solely responsible for keeping yourself informed after EC-Council's continuing certification requirements for maintaining your own certification. If you fail / do not complete the continuing certification requirements timeframe specified by EC-Council, your certification for that particular program will be revoked without further notice, and all rights pertaining to that certification (including the right to use the applicable marks) will be terminated.
- 3.5 Notwithstanding anything in this agreement to the contrary, EC-Council has the sole discretion to withdraw, suspend, or refuse to renew and/or grant you the certification if EC-Council learns at any point of time that the Candidate and/or the Certificate Member, as applicable, has cheated and/or used unethical measures and/or suppressed any material information leading to conflict of interest to obtain the relevant certification.
- 3.6 Notices: All notices herein shall be in writing and in English language. EC-Council may publish any notice online and/or send email at your registered email ID. You may wish to write to EC-Council at [certmanager@eccouncil.org](mailto:certmanager@eccouncil.org) and/or send notices by mail at the below addresses:

## For Europe, Middle East and Asia regions:-

### Attention: Director of Certification

Plot No: SI ,  
TIE Phase -I , Balanagar,  
Hyderabad 500037,  
INDIA

## USA and South America

### Attention: Director of Certification

101 C Sun Avenue NE,  
Albuquerque, NM 87109  
USA

## 4. TERM AND TERMINATION

- 4.1 **Term:** Upon being conferred the certification, you are required to maintain the certification and update the validity of the EC-Council certification via EC-Council's ECE program located at <https://cert.eccouncil.org/ece-policy.html>. The initial certification validity is three years and you are required to fulfill the terms and conditions of the ECE Program to retain the validity of the relevant certification. The term of this Agreement is coterminous with the validity of the certification if you are a Certified Member and if you are not a Certified Member, then the agreement shall be deemed to terminated at the end of your relevant certification exam as a Candidate.

# EC-Council CERTIFICATION AGREEMENT v5.0

- 4.2 **Effect of Termination:** Upon the termination of this Agreement, you as a Certified Member shall immediately cease all use of the Marks, all representations or claims that you hold any EC-Council Certifications, or any other statements that imply in any way that you are EC-Council certified. This obligation includes, but is not limited to, immediately removing the Marks from all web sites and electronic materials under your control, including resumes, profession profiles, and email signatures, as well as from all hard copy materials, including business cards. All unused business cards or other hard copy materials bearing the Marks shall be destroyed within ten (10) days of termination, and you agree to provide EC-Council a written statement under oath attesting to such destruction, if requested by EC-Council. Upon termination, you shall also lose all access to the related portals made available to you by EC-Council during the term by which you are a Certified Member.

## 5. LICENSE

- 5.1 If you are a Candidate and has not been conferred with certification, you shall not be granted the rights to use and/or display the EC-Council trademarks, logo, insignia (hereinafter "Marks") for whatsoever purpose, be it for promotional, advertising, marketing and/or publicity purposes. Failure to abide with this section shall attract legal recourse in the forms of injunctions, civil liability, and forfeiture of profits, and punitive damages and/or other legal sanctions deemed reasonable to address such breach.
- 5.2 Subject to the terms and conditions of this Agreement and the attainment of one or more of EC-Council certifications, EC-Council shall grant you in your capacity as Certified Member a nonexclusive and non-transferable license to only use and display the relevant Marks solely in connection with providing the professional services that correspond to the certification program that the Certified Member had earned.
- 5.3 Once certified, you may use the Marks such on such promotional display and advertising materials as it may, in your judgement, promote the professional services in correspondence to your certification.
- 5.4 You shall not use the Marks for any purposes that are not directly related to the provision of the professional services corresponding to your particular certification. You shall not use the Marks if any certification program unless you have completed the certification program requirements and have been notified by EC-Council in writing that you have achieved the certification status for that particular Program.
- 5.5 As a Certified Member, you shall not misrepresent your own certification status or qualifications so as to imply or suggest that EC-Council in any way endorses, sponsors or recommends you, or any of your products or services.
- 5.6 You also agree that your status as a Certified Member and your rights pertaining to the Marks as vested to you under this Agreement shall not permit you to hold yourself out as having any ownership rights over the official Training/Examination Materials. Any attempts/action which implies to the public that you have some degree of ownership to the official Training/Examination Materials shall be construed as a material breach of this Agreement and your certification shall be revoked with immediate effect.



# **EC-Council** CERTIFICATION AGREEMENT v5.0

## **6. OWNERSHIP OF MARKS BY CERTIFIED MEMBERS**

Once certified, no title or ownership of the Marks shall be transferred, either explicitly or impliedly, to you pursuant to this Agreement. EC-Council owns and retains all title and ownership of all intellectual property rights in the products, documentation, certificate and all other related materials and Marks. EC-Council does not transfer any portion of such title and ownership, or any of the associated goodwill to you, and this Agreement should not be construed to grant you any right or license, whether by implication, estoppel, or otherwise, except as expressly provided. You agree to be bound by and observe the proprietary nature of the materials acquired by reason of your certification under this Agreement.

## **7. CONDUCT OF BUSINESS OF CERTIFIED MEMBERS**

You as a Certified Member shall agree to (i) conduct business in a manner which reflects favorably at all times on the products, goodwill and reputation of EC-Council; (ii) avoid deceptive, misleading or unethical practices which are or might be detrimental to EC-Council or its products; and (iii) refrain from making any representations, warranties, or guarantees to customers that are inconsistent with the policies established by EC-Council. Without limiting the above, you are also obliged to not to misrepresent your certification status or level of skill and knowledge related thereto.

## **8. QUALITY OF PROFESSIONAL SERVICES BY CERTIFIED MEMBERS**

You shall also agree that it is of fundamental importance to EC-Council that the professional services are of the highest quality and integrity. Accordingly, you agree that EC-Council will have the right to determine in its absolute discretion whether the professional services meet EC-Council's standards of merchantability. In the event that EC-Council determines that you are no longer meeting accepted levels of quality and/or integrity, EC-Council agrees to advise you and to provide you with a commercially reasonable time of no less than one (1) month to rectify and meet the same.

## **9. RESERVATION OF RIGHTS AND GOOD WILL IN EC-COUNCIL**

EC-Council retains all rights not expressly conveyed to you by this Agreement. You must recognize the value of the publicity and goodwill associated with the Marks and acknowledge that the goodwill will exclusively inure to the benefit of, and belong to, EC-Council. You as a Certified Member shall have no rights of any kind whatsoever with respect to the Marks licensed under this Agreement except to the extent of the license granted in this Agreement.

## **10. NO REGISTRATION BY CERTIFIED MEMBER**

You agree not to file any new trademark, collective mark, service mark, certification mark, and/or trade name application(s), in any class and in any country, for any trademark, collective mark, service mark, certification mark, and/or trade name that, in EC-Council's opinion, is the same as, similar to, or that contains, in whole or in part, any or all of EC-Council's trade names, trademarks, collective marks, service marks, and/or certification marks, including, without limitation, the Marks licensed under this Agreement. You further agree to not to register or use as your own any internet domain name which contains EC-Council's Marks or other trademarks in whole or in part or any other name which is confusingly similar thereto. To the extent that Certified Member obtains or develops any rights in or to the EC-Council Marks or any confusingly similar trademarks, Certified Member agrees to assign, and does hereby irrevocably assign such rights to EC-Council. This section shall survive the expiration or termination of this Agreement.

# **EC-Council** CERTIFICATION AGREEMENT v5.0

## **11. PROTECTION OF RIGHTS BY CERTIFIED MEMBER**

- 11.1 You agree to assist EC-COUNCIL, to the extent reasonably necessary and at EC-Council's expense, to protect or to obtain protection for any of EC-Council's rights to the Marks.
- 11.2 If at any time EC-Council requests that you discontinue using the Marks and/or substitute using a new or different Mark, you shall immediately cease use of the Marks and cooperate fully with EC- Council to ensure all legal obligations have been met with regards to use of the Marks.

## **12. INDEMNIFICATION BY CERTIFIED MEMBER**

- 12.1 You shall agree to indemnify and hold EC-Council harmless against any loss, liability, damage, cost or expense (including reasonable legal fees) arising out of any claims or suits made against EC-Council (i) by reason of your threatened or actual breach of the terms and conditions under this Agreement; (ii) arising out of your use of the Marks in any manner whatsoever except in the form expressly licensed under this Agreement; and/or (iii) for any personal injury, product liability, or other claim arising from the promotion and/or provision of the professional services.

## **13. CONFIDENTIALITY**

- 13.1 Training/Examination Materials are the proprietary, confidential and copyrighted materials of EC-Council. Any disclosure of the contents of any EC-Council certification examination is strictly prohibited.
- 13.2 You, at all times, hereby agree to maintain the confidentiality of all Examination Materials and not to disclose, publish, reproduce, distribute, post or remove from the examination room, any portion of the Examination Materials. Failure to observe and comply with this provision shall be deemed as a breach and shall attract legal recourse in the forms of injunctions, civil liability, forfeiture of profits, punitive damages and/or other legal sanctions deemed reasonable to address such breach.
- 13.3 Your obligation of confidentiality hereunder shall terminate when you can establish that the Examination Materials (a) is already in the public domain or becomes generally known or published without breach of this Agreement; (b) is lawfully disclosed by a third party free to disclose such information; or (c) is legally required to be disclosed provided that you promptly notify EC-Council so as to permit such EC-Council to appear and object to the disclosure and further provided that such disclosure shall not change or diminish the confidential and/or proprietary status of the Confidential Information.
- 13.4 You further agree that, except as otherwise stated in this Agreement, you shall not use the name of EC-Council and/or its other corresponding entities, either expressed or implied in any of its advertising or sales promotional material.

# EC-Council CERTIFICATION AGREEMENT v4.0

## 14. LIMITATION OF LIABILITY

IN NO EVENT WILL EC-COUNCIL BE LIABLE TO YOU FOR ANY SPECIAL, DIRECT, INDIRECT, CONSEQUENTIAL PUNITIVE, EXEMPLARY OR ANY SIMILAR TYPE OF DAMAGES ARISING OUT OF OR IN ANY WAY RELATED TO THIS AGREEMENT.

## 15. GENERAL PROVISIONS

- 15.1 Governing Law and Venue:** This Agreement will in all respects be governed by the law of the State of New Mexico, excluding its conflicts of laws and provisions, and venue of any actions will be proper in the courts of the State of New Mexico of the United States of America.
- 15.2 Attorney's Fees:** In the event of any action arising out of or relating to this Agreement, the prevailing party shall be entitled to recover the costs and expenses of the action, including reasonable attorney's fees, incurred in connection with such action from the losing party.
- 15.3 Non-Waiver:** No waiver of any right or remedy on one occasion by either party will be deemed a waiver of such right or remedy on any other occasion.
- 15.4 Assignment:** Neither this Agreement nor any of your rights or obligations arising under this Agreement may be assigned without EC-Council's prior written consent. This Agreement is freely assignable by EC-Council, and will be for the benefit of EC-Council's successors and assigns.
- 15.5 Independent Contractors:** You acknowledge that you and EC-Council are independent contractors and you agree to not to represent yourself as, an employee, agent, or legal representative of EC-Council.
- 15.6 Compliance with Laws:** You agree to comply, at your own expense, with all statutes, regulations, rules, ordinances, and orders of any governmental body, department, or agency that apply to or result from your rights and obligations under this agreement.
- 15.7 Modifications:** Any modifications to the typewritten face of this Agreement will render it null and void. This Agreement will not be supplemented or modified by any course of dealing or usage of trade. Any modifications to this Agreement must be in writing and signed by both parties.
- 15.8 Revision of terms:** EC-Council reserves the right to revise the terms of this Agreement from time to time. In the event of a revision, your signing or otherwise manifesting assent to a new agreement may be a condition of continued certification..

**EC-Council**