**EC Council - iClass Weblink** :-

**https://iclass.eccouncil.org/our-courses/certified-chief-information-security-officer-cciso/#1593445871337-e921cc7b-488aCCISO**

**Exam Information**

* [**CCISO Certification**](https://ciso.eccouncil.org/cciso-certification/) . **CCISO Exam Information**

### Why CCISO?

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. The job of the CISO is far too important to be learned by trial and error. Executive level management skills are not areas that should be learned on the job.

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 sitting and 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.

### Minimum Requirements

In order to qualify to sit for the CCISO Exam without taking any training, candidates must have five years of experience in each of the 5 CCISO domains  verified via the [Exam Eligibility Application](https://iclass.eccouncil.org/wp-content/uploads/2020/07/CCISO-Exam-Eligibility-Application-Form-July-2020-Fillable.pdf).

To sit for the exam after taking training, candidates must have five years of experience in three of the five CCISO Domains verified via the [Exam Eligibility Application](https://iclass.eccouncil.org/wp-content/uploads/2020/07/CCISO-Exam-Eligibility-Application-Form-July-2020-Fillable.pdf).

#### Waivers for the CCISO are available to Self-Study Candidates

|  |  |
| --- | --- |
| **Domain** | **Education Waivers** |
| 1. Governance and Risk Management | Ph.D. Information Security – 3 years, MS Information Security Management, MS Information Security Engineering – 2 years, BS Information Security – 2 years |
| 2. Information Security Controls, Compliance, and Audit Management | Ph.D. Information Security – 3 years, MS Information Security Management, MS Information Security Engineering – 2 years, BS Information Security – 2 years |
| 3. Security Program Management & Operations | 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 | Ph.D. Information Security – 3 years, MS Information Security – 2 years, BS Information Security – 2 years |
| 5. Strategic Planning, Finance, Procurement, and Vendor Management | CPA, MBA, M. Fin. – 3 years |

**Exam Information**

[CCISO Renewal Fee](https://store.eccouncil.org/product/cciso-renewal-fee/)($100)    [CCISO Application Fee](https://www.paypal.com/cgi-bin/webscr?cmd=_s-xclick&hosted_button_id=CEEP2NLV63MAL)($100)         [Request Application](https://ciso.eccouncil.org/contact/)

Please see the [exam blueprint](https://ciso.eccouncil.org/wp-content/uploads/2019/03/CCSIO-Blue-Print-2019.pdf). In order to earn the CCISO, every applicant must pass the exam covering all 5 CCISO domains, regardless of experience in each domain. The exam consists of 150 multiple-choice questions administered over a two and a half hour period. The questions on the exam require extensive thought and evaluation.

**About the Exam**

There are three cognitive levels tested on the CCISO exam but only two tested on the EISM exam:

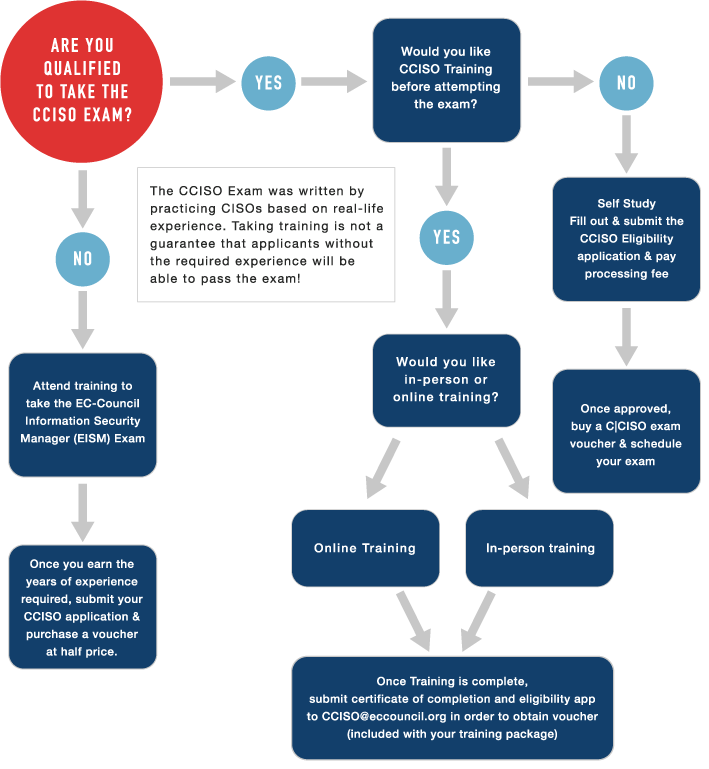
* **Level 1 – Knowledge**: This cognitive level of questions is used to recall memorized facts. This is the most basic cognitive level rarely accepted on certifications as it merely recognizes the candidate’s ability to memorize information. It can be effectively used when asking for basic definitions, standards or any concrete fact. This level appears on both the CCISO and EISM exam.
* **Level 2 – Application**: This cognitive level of questions is used to identify the candidate’s ability to understand the application of a given concept. It differs from Knowledge based questions in the sense that it requires the understanding and correct applicability of a given concept – not just the concept itself. This type of question often quires additional context before the actual question is provided in the stem. This level appears on both the CCISO and EISM exam.
* **Level 3 – Analysis**: This cognitive level of questions is used to identify the candidate’s ability to identify and resolve a problem given a series of variables and context. Analysis questions differ greatly from Application based questions in the sense that they require not only the applicability of a concept but also how a concept, given certain constrain can be used to solve a problem. This level appears on the CCISO and not on the EISM exam.

**Exam Format : Multiple Choice**

* Total number of questions : 150
* Exam duration : 2.5 Hours

**Passing Score**

In order to maintain the high integrity of our certifications exams, EC-Council Exams are provided in multiple forms (I.e. different question banks). Each form is carefully analyzed through beta testing with an appropriate sample group under the purview of a committee of subject matter experts that ensure that each of our exams not only has academic rigor but also has “real world” applicability. We also have a process to determine the difficulty rating of each question. The individual rating then contributes to an overall “Cut Score” for each exam form. To ensure each form has equal assessment standards, cut scores are set on a “per exam form” basis. Depending on which exam form is challenged, cut scores can range from 60% to 85%.



**Are you Ready to be a CCISO?**

[Test Your Skills!](https://ciso.eccouncil.org/cciso-assessment/)

**Subscribe to the CISO Podcast**

[Listen on Apple Podcasts](https://podcasts.apple.com/us/podcast/global-ciso-forum-podcast/id1495077396) [Listen on Stitcher](https://www.stitcher.com/podcast/global-ciso-forum-podcast?refid=stpr) [Listen on Spotify](https://open.spotify.com/show/2hZeiKX4fLiuSvocu0QlrO) [RSS Feed](https://feeds.feedburner.com/GlobalCisoForumPodcast)

**Latest News**

* [Global CISO Forum Podcast: Interview with Martin Knobloch](https://ciso.eccouncil.org/global-ciso-forum-podcast-interview-with-martin-knobloch/)
* [Sponsor Spotlight: No Starch Press](https://ciso.eccouncil.org/sponsor-spotlight-no-starch-press/)
* [Global CISO Forum Podcast: Interview with Dick Wilkinson](https://ciso.eccouncil.org/global-ciso-forum-podcast-interview-with-dick-wilkinson/)

**CCISO Body of Knowledge**



The EC-Council CCISO Body of Knowledge covers all five of the CCISO Information Security Management Domains in depth and was written by seasoned CISOs for current and aspiring CISOs.

[Get your copy today](https://iclass.eccouncil.org/our-courses/certified-chief-information-security-officer-cciso/)

**Featured Whitepaper**

* [Creating a Secure Computer User](https://ciso.eccouncil.org/creating-secure-computer-user/)08th Jul 2016

**C|CISO Assessment** (Step 1 of 6 - Domain 1)16

1. An organization recently implemented a Risk Management program in order to measure risk of IT Projects. In which of the following cases would this organization be more willing to acceptance vs. mitigate risk?\*

* + The organization uses a quantitative process to measure risk
  + The organization uses a qualitative process to measure risk
  + The organization’s risk tolerance is high
  + The organization’s risk tolerance is low

2. An organization is looking for a framework to measure the efficiency and effectiveness of their Information Security Management System (ISMS). Which of the following international standards can BEST assist this organization? \*

* + Payment Card Industry Data Security Standards (PCI-DSS)
  + Control Objectives for Information Technology (COBIT)
  + International Organization for Standardizations – 27004 (ISO-27004)
  + International Organization for Standardizations – 27005 (ISO-27005)

3. A global health care company is concerned about protecting confidential information. Which of the following is of MOST concern to this organization? \*

* + Compliance to the Payment Card Industry (PCI) regulations.
  + Compliance with privacy laws and regulations for each country where they operate.
  + Conform to local Human Resources laws and regulations for each country where they operate.
  + Alignment with International Organization for Standardization (ISO) standards.

4. A global retail company is working on defining a compliance management process. Which of the following are most likely to be included? \*

* + Payment Card Industry Data Security Standards (PCI-DSS)
  + Information Technology Infrastructure Library (ITIL)
  + International Organization for Standardization (ISO) standards
  + National Institute for Standards and Technology (NIST) standards

5. An organization is looking to implement a consistent Disaster Recovery and Business Continuity Process across all of its business units. Which of the following standards and guidelines can BEST address this organization’s need?\*

* + International Organization for Standardizations – 27005 (ISO-27005)
  + International Organization for Standardizations – 22301 (ISO-22301)
  + Information Technology Infrastructure Library (ITIL)
  + Payment Card Industry Data Security Standards (PCI-DSS)

6. The Information Technology Infrastructure Library version 3 (ITILv3) mainly leverages which of the following standards when addressing information security risk management: Choose the BEST answer.\*

* + International Organization for Standardization (ISO) 27799
  + International Organization for Standardization (ISO) 27005
  + National Institute of Standards and Technology (NIST) Special Publication 800-30
  + National Institute of Standards and Technology (NIST) Special Publication 800-124

7. Your information security program is technically well provisioned, however you are actively seeing sensitive employee data and financial information being exposed through compromised account credentials. From the choices provided below what should you do FIRST to minimize this threat?\*

* + Reset passwords for suspected compromised accounts.
  + Educate users about the threat of phishing.
  + Monitor perimeter firewall for signs of phishing.
  + Contact a reputable security vendor to install an anti-phishing appliance.

8. An effective method for reducing the impact of credential theft is (choose the best answer):\*

* + Gaining the trust of your users so they will listen to you.
  + Implementing employee monitoring so they don’t go to unauthorized sites.
  + Deploying multi-factor authentication so accounts are better protected.
  + Resetting passwords every thirty days.

9. Metrics capable of demonstrating that an organization is susceptible to, or has a high probability of being susceptible to, a risk that exceeds the acceptable risk appetite are known as:\*

* + Key Performance Indicators (KPI)
  + Key Risk Indicators (KRI)
  + Insurance Actuary Tables (IAT)
  + Risk Assumption Tables (RAT)

10. A primary consideration when selecting to transfer risk as a risk response measure is: Choose the BEST answer.\*

* + Capital cost
  + Selection of a security control vendor
  + Security consultant fees
  + Insurance cost

11. A CISO has a limited budget for security technology purchases. The desire is to create a tiered security architecture using a phased approach. Which of the following represents the best approach for obtaining the security program’s objectives and supporting the organization’s security needs?\*

* + Complete the easiest hardening actions first to demonstrate positive action toward the security goal
  + Apply technology against the highest target value infrastructure while closely monitoring spending
  + Install protections on Information technology (IT) assets experiencing the highest number of intrusive activities
  + Determine the necessary security program reporting metrics and apply protections according to monthly report results

12. According to the Risk IT Framework Process Model, Risk Evaluation (RE) comprises which three goals? Choose the BEST answer.\*\*

* + Articulate Risk, Manage Risk, React to Events
  + Establish and Maintain a Common Risk View, Integrate with Enterprise Risk Management, Make Risk-aware Business Decisions
  + Third Choice
  + Collect Data, Analyze Risk, Maintain Risk Profile

13. Your organization has made significant investments in physical security for the main data center facility to ensure that only authorized personnel may gain access. A recent audit reveled that employees had easily defeated the technical controls securing the back loading dock so that they could take smoke breaks without having to go through repeated searches and security screenings required when leaving and entering the facility. Which general security class should you focus on to remediate the root cause of this situation? Choose the BEST answer.\*

* + Technical Security Controls
  + Operational Security Controls
  + Management Security Controls
  + Baseline Security Controls

14. Your company leverages an employee self-service portal for common human resource related tasks such as providing annual tax documents, changing direct deposit information, and signing up for health benefits. Several employees have complained that they have not received their paychecks this month; everyone else received their paychecks as usual. What could be the cause?\*

* + Their respective financial institutions were compromised right before payroll was deposited and their accounts were emptied.
  + An accounting “glitch” skipped their pay accounts during payroll audit and failed to issue them a check.
  + They failed to submit their timecards by the deadline.
  + Their company credentials were stolen and used to modify bank routing and account information.

15. Controlled phishing campaigns against your own employees:\*

* + Help you identify areas where you have the potential to improve your training efforts to increase employee resilience against attacks.
  + Target employees that are not following company policy and therefore must be let go.
  + Reduces the amount of time that employees read real fraudulent email and therefore prevents their opportunity to be compromised.
  + Should not be conducted, because it desensitizes them to real world threats hindering their ability to detect phishing attempts.

16. Advanced Persistent Threat is best characterized by which of the following?\*

* + High volumes of unauthorized insider activities such as copying data onto portable storage devices or electronic destruction of high value assets
  + Creative insertions of malicious code into applications and databases using known code vulnerabilities and weaknesses
  + Continuous flooding of network perimeters with system requests causing long-term delays and interruptions
  + Methodical advancement of unauthorized access across systems as valuable assets are discovered using a variety of penetration techniques

17. John has been asked to conduct a vulnerability assessment of his company’s proprietary application. As result of his assessment, he discovered that it possible for an attacker to force an authorization step to take place before the authentication step is completed successfully. What type of issue would allow for this type of compromise to take place? \*

* + Maintenance hook
  + Backdoor
  + Race condition
  + Data validation error

18. Mary is a new security manager for a computer consulting company. She has found out that the company has lost intellectual property in the past because malicious employees installed rogue devices on the network, which were used to capture sensitive traffic. Mary needs to implement a solution that ensures only authorized devices are allowed access to the company network. Which of the following IEE standards was developed for this type of protection? \*

* + IEEE.802.1AR
  + IEEE.802.1AE
  + IEEE.802.1AF
  + IEEE.802.1XR

19. Your company has expanded and build a new branch office, which will have a new server room to support the office IS operations. To ensure that server room meets industry standards for securing egress in and out of the server room, what locking mechanism should be used for the primary and secondary server room entry doors?\*

* + The primary and secondary entrance doors should have access controlled through a swipe card and cipherlock
  + The primary entrance door should have access controlled through a security guard. The secondary doors should be secured from the inside and allow no entry.
  + The primary entrance door should have access controlled through a swipe card or cipher lock. Secondary doors should be secured from the inside and allow no entry.
  + The primary entrance door should have access controlled through a swipe card or cipher lock. Secondary doors should have a security guard.

20. As a CISO, you have been designated as the person in charge of developing incident response and forensics procedures that your company needs to carry out if an incident occurs. You need to ensure that the procedures map to the international principles for gathering and protecting digital evidence. You also need to ensure that if and when internal forensic teams are deployed, that they have labels, tags, evidence bags, cable ties, imaging software, and other associated tools. Which of the following best describes the organization that developed the best practices that you need to ensure that you company’s procedures map to? \*

* + Department of Defense Forensic Committee
  + International Forensic Standards Board
  + International Organization on Computer Evidence
  + International Activities Board

21. A CISO is considering a major security technology purchase and needs to understand capabilities, corporate history, customer feedback, and supportability of a broad range of companies and products. What is the best way to collect this type of initial information?\*

* + Use a Response for Proposal (RFP) approach for gathering information
  + Create a business case in order to communicate expected budget support requirements
  + Create a Return on Investment (ROI) document for executive peer budget analysis and reviews
  + Establish a competitive product review of a few selected technologies in a lab environment

22. As CISO for a large cooperation, you’ve outsourced your network security operations center to a service provider. Which of the following are the two MOST IMPORTANT Key Performance Indicators (KPIs) you would include in your Service Level Agreement (SLA)?\*

* + Incident response times and number of malicious events
  + Incident reporting times and number of unmitigated network attacks
  + Incident response times and number of unmitigated network attacks
  + Incident reporting times and number of malicious events

23. What is the MOST IMPORTANT thing to consider when writing the Statement of Work (SOW)?\*

* + The Service Level Agreements (SLA)
  + Appropriate allocation of dedicated resources
  + Reduction of the number of malicious attacks during the contract period
  + Ensure payment terms are at least NET 30

24. A CISO is required to create an annual security capital expense budget. Which of the following would be included in that part of her budget?\*

* + Fractional costs of employees from other business units who are required to periodically perform security duties
  + Security equipment purchases which are amortized over a longer period that the calendar budget year
  + Supporting business unit costs, such as legal advisement and auditing support for the program
  + All labor expenses realized by employees directly assigned to the security organization

25. A CISO has recently purchased a new web content filtering solution. As part of the business case, he estimated a useful life of 6 years for this technology, at which time it will be replaced. Which of the following best describes this analysis?\*

* + Technology acquisition life cycle
  + Capital expense planning
  + Return on investment
  + Cost benefit analysis

Domain 1: You are the newly hired Chief Information Security Officer for a company that has not previously had a senior level security practitioner. The company lacks a defined security policy and framework for their Information Security Program. Your new boss, the Chief Financial Officer, has asked you to draft an outline of a security policy and recommend an industry / sector neutral information security control framework for implementation. Your Corporate Information Security Policy should include which of the following?\*

* Information security theory
* Desktop configuration standards
* Incident response contacts
* Roles and responsibilities

Domain 2: An information security department is required to remediate system vulnerabilities when they are discovered. Please select the three primary remediation methods that can be used on an affected system.\*

* Software removal, install software patch, maintain system
* Discover software, Remove affected software, Apply software patch
* Install software patch, Operate system, Maintain system
* Install software patch, configuration adjustment, Software Removal

Domain 3: An organization has recently appointed a CISO. This is a new role in the organization and it signals the increasing need to address security consistently at the enterprise level. This new CISO, while confident with skills and experience, is constantly on the defensive and is unable to advance the IT security centric agenda. Which of the following is the MAIN reason the CISO has not been able to advance the security agenda in this organization?\*

* Lack of business continuity process
* Lack of a security awareness program
* Lack of influence with leaders outside IT
* Lack of identification of technology stake holders

Domain 4: Your company has many encrypted telecommunications links for their world-wide operations. Physically distributing symmetric keys to all locations has proven to be administratively burdensome, but symmetric keys are preferred to other alternatives. How can you reduce the administrative burden of distributing symmetric keys for your employer?\*

* Use certificate authority to distribute private keys
* Symmetrically encrypt the key and then use asymmetric encryption to unencrypt it
* Use asymmetric encryption for the automated distribution of the symmetric key
* Use a self-generated key on both ends to eliminate the need for distribution

Domain 5: A Chief Information Security Officer (CISO) recently had a third party conduct an audit of the security program. Internal policies and international standards were used as audit baselines. The audit report was presented to the CISO and a variety of high, medium and low rated gaps were identified. After determining the audit findings are accurate, which of the following is the MOST logical next activity?\*

* Create a briefing of the findings for executive management
* Begin initial gap remediation analyses
* Review the security organization’s charter
* Validate gaps with the Information Technology team