General

The International Association of Professional Security Consultants has created the Certified Security Consultant℠ (CSC℠) designation, which reflects a minimum criterion of knowledge and experience that an independent security consultant should have. Earning a CSC℠ designation requires that an applicant meets the qualifications outlined below and that they pass a 100-question multiple-choice examination.

Qualifications

IAPSC members are automatically qualified to test for the CSC℠. Applicants that are not members of the Association must meet the requirements below.
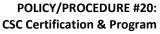
The Association will verify experience through references supplied.

I.   Experience

- Each candidate for certification shall have at least three years of documented security consulting experience, which includes an internal consultant/advisor for an organization. Each candidate for certification will show significant and measurable contribution to the security industry. Examples of contributions include but are not limited to: security-related presentations or public speaking; publishing; teaching; serving in a responsible charge position for a security industry association (officer, board member, committee chairperson). Each contribution must be security-related and verifiable. The Association may also accept other contributions at the discretion of the professional certification committee. Applicants must show a minimum of three significant and measurable contributions in five-years prior to their application.

- If security consulting experience is unverifiable, applicants may submit evidence of work product in the form of deliverables (survey report, written opinions, or schematics/drawings) from three (3) projects/clients over a three (3) year period. Client names and other identifying information will be redacted from each sample prior to submitting to the Professional Certification Committee for consideration.

II.   Education and Experience

- Each candidate for certification shall submit documentation of an earned baccalaureate degree from an accredited college or university or;

- 8 years of direct, broad security management experience shall be accepted by the Certification Committee as the equivalent of a degree or;

- The degree requirement may also be replaced with a combination of documented security management experience and a single certification. A Certified Protection Professional (CPP) or Certified Information Systems Security Professional (CISSP) shall be the equivalent of four (4) years of security management experience or a Physical Security Professional (PSP) shall be the equivalent of a two (2) years of security management experience. A single certification shall be permitted along with the remainder of documented security management experience as an equivalent to the degree requirement for a total of eight (8) years.

III.   Independence

- Independence shall include any requirements as defined by the association By-Laws.

IV.   Code of Ethics

Each Certified CSC℠ Person will adhere to the Association's code of conduct and ethics.

A. Enforcement

Enforcement shall be in accordance with code of ethics and related by-laws.

Background Check

The Association shall conduct a criminal background check and education verification check to confirm the application. The non-member, non-refundable portion of the application fee will cover the background check.

Attestation

CSCs℠ shall sign a statement declaring they have read, understood, and will abide by this policy

Reference Material

REFERENCE	AUTHOR
ASIS General Security Risk Assessment Guideline (2003)	ASIS Commission on Standards and Guidelines
The Comprehensive Forensic Services Manual (2000)	Babitsky, Steven Mangraviti, James Todd, Christopher
Designing Physical Access Control Systems (2017)	Bale, Ross
Premise Security Experts and Admissibility Considerations under Daubert & Kumho (2010)	Bates, Norm Frank, Danielle
The Design and Evaluation of Physical Protection Systems (2nd Edition)	Garcia, Mary Lynn
Forensic Methodology	IAPSC Best Practice
IAPSC Code of Ethics	IAPSC Best Practice
Security Consulting (4th Edition)	Sennewald, Charles
Becoming an Independent Security Consultant (2016)	Silva, Michael
Strategic Security Management (2007)	Vellani, Karim
Security Risk Assessment, Managing Physical & Operational Security (1st Edition)	White, John

Domains, Tasks, and Knowledge Statements

DOMAIN I: SERVING THE CLIENT (20%)
Task 01/01 Professionally Serving the Client

Knowledge of:
- 01/01/01: Client Relations
- 01/01/02: Communications
- 01/01/03: Analyzing & Assessing Client Needs

Task 01/02 Implementing Work Product

Knowledge of:
- 01/02/01: Project Management
- 01/02/02: Time Management
- 01/02/03: The Final Report
- 01/02/04: The Final Presentation

DOMAIN II: SECURITY CONSULTING METHODS (70%)
Task 02/01 Understanding Security Management Consulting

Knowledge of:
- 02/01/01: Threat Assessment & Crime Analysis
- 02/01/02: Vulnerability: Security Surveys, Security Audits, Security Reviews, and Risk Assessments
- 02/01/03: Security Countermeasures: Physical, Technical, Personnel, Training, and Policies & Procedures
- 02/01/04: Security Organization and Management
- 02/01/05: Liability Prevention
- 02/01/06: Crime Prevention / Reduction
- 02/01/07: Anti-terrorism Measures
- 02/01/08: Facility Emergency Planning & Business Continuity
- 02/01/09: Convergence: Security Management and IT

Task 02/02 Understanding Technical Security Consulting

Knowledge of:
- 02/02/01: Physical Security Assessments & Surveys
- 02/02/02 Basics of System Design & Integration
- 02/02/03: Security Hardware Functions & Applicability
- 02/02/04: Technical Specifications
- 02/02/05: Project Management Practices
- 02/02/06: Phases of Project Life Cycle

Task 02/03 Understanding Forensic Consulting

Knowledge of:
- 02/03/01: Expert Witness and Role as an Educator to the Court System
- 02/03/02: Civil Legal Process: Foreseeability, Duty, Breach of Duty, Proximate Cause
- 02/03/03: Discovery
- 02/03/04: Expert Reports
- 02/03/05: Crime Analysis and Foreseeability Measures: Prior-Similars and Totality of the Circumstances

- 02/03/06: Security Survey
- 02/03/07: Federal & State Laws and Relevant Court Opinions

DOMAIN III: BUSINESS ETHICS (10%)
Task 03/01 General Ethical Standards

Knowledge of:
- 03/01/01: Basic Responsibilities
- 03/01/02: Professional Practices & Conduct
- 03/01/03: Client Engagements / Arrangements
- 03/01/04: Fees
- 03/01/05: Conflicts of Interest and Non-Disclosure

Expiration

The first expiration date is three years from December 31st in the year in which the test was passed. For example, if the test was passed on April 2, 2020, the first expiration will be three years from December 31, 2020, which will be December 31, 2023. Recertification will be required every three years thereafter on December 31st.

Application & Testing Deadline

Candidates have one (1) year from the time the IAPSC accepts the application to sit for the certification exam.

Fees

The CSC application fee is non-refundable.

- IAPSC Member: $300
- Non-Member: $500 - *Please note: $200 of this fee is for conducting the background check and is non-refundable.*

Testing & Retesting

Testing
- 70% or higher required to pass.
- Self-proctored: 120 minutes to complete 100 questions.
- The candidate must complete an affirmation at the beginning of the test, stating they understand the test is NOT an open book. The candidate cannot have any notes or documents containing information from the materials with them during the exam.

Retesting
If a candidate does not pass the exam, they cannot re-test for at least 90 days and the re-test must be completed within 6 months of the first test. There will be no charge for the first re-test.

If a candidate does not pass the re-test, there will be a $100 fee to take the test a third time: again, the candidate cannot re-test for at least 90 days from the last test and must retest within 6 months.

If the test is not passed after 3 tries the candidate must re-apply to test and pay the full application fee.

IAPSC Headquarters

`

CSC^{SM} Applications

IAPSC Headquarters will receive all applications to sit for the CSC exam.

- Applications from members in good standing will be processed promptly.

  Applications from non-members will follow the below steps:
  - For applications from non-members, IAPSC Headquarters will perform the first-level review to determine if the applicant meets all the requirements. Then forward the application to the CSC Committee Chair with a recommendation to allow the application to proceed or not.
  - The first level review will include an investigation into the applicant's business activities to ensure full compliance with the CSC qualifications. This will include actions such as reviewing the applicant's web site and business-related social media platforms as applicable.
  - After the CSC Committee approves the application, IAPSC Headquarters will perform a background check to verify criminal records and education. The applicant will not receive test access until the background check comes back clear to proceed.

  After a candidate passes the CSC exam IAPSC Headquarters will:
  - Send out a congratulatory email and updated certificate. The Executive Committee & Board of Directors shall be copied on the email.
  - Add their name to the IAPSC website list of CSCs.
  - Announce the certification in the IAPSC newsletter to alert other members of this accomplishment.

  For those instances when a candidate does not pass the exam, IAPSC Headquarters will send out an an email describing the re-testing procedures and requirements contained within this policy.

CSC Committee

The CSC Committee shall be made up of currently CSC certified members. Committee responsibilities include:

- Reviewing CSC references every three (3) years, updating as appropriate (such as a newer edition of a publication), and modifying related test bank questions as needed.

- Maintain a test bank of 200 multiple questions for the CSC exam.

- Review all CSC applications and recertification applications to determine acceptability.

  - The Chair shall make the first review and refer those issues that are still questionable to the whole committee.

- Promote the certification among the membership and outside the association.

CSC Recertification Procedure

Every Certified Security Consultant (CSC) has a continuing education requirement of 60 recertification credits over the 36-month certification period.

Credit values for each recertification activity are available on the IAPSC website. Credit-bearing

activities can include security-related presentations or public speaking; publishing; attending an educational event; and/or serving in a leadership position for a security industry association. Each contribution must be security-related and verifiable with documentation provided as an attachment to the application form.

CSCs must submit their completed application, recertification fee, and the 60 credits by December 31 of the year of expiration.

The CSC Committee and IAPSC Board understand there are extenuating circumstances. For this reason, a three-month grace period is in place. Formal, written requests for an extension or explanations for delinquency must be submitted to Association headquarters by no later than December 31 of the year of the CSCs expiration date. If after review, an extension is granted, an application, recertification fee, and the 60 credits must be submitted to Association headquarters by no later than March 31. Credits must have been achieved during the recertification period. A late fee of $65.00 for members and $100.00 for non- members will apply.

Refunds will not be granted.

CSCs that fail to observe this policy will be referred to the IAPSC Committee and IAPSC Board of Directors for appropriate action.

Recertification Communication Plan

January of the year of recertification all CSCs due to re-certify that year receive notification that their certification expires on December 31 of that year and an outline of the procedure that must be followed.

IAPSC will include regular recertification reminders through the newsletter.

Individuals due for recertification within the year will receive bi-monthly email reminders through September, thereafter bi-weekly reminders.

By November 1st of each year, the CSC committee will receive a list of all CSCs due for renewal that year that remain outstanding.

Failure to Recertify

Those that fail to recertify are no longer permitted to the CSC designation for any purpose such as signature blocks, web sites, advertising material, or resumes.