CSSLP®

Certified Secure Software Lifecycle Professional

Application vulnerabilities continue to top the list of cyber security concerns. While attackers and researchers continue to expose new application vulnerabilities, the most common application flaws are previous, rediscovered threats. This high volume of known application vulnerabilities suggests that many development teams do not have the security resources needed to address all potential security flaws and a clear shortage of qualified professionals with application security skills exists. Without action, this soft underbelly of business and governmental entities has and will continue to be exposed with serious consequences—data breaches, disrupted operations, lost business, brand damage, and regulatory fines. This is why it is essential for software professionals to stay current on the latest advances in software development and the new security threats they create.

The Certified Secure Software Lifecycle Professional (CSSLP®) certification validates that software professionals have the expertise to incorporate security practices – authentication, authorization and auditing – into each phase of the software development lifecycle, from software design and implementation to testing and deployment.

WHY BECOME A CSSLP

The CSSLP Helps You:

- Validate your expertise in application security.
- Conquer application vulnerabilities offering more value to your employer.
- Demonstrate a working knowledge of application security.
- Differentiate and enhance your credibility and marketability on a worldwide scale.
- Affirm your commitment to continued competence in the most current best practices through (ISC)²'s Continuing Professional Education (CPE) requirements.

The CSSLP Helps Employers:

- Break the penetrate and patch test approach.
- Reduce production cost, vulnerabilities and delivery delays.
- Enhance the credibility of your organization and its development team.
- Reduce loss of revenue and reputation due to a breach resulting from insecure software.
- Ensure compliance with government or industry regulations.

CSSLP INSIGHTS

"Having engineers and developers who have hands-on experience with the CSSLP domains is vital to your organizations' success."

Richard Tychansky, CSSLP
United States

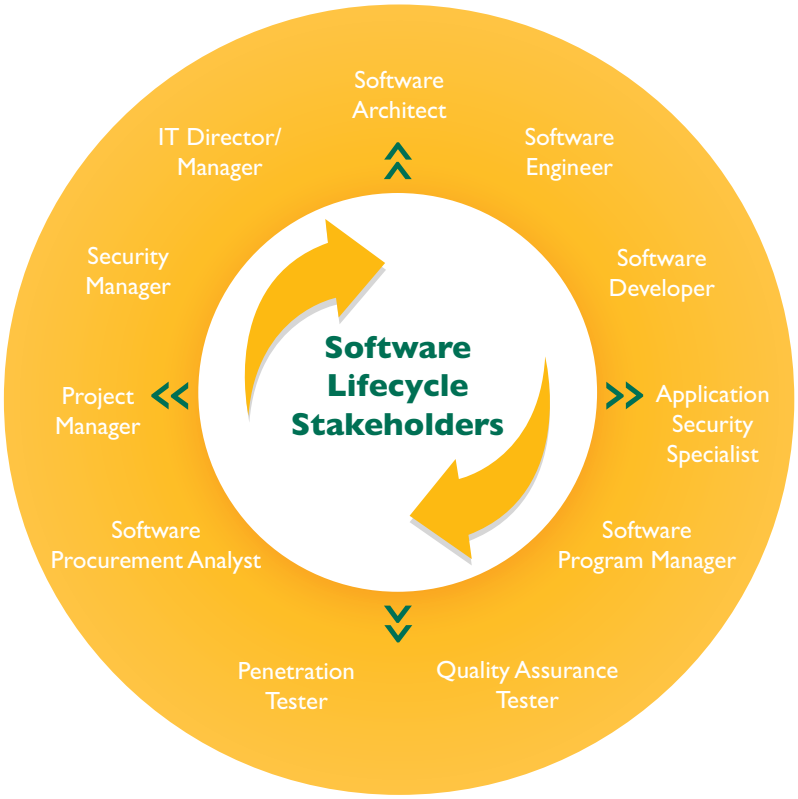
"The need for secure software is critical to protecting businesses and consumers. A key solution is ensuring software development professionals are fully versed in secure software concepts and best practices. That's what makes the CSSLP so invaluable, and the ANSI accreditation further validates its worth to individuals and organizations."

Glenn Leifheit, CISSP, CSSLP
Principal Security Architect
Microsoft - United States

The CSSLP has been approved by the U.S. Department of Defense (DoD) to meet the criteria of Directive 8570.1M. This mandate requires that all DoD information assurance workers obtain a professional certification accredited under the global ANSI/ISO/IEC Standard 17024.

WHO SHOULD BECOME A CSSLP

CSSLP® is for all software lifecycle stakeholders with at least four years professional experience.



CSSLP candidates must possess a minimum of four years cumulative paid full-time professional work experience in the software development lifecycle (SDLC) in one or more of the eight domains of the (ISC)²® CSSLP CBK® or three years of recent work experience with an applicable four-year college degree.

ENGAGE WHILE OBTAINING EXPERIENCE

Associate of (ISC)²

You don't have to spend years in the field to demonstrate your competence in software security. Become an Associate of (ISC)², and you're already part of a reputable and credible organization, earning recognition from employers and peers for the industry knowledge you've already gained.

Participation Requirements

Associate of (ISC)² status is available to those knowledgeable in key areas of industry concepts but lacking the work experience. As a candidate, you must successfully pass the CSSLP examination and subscribe to the (ISC)² Code of Ethics, however to earn the CSSLP credential you will have to acquire the necessary years of professional experience required, provide proof and be endorsed by a member of (ISC)² in good standing. If you are working towards this credential, you will have a maximum of five years from your exam pass date to acquire the necessary five years of professional experience. An Annual Maintenance Fee (AMF) of US$35 applies and 15 Continuing Professional Education (CPE) credits must be earned each year to remain in good standing.

For more information on how you can become an Associate of (ISC)², visit **www.isc2.org/associate**.

The CSSLP® CBK® contains the largest, most comprehensive, collection of best practices, policies, and procedures, to ensure a security initiative across all phases of application development, regardless of methodology.

The comprehensive (ISC)²® CSSLP CBK Training Program covers the following domains:

- **Secure Software Concepts** – security implications and methodologies within centralized and decentralized environments across the enterprise's computer systems in software development.
  - Core Concepts
  - Security Design Principles
  - Privacy
  - Governance, Risk and Compliance
  - Software Developement Methodologies
- **Secure Software Requirements** – capturing security controls used during the requirements phase to integrate security within the process, to identify key security objectives, and to maximize software security while minimizing disruption to plans and schedules.
  - Policy Decomposition
  - Data Classification & Categorization
  - Functional Requirements
  - Operational Requirements
- **Secure Software Design** – translating security requirements into application design elements including documenting the elements of the software attack surfaces, conducting threat modeling, and defining any specific security criteria.
  - Design Processes
  - Design Considerations
  - Securing Commonly Used Architecture
  - Technologies
- **Secure Software Implementation/Coding** – involves the application of coding and testing standards, applying security testing tools including 'fuzzing', static-analysis code scanning tools, and conducting code reviews.
  - Declarative versus Imperative (Programmatic) Security
  - Vulnerability Database / Lists
  - Defensive Coding Practices and Controls
  - Source Code and Versioning
  - Developement and Build Environment
  - Code / Peer Review
  - Code Analysis
  - Anti-tampering Techniques
- **Secure Software Testing** – integrated QA testing for security functionality and resiliency to attack.
  - Testing Artifacts
  - Testing for Security and Quality Assurance
  - Types of Testing
  - Impact Assessment and Corrective Action
  - Test Data Lifecycle Management
- **Software Acceptance** – security implications in the software acceptance phase including completion criteria, risk acceptance and documentation, Common Criteria and methods of independent testing.
  - Pre-Release or Pre-Deployment
  - Post-Release
- **Software Deployment, Operations, Maintenance and Disposal** – security issues around steady state operations and management of software. Security measures that must be taken when a product reaches its end of life.
  - Installation and Deployment
  - Operations and Maintenance
  - Software Disposal
- **Supply Chain & Software Acquisition** – provides a holistic outline of the knowledge and tasks required in managing risk for outsourced development, acquisition, and procurement of software and related services.
  - Supplier Risk Assessment
  - Supplier Sourcing
  - Software Developement Test
  - Software Delivery, Operations & Maintenance
  - Supplier Transitioning

Download a copy of the CSSLP Exam Outline at **www.isc2.org/exam-outline**.

EDUCATION DELIVERED YOUR WAY

Official (ISC)²® CSSLP® CBK® Training Program

The Official Training Program is your exclusive way to learn security best practices and industry standards for the software lifecycle – critical information to CSSLP. Through this program you will gain knowledge and learn how security should be built into each phase of the software lifecycle. It also details essential security measures that should take place, beginning with the requirement phase, through software specification and design, software testing and ultimately disposal.

This intense program provides an in-depth breakdown of the CSSLP domains, while identifying key study areas, including:

- 100% up-to-date material
- Contributions from CSSLPs, (ISC)² Authorized Instructors and subject matter experts
- An overview of the scope of security

"Security has been an afterthought for many years. It's hard to change old habits. This course was very valuable for attempting to change old habits by reviewing the SDLC and understanding where and how it can be secured."

David Lindberg, CISSP
Blue Cross Blue Shield of Minnesota

The Official CSSLP CBK Training Program is offered in the following formats:

- **Classroom** Delivered in a multi-day, classroom setting. Course material focuses on covering the eight CSSLP domains. Available throughout the world at (ISC)² facilities and (ISC)² Official Training Providers.

- **Private On-site** Host your own CSSLP CBK Seminar on- or off-site. Available for larger groups, this often saves employee travel time and expense. Group pricing also applies to organizations with 15 or more employees planning to sit for the exam.

- **Live OnLine** Educate yourself from the convenience of your computer. Live OnLine brings you the same award winning course content as the classroom based or private on-site seminars and the benefit of an (ISC)² Authorized Instructor.

  Visit **www.isc2.org/csslpedu** for more information or to register.

"The course for CSSLP was very comprehensive. Even after 20+ years in application development and project management, the material covered many topics where new strategies may be applied to help my organization to reach higher levels of maturity in securing applications, thus, protecting assets and reputation."

Susan Croely,
Spectra Energy

OFFICIAL TRAINING PROVIDERS

The Official (ISC)² CBK Training Program is available throughout the world at (ISC)² facilities and through (ISC)² Official Training Providers. The Official (ISC)² CBK Training Program is conducted only by (ISC)² Authorized Instructors who are experts in their field and have demonstrated their mastery of the covered domains.

Be wary of training providers that are not authorized by (ISC)². Be certain that your educator carries the (ISC)² Official Training Provider logo to ensure that you are experiencing the best and most current programs available.

2013 SC Magazine Award Winner – Best Professional Training Program, (ISC)² Education

Exam Outline - Free

Your primary resource in your study efforts to become a CSSLP®. The exam outline contains an exam blueprint that outlines major topics and subtopics within the domains, a suggested reference list for further study, exam information and registration/administration policies and instructions. **www.isc2.org/exam-outline**

Official (ISC)²® Guide to the CSSLP CBK®

Recognized as one of the best application security tools available, it's both up-to-date and relevant, reflecting the latest developments in this ever-changing field and providing an intuitive approach to the CSSLP CBK.

Numerous illustrated examples and practical exercises are included in this book to help the reader understand the concepts within the CBK. **www.isc2.org/store**

studISCope Self Assessment

Experience the CSSLP certification exam as closely as possible before you take it. Each 100 question studISCope, provides the look and feel of the exam while identifying key domains to study. You'll even receive a personalized study plan. **www.isc2.org/studiscope**

CBK Domain Previews – Free Webcast Channel

View a series of short webcasts that provide a detailed overview of each domain of the CSSLP, the value of certification and how to study for the exam. **www.isc2.org/previews**

CHECKLIST FOR CERTIFICATION

Obtain the Required Experience - Attest that you possess a minimum of four years cumulative paid full-time professional work experience in the software development lifecycle (SDLC) in one or more of the eight domains of the (ISC)²® CSSLP® CBK® or three years of recent work experience with an applicable four-year college degree. If you do not have the required experience, you may still sit for the exam and become an Associate of (ISC)² until you have gained the required experience.

Study for the Exam - Utilize these optional educational tools to learn the CSSLP CBK. This includes:

- Exam Outline
- CBK Domain Preview Webcasts
- Official Textbook
- studISCope Self Assessment
- Official Training Program

Register for the Exam

- Visit **www.isc2.org/certification-register-now** to schedule an exam date
- Submit the examination fee

Pass the Exam - Pass the CSSLP examination with a scaled score of 700 points or greater. Read the Exam Scoring FAQs at **www.isc2.org/exam-scoring-faqs**.

Complete the Endorsement Process - Once you are notified that you have successfully passed the examination, you will have nine months from the date you sat for the exam to complete the following endorsement process:

- Complete an Application Endorsement Form
- Subscribe to the (ISC)² code of ethics
- Have your form endorsed by an (ISC)² member

The credential can be awarded once the steps above have been completed and your form has been submitted.* Get the guidelines and form at **www.isc2.org/endorsement**.

Maintain the Certification - Recertification is required every three years, with ongoing requirements to maintain your credentials in good standing. This is primarily accomplished through earning 90 Continuing Professional Education (CPE) credits every three years, with a minimum of 15 CPEs earned each year after certification. If the CPE requirements are not met, CSSLPs must retake the exam to maintain certification. CSSLPs must also pay an Annual Maintenance Fee (AMF) of US$100.

MEMBER BENEFITS

FREE:

(ISC)² One-Day SecureEvents
Industry Initiatives
Certification Verification
Chapter Program
(ISC)² Receptions/Networking Opportunities
(ISC)² Global Awards Program
Online Forum
(ISC)² e-Symposium Webinars
ThinkTANK
Global Information Security Workforce Study
InfoSecurity Professional Magazine
Safe and Secure Online Volunteer Opportunities
InterSeC

DISCOUNTED:

(ISC)² Security Congress
(ISC)² Local Two-Day Secure Events
Industry Conferences
The (ISC)² Journal

Maintain the certification with required CPEs and AMF

For more information on the CSSLP, visit **www.isc2.org/csslp**.

**Audit Notice - Passing candidates will be randomly selected and audited by (ISC)² prior to issuance of any certificate. Multiple certifications may result in a candidate being audited more than once.*

*Formed in 1989 and celebrating its 25th anniversary, (ISC)²® is the largest not-for-profit membership body of certified information and software security professionals worldwide, with nearly 100,000 members in more than 135 countries. Globally recognized as the Gold Standard, (ISC)² issues the Certified Information Systems Security Professional (CISSP®) and related concentrations, as well as the Certified Secure Software Lifecycle Professional (CSSLP®), the Certified Cyber Forensics Professional (CCFP℠), Certified Authorization Professional (CAP®), HealthCare Information Security and Privacy Practitioner (HCISPP℠), and Systems Security Certified Practitioner (SSCP®) credentials to qualifying candidates. (ISC)²'s certifications are among the first information technology credentials to meet the stringent requirements of ISO/IEC Standard 17024, a global benchmark for assessing and certifying personnel. (ISC)² also offers education programs and services based on its CBK®, a compendium of information and software security topics. More information is available at **www.isc2.org**.*