CSSLP - Certified Secure Software Lifecycle Professional

(PLEASE NOTE: Effective July 1, 2017, the CSSLP exam is based on a new exam outline.)

Why Should I Get the CSSLP Certification?

The Benefits of CSSLP Certification to the Professional

Many organizations have adopted the CSSLP as the preferred credential to convey one's expertise on security in the software development lifecycle. In today's interconnected world, security must be included within each phase of the software lifecycle. 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 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

How to Get Your CSSLP Certification

Here are the steps to become a certified CSSLP:

1. Obtain the Required Experience

Candidates must have a minimum of 4 years cumulative paid full-time Software Development Lifecycle (SDLC) professional experience in 1 or more of the 8 domains of the CSSLP CBK. Earning a 4-year college degree or regional equivalent will waive 1 year of the required experience. Only a 1 year experience exemption is granted for education. 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.

PLEASE NOTE: Effective July 1, 2017, the CSSLP exam is based on a new exam outline.

2. Schedule the Exam

- Create an account at **Person Vue** and schedule your exam.
- Complete the Examination Agreement, attesting to the truth of your assertions regarding professional experience, and legally committing to the adherence of the **(ISC)² Code of Ethics**.
- Review the **Candidate Background Questions**.
- Submit the examination fee.

3. Pass the Exam

Pass the CSSLP examination with a scaled score of 700 points or greater. Read the **Exam Scoring FAQs**.

4. Complete the Endorsement Process

Once you are notified that you have successfully passed the examination, you will be required to have your application endorsed before the credential can be awarded. An **endorsement form** for this purpose must be completed and signed by an (ISC)² certified professional who is an active member, and who is able to attest to your professional experience. With the Endorsement Time limit, you are required to become certified within 9 months of the date of your exam OR become an Associate of (ISC)². If you do not become certified or an Associate of (ISC)² within 9 months of

the date of your exam you will be required to retake the exam in order to become certified. [(ISC)² can act as an endorser for you if you cannot find a certified individual to act as one.] Please refer to the **Endorsement Assistance Guidelines** for additional information about the endorsement requirements.

5. Maintain the CSSLP Certification
Recertification is required every three years, with ongoing requirements to maintain your credentials in good standing. This is primarily accomplished through continuing professional education (CPE) credits. CSSLPs are required to earn and post am minimum of 30 CPE credits (of the 90 CPE credits required in the three-year certification cycle) and pay the AMF of US$100 during each year of the three-year certification cycle before the member's certification or recertification annual anniversary date.

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

CSSLP Domains
PLEASE NOTE: Effective July 1, 2017, the CSSLP exam is based on a new exam outline

The CSSLP examination domains and weights are:

Domains	**Weight**
1. Secure Software Concepts	13%
2. Secure Software Requirements	14%
3. Secure Software Design	16%
4. Secure Software Implementation/Programming	16%
5. Secure Software Testing	14%
6. Secure Lifecycle Management	10%
7. Software Deployment, Operations, Maintenance	9%
8. Supply Chain and Software Acquisition	8%
Total	**100%**

Secure Software Concepts

- Core concepts
- Security design principles
- **Secure Software Requirements**
- Identify security requirements
- Interpret data classification requirements
- Identify privacy requirements
- Develop misuse and abuse cases
- Include security in software requirement specifications
- Develop security requirement traceability matrix
- **Secure Software Design**
- Perform threat modelling
- Define the security architecture
- Perform secure interface design
- Perform architectural risk assessment
- Model (non-functional) security properties and constraints
- Model and classify data
- Evaluate and select reusable secure design
- Perform design security review
- Design secure assembly architecture for component-based systems
- Use security enhancing architecture and design tools

- Use secure design principles and patterns

Secure Software Implementation/Programming

- Follow secure coding practices
- Analyze code for security vulnerabilities
- Implement security controls
- Fix security vulnerabilities
- Look for malicious code
- Securely reuse third party code or libraries
- Securely integrate components
- Apply security during the build process
- Debug security errors

Secure Software Testing

- Develop security test cases
- Develop security testing strategy and plan
- Identify undocumented functionality
- Interpret security implications of test results
- Classify and track security errors
- Secure test data
- Develop or obtain security test data
- Perform verification and validation testing (e.g., IV&V)

Software Lifecycle Management

- Secure configuration and version control
- Establish security milestones
- Choose a secure software methodology
- Identify security standards and frameworks
- Create security documentation
- Develop security metrics
- Decommission software
- Report security status
- Support governance, risk and compliance (GRC**)**

Software Deployment, Operations and Maintenance

- Perform implementation risk analysis
- Release software securely
- Securely store and manage security data
- Ensure secure installation
- Perform post-deployment security testing
- Obtain security approval to operate
- Perform security monitoring (e.g., managing error logs, audits, meeting SLAs, CIA metrics)
- Support incident response
- Support patch and vulnerability management
- Support continuity of operations

Supply Chain and Software Acquisition

- Analyze security of third party software
- Verify pedigree and provenance
- Provide security support to the acquisition process

CSSLP Course Overview

Led by an (ISC)² authorized instructor, this training seminar provides a comprehensive review of application security concepts and industry best practices, covering the 8 domains of the CSSLP CBK:

- Secure Software Concepts
- Secure Software Requirements
- Secure Software Design
- Secure Software Implementation/Programming
- Secure Software Testing
- Secure Lifecycle Management
- Software Deployment, Operations, Maintenance
- Supply Chain and Software Acquisition

Several types of activities are used throughout the course to reinforce topics and increase knowledge retention. These activities include open ended questions from the instructor to the students, matching and poll questions, group activities, open/closed questions, and group discussions. This interactive learning technique is based on sound adult learning theories.

This training course will help candidates review and refresh their application security knowledge and help identify areas they need to study for the CSSLP exam and features:

- Official (ISC)² courseware
- Taught by an authorized (ISC)² instructor
- Student handbook
- Collaboration with classmates
- Real-world learning activities and scenarios

Who should attend?
This course is designed for professionals who demonstrate a globally recognized level of competence, as defined in a common body of knowledge, by assuring security throughout the software lifecycle. They incorporate security when planning, designing, developing, acquiring, testing, deploying, maintaining, and/or managing software to increase its trustworthiness.

The course is intended for students who have at least four years of direct full-time secure software lifecycle professional work experience in one or more of the 8 domains of the CSSLP CBK, or three years of direct full-time secure software lifecycle professional work experience in one or more of the eight domains of the CSSLP CBK with a four-year college degree in an information technology discipline. The course builds on and brings together the holistic view of the topics covered in the everyday environment of an information assurance professional. Experience in the following professions will greatly enhance the learning environment.

- Software developers
- Engineers and architects
- Product managers
- Project managers
- Software QA
- QA testers
- Business analysts
- Professionals who manage these stakeholders

Learning Objectives

- The goal of the **Security Software Concepts** module is to provide the learner with concepts related to the core software security requirements and foundational design principles as they relate to issues of privacy, governance, risk, and compliance. Learners will understand the software methodologies needed in order to develop software that is secure and resilient to attacks.
- The goal of **the Security Software Requirements** module is to provide the learner with concepts related to understanding the importance of identifying and developing software with secure requirements. The learner will be able to incorporate security requirements in the development of software in order to produce software that is reliable, resilient, and recoverable.
- The design phase of **secure software development** is one of the most important phases in the Software Development Lifecycle. The Security Software Design module provides the learner with an understanding of how to ensure that software security requirements are included in the design of the software. Learners will

gain knowledge of secure design principles and processes, and be exposed to different architectures and technologies for securing software.

- The **Security Software Implementation/Coding** module provides the learner with an understanding of the importance of programming concepts that can effectively protect software from vulnerabilities. Learners will touch on topics such as software coding vulnerabilities, defensive coding techniques and processes, code analysis and protection, and environmental security considerations that should be factored into software.
- The **Security Software Testing** module addresses issues pertaining to proper testing of software for security, including the overall strategies and plans. Learners will gain an understanding of the different types of functional and security testing that should be performed, the criteria for testing, concepts related to impact assessment and corrective actions, and the test data lifecycle.
- The **Software Acceptance** module provides an understanding of the requirements for software acceptance, paying specific attention to compliance, quality, functionality, and assurance. Participants will learn about pre- and post-release validation requirements and well as pre-deployment criteria.
- The **Software Deployment, Operations, Maintenance, and Disposal** module provides the learner with knowledge pertaining to the deployment, operations, maintenance, and disposal of software from a secure perspective. This is achieved by identifying processes during installation and deployment, operations and maintenance, and disposal that can affect the ability of the software to remain reliable, resilient, and recoverable in its prescribed manner.
- The **Supply Chain and Software Acquisition** module provides the learner with knowledge on how to perform effective assessments on an organization's cyber-supply chain, and describes how security applies to the supply chain and software acquisition process. Learners will understand the importance of supplier sourcing and being able to validate vendor integrity, from third-party vendors to complete outsourcing. Finally, learners will understand how to manage risk through the adoption of standards and best practices for proper development and testing across the entire lifecycle of products.

- CSSLP Snapshot
- CSSLP certification recognizes the key qualifications of those involved in building secure software. It is the only certification that addresses the need for software and security professionals who possess the knowledge and experience to implement security best practices throughout the software development lifecycle (SDLC).
- CSSLPs understand the importance of secure software and their role in protecting organizations and intellectual property from evolving threats. With an increasing number of attacks exploiting vulnerabilities in software, the demand for professionals with application security expertise is on the rise. CSSLPs have proven their ability to incorporate security - authentication, authorization, encryption, auditing, and more - into each phase of the SDLC and their commitment to staying current with the latest advances in software security.

- What's Required?
- Candidates must have a minimum of 4 years cumulative paid full-time Software Development Lifecycle (SDLC) professional experience in 1 or more of the 8 domains of the CSSLP CBK. Earning a 4-year college degree or regional equivalent will waive 1 year of the required experience. Only a 1 year experience exemption is granted for education.

- What Job Title Do You Have?
- CSSLPs hold a range of titles including software architect, software developer, application security specialist, security manager, IT director, and vice president of IT audit. The certification is relevant to any software and security professional involved in the software development process, from software design and implementation to testing and deployment.

- What's a Typical Day Like for a CSSLP?
- Because CSSLPs represent such a wide cross-section of software and security professionals, the day can vary from person to person. CSSLPs often spend part of their day researching industry events to understand the emerging risks and cyber security landscape, as well as the trending threats, technologies, and exploits and how they may impact applications and associated development processes - from requirements, architecture, and design, to coding, testing, and deployment. Security activities can range from performing security architecture walk-throughs to doing vulnerability assessments, penetration testing, and source code review. CSSLPs with more management responsibilities often provide training for development teams on software security best practices.

- What's Your Job Setting Like?
- CSSLPs often work in team environments as either leaders or highly valued contributors. CSSLPs who work for software providers may be required to travel to customer locations, and those with more IT security-related titles may be found in areas of the organization such as the network operations center.

- What Skill Sets are Most Important to Your Job?
- In addition to possessing the skills to develop software that performs as expected, CSSLPs must have a deep understanding of the security landscape, application vulnerabilities, and evolving ways in which software can be exploited. They also need to know what tools and methodologies are required to effectively address these threats. Curious and creative by nature, CSSLPs are driven to understand how things work so they can help build innovative and secure software. But they must also know how to break things and make them not work. Their knowledge of how hackers can take advantage of code is critical, enabling them to identify vulnerabilities and build more secure software from the start - before any security breaches can occur.

- If a Security Breach were to Take Place, What is Your Role in Handling Remediation and/or Prevention?
- CSSLPs provide critical insight to the security teams in the event of a breach. Their expertise is called upon to quickly diagnose what software assets might be involved and where they are located. More than anyone else, CSSLPs understand the threat vectors and how software can be accessed and potentially used by hackers. Their expertise is vital in helping the response teams swiftly respond and manage the remediation efforts.

Who should obtain the CSSLP certification?

The Certified Secure Software Lifecycle Professional (CSSLP) is for everyone involved in the SDLC. CSSLPs often hold positions such as the following:

- Software Architect
- Software Engineer
- Software Developer
- Application Security Specialist
- Software Program Manager
- Quality Assurance Tester
- Penetration Tester
- Software Procurement Analyst
- Project Manager
- Security Manager
- IT Director/Manager

Globally Recognized Proficiency in Application Security

The CSSLP draws from a comprehensive, up-to-date, global common body of knowledge that ensures software professionals have deep knowledge and understanding of how to build secure software. CSSLP tests one competence in the following 8 domains:

- Secure Software Concepts
- Secure Software Requirements
- Secure Software Design
- Secure Software Implementation/Programming
- Secure Software Testing
- Secure Lifecycle Management
- Software Deployment, Operations, Maintenance
- Supply Chain and Software Acquisition

CSSLP Exam Information

Length of exam	4 hours
Number of questions	175
Question format	Multiple choice questions
Passing grade	700 out of 1000 points

Exam Language	English
Testing center	Pearson Vue Testing Center