301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

View Full Course Details including Latest Schedule Online

(ISC)²

CSSLP (Certified Secure Software Lifecycle Professional)

This training course focuses on how to learn how to incorporate security best practices into every phase of the software development lifecycle.

BONUS! Cyber Phoenix Subscription Included: All Phoenix TS students receive complimentary ninety (90) day access to the Cyber Phoenix learning platform, which hosts hundreds of expert asynchronous training courses in Cybersecurity, IT, Soft Skills, and Management and more!

Course Overview

Official (ISC)²® Training Seminar for the Certified Secure Software Lifecycle Professional (CSSLP®) provides a comprehensive review of the knowledge required to incorporate security practices – authentication, authorization and auditing – into each phase of the Software Development Lifecycle (SDLC), from software design and implementation to testing and deployment. This training course will help students review and refresh their knowledge and identify areas they need to study for the CSSLP exam. Content aligns with and comprehensively covers the eight domains of the (ISC)² CSSLP Common Body of Knowledge (CBK®).

Official courseware is developed by (ISC)² – creator of the CSSLP CBK – to ensure your training is relevant and up-to-date. Our instructors are verified security experts who hold the CSSLP and have completed intensive training to teach (ISC)² content.

This course will fully prepare you for the (ISC)2 ® CSSLP® Certification exam.

Before enrolling in the course, you should have at least four years of experience in Software Development Lifecycle (SDLC) professional work in one or more of the 8 domains of the CSSLP CBK.

Schedule

DATE	LOCATION	
6/17/24 - 6/21/24 (5 days)	**Live Online** Open	Contact Us
9/09/24 - 9/13/24 (5 days)	**Live Online** Open	Contact Us
10/07/24 - 10/11/24 (5 days)	**Live Online** Open	Contact Us

Program Level

Advanced

Training Delivery Methods

Group Live

Duration

5 Days / 32 hours Training

CPE credits

26 NASBA CPE Credits

Field of Study

Information Technology

Advanced Prep

N/A

Course Registration

Candidates can choose to register for the course by via any of the below methods:

- Email: Sales@phoenixts.com
- Phone: 301-582-8200
- Website: www.phoenixts.com

Upon registration completion candidates are sent an automated course registration email that includes attachments with specific information on the class and location as well as pre-course study and test preparation material approved by the course vendor. The text of the email contains a registration confirmation as well as the location, date, time and contact person of the class.

Online enrolment closes three days before course start date.

On the first day of class, candidates are provided with instructions to register with the exam provider before the exam date.

Complaint Resolution Policy

To view our complete Complaint Resolution Policy policy please click here: Complaint Resolution Policy

Refunds and Cancellations

To view our complete Refund and Cancellation policy please click here: Refund and Cancellation Policy

Course Outline

Chapter 1: Secure Software Concepts Domain

- Define core security objectives for software development.
- Describe the information security triad and explain the main mechanisms of confidentiality, integrity and availability of information.
- Characterize the relationship between information security and data privacy.
- Describe accountability, auditing and logging in the context of software security.
- Explain non-repudiation, digital signatures, benefits of code signing and blockchain.
- Understand the foundational concepts behind security design principles with respect to secure software development.

Chapter 2: Secure Software Lifecycle and Risk Management Domain

- Understand and describe OWASP's Software Assurance Maturity Model (OpenSAMM) and Building Security In Maturity Model (BSIMM).
- Define and recognize security configuration standards and benchmarks.
- Understand and describe security-focused configuration management processes.
- Recognize security milestones.
- Explain and illustrate incorporation of software security practices into the SDLC processes.
- Discuss security in predictive and adaptive planning for software development.
- Describe DevOps and DevSecOps.
- Describe System Security Plan.
- Recognize security-relevant documentation.
- Evaluate metrics in software development.
- Recognize attack surface evaluation for measuring security in software.
- Describe software decommissioning, end-of-life policy and processes.
- Discuss data disposition.
- Explain information system continuous monitoring (ISCM).
- Describe security information event management (SIEM).
- Recognize risk management terminology and describe the risk management process.
- Explain regulations and legal aspects pertaining to intellectual properties and security breaches.
- Discuss architectural risk assessment.
- Describe operational risks relevant to integration and deployment environment.
- Recognize the importance of personnel training.
- Describe security champions and discuss the importance of security education and guidance.
- Explain retrospectives and continuous improvement in Agile development environments. Discuss lessons learned with respect to the processes used to build software.

Chapter 3: Secure Software Requirements Domain

- Discuss requirements management and identify sources for software security requirements.
- Recognize functional and nonfunctional requirements and explain the importance of security-focused stories in SCRUM/SCRUM-like methodologies.
- Analyze misuse/abuse cases and recognize their relevance to known attack patterns.
- Describe Security Requirements Traceability Matrix (STRM) and discuss how security requirements flow down to suppliers/providers.
- Analyze security policies and their supporting elements as internal sources for security requirements.
- Explain compliance requirements and recognize laws, regulations and industry standards as external sources for security requirements.
- Discuss security standards and frameworks.
- Describe data governance, explain data ownership, and recognize relevant roles and responsibilities.
- Describe data classification and explain security labeling and marking.

- Recognize data types, structured and unstructured.
- Describe the data lifecycle and explain the process for secure data retention and destruction.
- Discuss privacy risk, recognize privacy laws and regulations, and explain the requirements for safeguarding personal information.
- Discuss data anonymization and enumerate various approaches for anonymization.
- Explain user consent, data retention and data disposition in the context of privacy.
- Recognize implications of cross-border data transfer and restrictions for the transfer of personal data.

Chapter 4: Secure Software Architecture and Design Domain

- Understand common threats; describe the threat modeling process, tools and methodologies and explain the process of attack surface evaluation and management.
- Discuss threat intelligence and describe the sources for cyber threat information.
- Discuss the process of identification and prioritization of security controls and describe security properties and constraints on the design and constraints imposed by the deployment environment.
- Describe various architectures and discuss their security-relevant aspects.
- Describe pervasive computing and IoT, discuss various contactless technologies and discuss their security and privacy aspects.
- Explain embedded software and discuss the update challenge and discuss Field-Programmable Gate Array (FPGA) and microcontroller security.
- Explain cloud computing, service models and deployment models, and describe the shared security responsibility model. Discuss mobile applications security.
- Discuss hardware platform concerns, side channel mitigation, speculative execution mitigation, and Hardware Security Modules (HSM).
- Explain cognitive computing, machine learning and artificial intelligence.
- Discuss control systems and their applications in various areas and safety criticality aspects.
- Evaluate security criteria of interfaces, out-of-band management and log interfaces.
- Understand upstream and downstream dependencies, protocol design choices and their security ramifications.
- Describe various authentication and authorization mechanisms; explain credential management and the digital certificate standard.
- Discuss flow controls and data loss prevention; compare and contrast virtual machines and containers.
- Explain the trusted computing base (TCB) and the trusted platform module (TPM).
- Discuss database security, programming language environment, and operating system controls and services.
- Discuss secure architecture and secure design principles, and explain secure design patterns.
- Explain verification of the design, formal and informal secure code reviews and the code inspection process.

Chapter 5: Secure Software Implementation Domain

- Explain the need for establishing and enforcing secure coding standards.
- Describe different approaches for implementing security in managed applications.
- Describe common flaws in software and corresponding mitigation strategies.
- Discuss input validation, output encoding, authentication, session management, access control, cryptographic practices, error and exception management practices and logging.
- Explain type safety, memory management and isolation
- Discuss cryptography, applications to transit and storage, cryptographic agility, cryptographic libraries and encryption algorithm selection.
- Explain access control, trust zones and function permissions.
- Explain vulnerability databases and lists.
- Discuss Common Vulnerabilities and Exposures (CVE), Common Weakness Enumerations (CWE) and Common Attack Pattern Enumeration and Classification (CAPEC).
- Enumerate OWASP Top 10 Web Application Security Risks.
- Describe categorization of controls by type and by function.
- Describe controls to prevent common web application vulnerabilities
- Describe OWASP Proactive Controls and critical focus areas around building secure software.
- Evaluate the risks associated with using third-party and open-source components and libraries.
- Describe Software Composition Analysis (SCA) and open source management.
- Discuss OWASP Dependency Check and Dependency Track.
- Discuss API integration and evaluate the security aspects.
- Describe system-of-systems.

Chapter 6: Secure Software Testing Domain

- Explain functional and nonfunctional security testing, purpose and the phases in penetration testing fuzzing and its variations and limitations.
- Explain vulnerability scanning and content scanning.
- Discuss simulation, understand configuration drifts in development environments and describe real user monitoring and synthetic monitoring.
- Describe fault injection, stress testing and break testing.
- Describe various types of functional testing, including unit testing, integration testing and regression testing.
- Describe various types of nonfunctional testing, including scalability, interoperability and performance testing.
- Describe cryptographic validation and explain Pseudo-Random Number Generators and entropy.
- Explain test strategy and describe functional and nonfunctional testing.
- Explain the relationship between use cases and misuse and abuse cases and the importance of creating misuse and abuse cases.
- Explain test strategy and describe functional and nonfunctional testing.
- Describe test cases and test harness.

- Explain black-box and white-box testing, objectives and code coverage.
- Discuss application security testing (AST) methods and explain their benefits and limitations.
- Discuss manual code reviews and describe searching for embedded malicious code.
- Recognize software security-relevant standards, explain crowdsourcing benefits and concerns and discuss bug bounty.
- Explain the security implications of test results on product management and prioritization of remediation efforts.
- Explain break-build criteria.
- Describe the process of tracking security defects.
- Explain risk scoring, and the Common Vulnerability Scoring System (CVSS).
- Explain generation of test data, security of test data, ramifications of using production data in the test environment and database referential integrity and constraints.
- Describe the process of verification and validation testing and explain acceptance testing.
- List various software documentation and explain undocumented functionality.
- Describe OWASP's Application Security Verification Standard (ASVS), its structure and its goals.

Chapter 7: Secure Software Deployment, Operations and Maintenance Domain

Learning Objectives

- Explain secure integration, build and deployment.
- Describe the secure software toolchain.
- Describe build artifacts and discuss mobile application and platform security.
- Describe security data, including credentials, keys and certificates and discuss ramifications of failing to protect them in production.
- Describe vaults used to manage secrets and discuss key vault considerations.
- Describe the secure bootstrapping process, hardening and the least privilege principle with respect to secure software installation.
- Explain secure software activation methods and security policy implementation with respect to secure software installation.
- Describe the Authorization to Operate (ATO) process and the steps involved.
- Explain risk acceptance.
- Explain post-deployment verification, issue tracking and testing constraints.
- Describe security testing automation.
- Describe the benefits of information security continuous monitoring(ISCM)and list some considerations for its implementation.
- Describe events, logs and threat intelligence.
- Explain computer security incidents, incident response and forensics.
- Describe incident precursors and indicators, monitoring logs and alerts and root-cause analysis.
- Describe security patch management and explain the timing, prioritization and testing aspects of security patches.
- Describe vulnerability management and vulnerability scan tools.

- Explain the operations of web application firewalls.
- Explain locality of reference, address space layout randomization and data execution prevention.
- Explain continuity of operations, business impact analysis, data backup and restore and data archiving.
- Discuss disaster recovery (DR), data residency requirement aspect of DR, resiliency and erasure code.

Chapter 8: Secure Software Supply Chain Domain

- Describe the software supply chain.
- Recognize participants in the supply chain.
- Explain software supply chain risk management.
- Explain security risks associated with third party/open source code and recognize OWASP's Software Component Verification Standard (SCVS).
- Describe software supply chain attacks.
- Explain the risks associated with peer-to-peer applications and file sharing.
- Explain code repository and build environment security.
- Explain cryptographically hashed, digitally signed components.
- Describe security in the acquisition process and audit of security policy compliance.
- Explain third-party vulnerability/incident notification and reporting and maintenance and support structure.
- Explain commercial and open-source software licenses.
- Explain vendor/supplier security track record in acquisition and the right-to-audit clause in contracts.
- Explain contractual requirements for intellectual property(IP) ownership inout sourcing relationships, code escrow, liability, warranty and service-level agreements (SLAs).

Chapter 9: Applied Scenario Activities

Learning Objectives

- Apply security through the SDLC via animated video-based scenarios and corresponding activities.

Exam Information

CSSLP Certification Exam Details:

In order to take the CSSLP certification exam, candidates must register with (ISC)^2.

- Number of questions: 175
- Passing score: 700 points or greater
- Test duration: 4 Hours

- Test format: Multiple choice
- Test delivery: Pearson Vue

CSSLP Certification Exam Domains:

- Domain 1: Secure Software Concepts
- Domain 2: Secure Software Requirements
- Domain 3: Secure Software Architecture and Design
- Domain 4: Secure Software Implementation
- Domain 5: Secure Software Testing
- Domain 6: Secure Software Lifecycle Management
- Domain 7: Secure Software Deployment, Operations, Maintenance
- Domain 8: Secure Software Supply Chain

Finance your CSSLP Training!

We have partnered with Meritize to provide our students with financing options to fund your education. Check your loan options in minutes without impacting your credit score. Click here to apply

CSSLP Certification Training FAQs

What is the average salary for a CSSLP?

According to payscale.com, the average salary for a professional with a CSSLP Certification earns $107,000 annually.

Who should take CSSLP Certification Training?

This course is ideal for software architects, engineers, developers and procurement analysts, as well as, application security specialists, software program managers, quality assurance testers and penetration testers.

What is the CSSLP Certification

The CSSLP certification validates that the certified professional has the expertise to include the best security practices, auditing, and authorization into each phase of the Software Development Lifecycle (SDLC). You can learn more about in our blog post What Is The CSSLP Certification?

BONUS! Cyber Phoenix Subscription Included: All Phoenix TS students receive complimentary ninety (90) day access to the Cyber Phoenix learning platform, which hosts hundreds of expert asynchronous training courses in Cybersecurity, IT, Soft Skills, and Management and more!

Phoenix TS is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints re-garding registered sponsors may be submitted to the National Registry of CPE Sponsors through its web site: www.nasbaregistry.org

301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

Starting at **$3,084**

ATTENTION

For GSA pricing or Contractor quotes call 301-258-8200 – Option 2.

GSA

Price Match Guarantee

We'll match any competitor's price quote. Call us at 240-667-7757.

This **CSSLP Certification Training** course includes:

- 5 days of instructor-led training
- ISC2 CSSLP Exam Voucher
- ISC2 CSSLP Certification practice exams
- ISC2 CSSLP Certification Exam guide
- CSSLP Certification Exam onsite scheduling
- Certificate of completion for up to 40 CEUs/CPEs to be used toward renewing relevant certifications
- CSSLP Certification Training course retake guarantee
- CSSLP satisfies DOD 8570-.01-M requirements for IASAE I
- The CSSLP Certification follows the NICE Cybersecurity Workforce Framework

10420 Little Patuxent Parkway Suite 500 Columbia, MD 21044

- Notepad, pen and highlighter
- Variety of bagels, fruits, doughnuts and cereal available at the start of class*
- Tea, coffee and soda available throughout the day*
- Freshly baked cookies every afternoon*

**denotes this benefit is only available at participating locations.*