INFOSEC Skills
LIVE BOOT CAMPS

Get live, expert instruction from anywhere.

(ISC)² CSSLP Boot Camp

Become an (ISC)² Certified Secure Software Lifecycle Professional (CSSLP). You'll leave this boot camp with the knowledge and expertise needed to apply best practices to each phase of the software development lifecycle — from design and implementation to testing and deployment.

Course description

Infosec's CSSLP Boot Camp teaches you how to incorporate security practices throughout the software development lifecycle. You'll learn key policies, procedures and best practices related to secure software development and how to incorporate them into each phase of the development lifecycle.

You'll leave fully prepared to earn your CSSLP certification and prove to employers that you have the knowledge and skills necessary to implement secure software development and help mitigate cyber threats.

Who should attend

- Software developers
- Software architects
- Software engineers
- Application security specialists
- Penetration testers
- Project managers
- Anyone involved in the software development lifecycle (SDLC)

Boot camp at a glance

What you'll learn

- ✓ Secure software concepts, requirements and design
- ✓ Incorporating authentication, authorization and auditing
- ✓ Supply chain, software acquisition and more!

Delivery methods

- ✓ Online
- ✓ In person
- ✓ Team onsite

Training duration

- ✓ Immediate access to Infosec Skills
- ✓ 5-day boot camp, plus a day to take the exam
- ✓ 90-day extended access to all boot camp materials

The hands-on cybersecurity training platform that moves as fast as you do

Infosec Skills boot camps are engineered to match the way today's cybersecurity professionals prefer to learn. In addition to days of live training from an experienced pro, you'll get unlimited access to 100s of additional hands-on cybersecurity courses and cyber ranges to help you advance your skills before, during and after your boot camp. Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, or get a head start on your next certification goal.

Start training immediately

Prepare for your boot camp with immediate access to the Infosec Skills on-demand training library.

Learn by doing in the cyber range

Put what you've learned into practice with 100s of browser-based labs and hands-on projects.

Get unlimited custom practice exams

Uncover knowledge gaps with unlimited practice exams attempts and skill assessments.

700+ IT and security courses

Earn CPEs and build new skills with 100s of additional training courses.

What's included

- Five days of live, expert CSSLP instruction
- Exam Pass Guarantee
- Exam voucher
- 100% Satisfaction Guarantee
- Free 90-day Infosec Skills subscription (access to 1,400+ additional courses and labs)
- 90-day extended access to all boot camp video replays and materials
- Knowledge Transfer Guarantee

Prerequisites

In order to obtain the CSSLP certification, you must have:

- At least four years of professional Software Development Lifecycle (SDLC) experience
- A work history reflecting direct experience in at least one of the eight domains listed in the (ISC)² CSSLP Common Body of Knowledge (CBK)

However, you can become an Associate of (ISC)² by passing the exam without the required work experience.

CSSLP objectives

This boot camp prepares you to pass the (ISC)² CSSLP exam, which covers eight domain areas required for the daily job functions of software professionals:

- Secure software concepts: Core concepts and secure design principles for controlling the behavior, use and content of the system
- Secure software requirements: Capturing functional and non-functional security requirements in the requirements gathering phase
- Secure software architecture and design: Translating security requirements into application design elements
- Secure software implementation: Applying secure coding and testing standards and tools to avoid introducing security vulnerabilities
- Secure software testing: Testing for security functionality and resiliency to attack
- Secure software lifecycle management: Strengthening the overall security posture of the software
- Secure software deployment, operations, maintenance: Security issues around steady-state operations and management of software
- Secure software supply chain: Provides a holistic outline of the knowledge and tasks required in managing risk for outsourced development, acquisition and procurement of software and related services

Learn from experts

We don't just have great instructors, our instructors have years of industry experience and are recognized as experts. Over the past 15 years, we've helped tens of thousands of students get certified and advance their careers.

Industry-leading exam pass rates

Infosec's courseware materials are always up to date and synchronized with the latest CSSLP exam objectives. Our industry-leading curriculum and expert instructors have led to the highest pass rates in the industry. More than 93% of Infosec students pass their certification exams on their first attempt.

Skill up and get certified, guaranteed

Exam Pass Guarantee

If you don't pass your exam on the first attempt, get a second attempt for free. Includes the ability to re-sit the course for free for up to one year.

100% Satisfaction Guarantee

If you're not 100% satisfied with your training at the end of the first day, you may withdraw and enroll in a different online or in-person course.

Knowledge Transfer Guarantee

If an employee leaves within three months of obtaining certification, Infosec will train a different employee for free for up to one year.

What our students are saying

I really appreciate that our instructor was extremely knowledgeable and was able to provide the information in a way that it could be understood. He also provided valuable test-taking strategies that I know not only helped me with this exam, but will help in all exams I take in the future.

Michelle Jemmott
Pentagon

Excellent! Our instructor had a vast background and related the materials to real life. Much better than just teaching the materials to pass an exam … but he did that as well. He went out of his way in class. The extra materials really benefited us when we returned to our real jobs! Great experience!

John Peck
EPA

Very impressed with Infosec. My instructor did a great job delivering the information strategically and in a way for all to understand. I would definitely take another class/certification prep course.

Sylvia Swinson
Texeltek

The instructor was able to take material that prior to the class had made no sense, and explained it in real world scenarios that were able to be understood.

Erik Heiss
United States Air Force

The course was extremely helpful and provided exactly what we needed to know in order to successfully navigate the exam. Without this I am not confident I would have passed.

Robert Caldwell
Salient Federal Solutions

(ISC)² CSSLP details

Our instructors give you 100% of their time and dedication to ensure that your time is well spent. You receive an immersive experience with no distractions! The typical daily schedule is:

	Day 1	Day 2	Day 3	Day 4	Day 5	Day 6
Morning session	Secure software concepts	Secure software architecture and design	Secure software implementation	Secure software testing	Secure software deployment, operations, maintenance	Take the CSSLP exam
Afternoon session	Secure software requirements	Secure software architecture and design	Secure software implementation	Secure software lifecycle management	Secure software supply chain	
Evening session	Optional group & individual study	Optional group & individual study	Optional group & individual study	Optional group & individual study	Optional group & individual study	

Schedule may vary from class to class

Before your boot camp

Start learning now. You'll get immediate access to all the content in Infosec Skills, including an in-depth CSSLP prep course, the moment you enroll. Prepare for your live boot camp, uncover your knowledge gaps and maximize your training experience.

During your boot camp

Secure software concepts

- Core concepts
- Security design principles

Secure software requirements

- Define software security requirements
- Identify and analyze compliance requirements
- Identify and analyze data classification requirements
- Identify and analyze privacy requirements
- Develop misuse and abuse cases
- Develop security requirement traceability matrix (SRTM)
- Ensure security requirements flow down to suppliers/providers

Secure software architecture and design

- Perform threat modeling
- Define the security architecture
- Performing secure interface design
- Performing architectural risk assessment
- Modeling (non-functional) security properties and constraints
- Model and classify data

- Evaluate and select reusable secure design
- Perform security architecture and design review
- Define secure operational architecture (e.g., deployment topology, operational interfaces)
- Use secure architecture and design principles, patterns and tools

Secure software implementation

- Adhere to relevant secure coding practices (e.g., standards, guidelines and regulations)
- Analyze code for security risks
- Implement security controls (e.g., watchdogs, file integrity monitoring (FIM), anti-malware)
- Address security risks (e.g. remediation, mitigation, transfer, accept)
- Securely reuse third-party code or libraries (e.g., software composition analysis (SCA))
- Securely integrate components
- Apply security during the build process

Secure software testing

- Develop security test cases
- Develop security testing strategy and plan
- Verify and validate documentation (e.g., installation and setup instructions, error messages, user guides, release notes)
- Identify undocumented functionality
- Analyze security implications of test results (e.g., impact on product management, prioritization, break build criteria)
- Classify and track security errors
- Secure test data
- Perform verification and validation testing

Secure software lifecycle management

- Secure configuration and version control (e.g., hardware, software, documentation, interfaces, patching)
- Define strategy and roadmap
- Manage security within a software development methodology
- Identify security standards and frameworks
- Define and develop security documentation
- Develop security metrics (e.g., defects per line of code, criticality level, average remediation time, complexity)
- Decommission software
- Report security status (e.g., reports, dashboards, feedback loops)
- Incorporate integrated risk management (IRM)
- Promote security culture in software development
- Implement continuous improvement (e.g., retrospective, lessons learned)

Software software deployment, operations and maintenance

- Perform operational risk analysis
- Release software securely
- Securely store and manage security data
- Ensure secure installation
- Perform post-deployment security testing
- Obtain security approval to operate (e.g., risk acceptance, sign-off at appropriate level)
- Perform information security continuous monitoring (ISCM)
- Support incident response
- Perform patch management (e.g. secure release, testing)
- Perform vulnerability management (e.g., scanning, tracking, triaging)
- Runtime protection (e.g., runtime application self-protection (RASP), web application firewall (WAF), address space layout randomization (ASLR))
- Support continuity of operations
- Integrate service level objectives (SLO) and service level agreements (SLA) (e.g., maintenance, performance, availability, qualified personnel)

Secure software supply chain

- Implement software supply chain risk management
- Analyze security of third-party software
- Verify pedigree and provenance
- Ensure supplier security requirements in the acquisition process
- Support contractual requirements (e.g., intellectual property (IP) ownership, code escrow, liability, warranty, end-user license agreement (EULA), service level agreements (SLA))

After your boot camp

Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, get a head start on your next certification goal or start earning CPEs.

About Infosec

Infosec's mission is to put people at the center of cybersecurity. We help IT and security professionals advance their careers with skills development and certifications while empowering all employees with security awareness and phishing training to stay cyber-safe at work and home. Learn more at infosecinstitute.com.

INFOSEC