Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

CSSLP - Certified Secure Software Life cycle Professional

CSSLP is the only certification in the industry designed to validate an individual’s competency in incorporating security into each phase of the software lifecycle - that will help mitigate application vulnerability threats. SecureNinja's CSSLP (Certified Secure Software Lifecycle Professional) training and certification boot camp in Washington, DC, San Diego, CA and Columbia, MD, covers the exam objectives that measure security best practices and industry standards for the software lifecycle - critical information to a CSSLP. This is where you will learn tools and processes on how security should be built into 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. This 5-day immersive boot camp covers all of the latest exam objectives complete taught by a master of the CSSLP.

CSSLP Benefits

As a CSSLP, you will be seen as a leader in your organization. A status you'll rightly deserve because you'll understand how to:

- Break the penetrate and patch testing approach
- Reduce production costs, 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

Topics Covered

The CSSLP examination tests the breadth and depth of a candidate’s knowledge by focusing on the seven domains which comprise the CSSLP, taxonomy of information security topics:

- **Secure Software Concepts** - Security implications in software development and for software supply chain integrity
- **Secure Software Requirements** - Capturing security requirements in the requirements gathering phase
- **Secure Software Design** - Translating security requirements into application design elements
- **Secure Software Implementation/Coding** - Unit testing for security functionality and resiliency to attack, and developing secure code and exploit mitigation
- **Secure Software Testing** - Integrated QA testing for security functionality and resiliency to attack
- **Software Acceptance** - Security implication in the software acceptance phase
- **Software Deployment, Operations, Maintenance, and Disposal** - Security issues around steady-state operations and management of software

Web: www.secureninja.com
Phone: 703.535.8600
Email: info@secureninja.com

Who Should Attend

Each software lifecycle (SLC) stakeholder is responsible for a certain phase(s) of the SLC, but all phases must have security built into them. CSSLP is for all the stakeholders involved in the process. Each of the 7 Domains of the CSSLP covers how to build security into the different phases.

CSSLP stakeholders include:

- Auditors
- Top Management
- Business Unit Heads
- IT Manager
- Security Specialists
- Application Owners
- Developers & Coders
- Project Managers Team Leads
- Technical Architects
- Quality Assurance Managers
- Business Analysts
- Industry Group Delivery Heads
- Client-Side PM

Prerequisites

CSSLP is for everyone involved in the Software Lifecycle with at least 4 years of experience.

Required Exam

ISC2 CSSLP Exam

- Format: 125 multiple-choice questions.
- Duration: 3 hours.
- Passing Score: 700 out of 1000 points.

Course Length

- 5 Days
- 40 hours

Follow-on Courses

CISSP