

CSSLP — Certified Secure Software Lifecycle Professional Preparation Training

Delivered from Hacky Security's own curriculum, by instructors who also work our security operations centre. Classroom, online live, or at your office.

PROFESSIONAL

32 HOURS

4 DAYS

At a glance

COURSE	CSSLP — Certified Secure Software Lifecycle Professional	WHAT IS INCLUDED ✓ Instructor-led delivery by practitioners who also work our SOC ✓ Hands-on lab access for the duration of the course ✓ Course materials and lab guides ✓ Hacky Security certificate of completion ✓ Post-course support by email
TRACK	ISC2	
DOMAIN	Cyber Security	
LEVEL	Professional	
DURATION	32 hours (about 4 days)	
DELIVERY	Classroom · Online live · On-site at your office	
LANGUAGE	English	
CLASS SIZE	Small cohorts — everyone gets lab time	

Who this is for

This is a professional course. It suits people already working in or moving into Cyber Security who want structured, hands-on preparation rather than a video library. If you are unsure whether the level fits your team, send us the job titles and we will tell you honestly — including if a different course would serve you better.

Course outline

About this course map

CSSLP — Certified Secure Software Lifecycle Professional — is ISC2's certification for the place most vulnerabilities are actually born: the software development lifecycle. It is not a penetration-testing certification and not a management one. It sits with the people who build software — developers, architects, engineers, and the security professionals who work alongside them — and it covers how to bake security into every stage, from the first requirement to the retirement of the system.

The premise is simple and correct: a flaw caught in design costs a fraction of the same flaw caught in production, and almost every expensive breach traces back to a decision made early and cheaply. CSSLP is the credential that proves someone thinks about security across the whole lifecycle rather than bolting it on at the end.

This preparation programme follows the eight CSSLP domains, each mapped to a phase of the lifecycle it governs.

Domain 01 — Secure software concepts

The principles every later domain applies.

- Core security concepts: confidentiality, integrity, availability, and the rest
- Security design principles: least privilege, defence in depth, secure defaults, fail securely
- Risk management as it applies to software
- Regulatory, privacy and compliance drivers for secure development

Domain 02 — Secure software requirements

Security starts before a line of code is written.

- Deriving security requirements from business and regulatory needs
- Data classification and its consequences for the design
- Abuse cases: specifying how the system must resist misuse
- Building security acceptance criteria into the requirements

Domain 03 — Secure software architecture and design

Designing a system that is secure by construction.

- Threat modelling: finding the weaknesses before they are built
- Secure design patterns and architectural risk analysis
- Designing authentication, authorisation and session management properly
- Security in the architecture of distributed and cloud systems

Domain 04 — Secure software implementation

Writing the code without the classic flaws.

- The common vulnerability classes and how they enter code
- Secure coding practices across languages
- Input validation, output encoding and safe error handling
- Managing secrets, and the risks of third-party and open-source components

Domain 05 — Secure software testing

Proving the security, not assuming it.

- Security test planning and case design
- Static and dynamic analysis, and where each finds what
- Penetration testing and fuzzing as part of the lifecycle
- Interpreting results and tracking remediation

Domain 06 — Secure software lifecycle management

Running the whole thing as a repeatable process.

- Integrating security into the development methodology, Agile included
- Configuration and change management
- Security metrics: measuring whether the programme works
- Retirement and secure decommissioning of software

Domain 07 — Secure software deployment, operations and maintenance

Security does not end at release.

- Secure deployment and hardening of the runtime environment
- Operational monitoring and incident handling for the application
- Patch and vulnerability management over the system's life
- Continuity and the security of the operational pipeline

Domain 08 — Secure software supply chain

The domain that has become the story of the last several years.

- Supplier and third-party risk in the software you ship
- Managing open-source and component risk
- Integrity of the build and release pipeline
- Software provenance and the bill of materials

Sitting the official exam

Exam voucher sold separately. We buy it from the certification body on your behalf and send you the code — you book your own exam date. This course is Hacky Security's own preparation training. The certification itself is awarded by the certification body, not by us.

Investment

Priced per cohort. Tell us how many people and which delivery mode and we will send a quote the same working day.

Book this course

Tell us how many people, where, and when — we will come back with dates and a quote within one working day.

+91-8091900310 • info@hackysecurity.com

<https://hackysecurity.com/courses/csslp/>

CHANDIGARH • SHIMLA • DELHI • DUBAI • LONDON

Independent preparation training delivered from Hacky Security's own curriculum. Hacky Security Private Limited is not affiliated with or endorsed by the certification body named in this document. Certification names and codes are the trademarks of their respective owners and are used only to describe what this course prepares you for. Prices, durations and outlines are indicative and may change; the quotation we send you is the binding one. Issued 19 September 2026.