CYBER SECURITY

Certified Secure Software Lifecycle Professional (CSSLP®)

LENGTH	PRICE (Excl. GST)
5 days	**NZD 3850**

WHY STUDY THIS COURSE

Gain the core knowledge and learn the best security practices for the software development lifecycle (SDLC) and prepare for globally recognised CSSLP® secure software development certification. It is a proven way to build your career and better incorporate security practices into each phase of the SDLC.

CSSLP certification recognises leading application security skills. It shows employers and peers you have the advanced technical skills and knowledge necessary for authentication, authorisation and auditing throughout the SDLC using best practices, policies and procedures established by the cybersecurity experts at ISC2.

CSSLP meets the stringent requirements of ANSI/ISO/IEC Standard 17024.

Please note: The exam is not included in the course fee but can be purchased separately. Please contact us for a quote.

Introducing Certified Secure Software Lifecycle Professional (CSSLP®)
Can't see the video above? Click here to open it in a new screen.

ISC2 AT LUMIFY WORK

ISC2: The world's leading cyber security and IT security professional organisation. Lumify Work is one of only a few select training providers in Australia with campuses in New Zealand and the Philippines. We offer official ISC2 courses and training materials.

ISC2
OFFICIAL TRAINING
PREFERRED
PARTNER

CYBER SECURITY

Certified Secure Software Lifecycle Professional (CSSLP®)

COURSE SUBJECTS

WHAT YOU'LL LEARN

The broad spectrum of topics included in the CSSLP Common Body of Knowledge (CBK®) ensure its relevancy across all disciplines in the field of information security.

The Certified Secure Software Lifecycle Professional (CSSLP) validates that software professionals have the expertise to incorporate security practices – authentication, authorisation and auditing – into each phase of the software development lifecycle (SDLC), from software design and implementation to testing and deployment.

This course provides in-depth coverage of the eight domains required to prepare for the CSSLP exam. Refer to the CSSLP Exam Outline for a deeper dive into the CSSLP domains.

1. Secure Software Concepts

- Core Concepts
- Security Design Principles

2. Secure Software Requirements

- Define Software Security Requirements
- Identify and Analyse Compliance Requirements
- Identify and Analyse Data Classification Requirements
- Identify and Analyse Privacy Requirements
- Develop Misuse and Abuse Cases
- Develop Security Requirement Traceability Matrix (STRM)
- Ensure Security Requirements Flow Down to Suppliers/Providers

3. Secure Software Architecture and Design

- Perform Threat Modeling
- Define the Security Architecture
- Performing Secure Interface Design
- Performing Architectural Risk Assessment
- Model (Non-Functional) Security Properties and Constraints
- Model and Classify Data

https://www.lumifywork.com/en-nz/courses/certified-secure-software-lifecycle-professional-csslp/

> *My instructor was great being able to put scenarios into real world instances that related to my specific situation.*
>
> *I was made to feel welcome from the moment I arrived and the ability to sit as a group outside the classroom to discuss our situations and our goals was extremely valuable.*
>
> *I learnt a lot and felt it was important that my goals by attending this course were met.*
>
> *Great job Lumify Work team.*

AMANDA NICOL
IT SUPPORT SERVICES MANAGER - HEALTH WORLD LIMITED

- 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

4. Secure Software Implementation

- Adhere to Relevant Secure Coding Practices (e.g., standards, guidelines and regulations)
- Analyse 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

5. 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
- Analyse Security Implications of Test Results (e.g., impact on product management, prioritisation, break build criteria)
- Classify and Track Security Errors

Lumify Work Customised Training

We can also deliver and customise this training course for larger groups saving your organisation time, money and resources.

For more information, please contact us on 0800 835 835.

- Secure Test Data
- Perform Verification and Validation Testing

6. 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)

7. Secure Software Deployment, Operations, 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 Randomisation (ASLR))
- Support Continuity of Operations
- Integrate Service Level Objectives (SLO) and Service Level Agreements (SLA) (e.g., maintenance, performance, availability, qualified personnel)

8. Secure Software Supply Chain

- Implement Software Supply Chain Risk Management
- Analyse 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))

CYBER SECURITY

Certified Secure Software Lifecycle Professional (CSSLP®)

WHO IS THE COURSE FOR?

The ISC2 CSSLP is ideal for software development and security professionals responsible for applying best practices to each phase of the SDLC – from software design and implementation to testing and deployment – including those in the following positions:

- 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

PREREQUISITES

To qualify for this certification, you must pass the exam and have at least four years of cumulative, paid work experience as a software development lifecycle professional in one or more of the eight domains of the ISC2 CSSLP Common Body of Knowledge.

A relevant four-year degree can satisfy one year of required experience. Learn more about the ISC2 CSSLP Experience Requirements.

A candidate who doesn’t have the required experience to become a CSSLP may become an Associate of ISC2 by successfully passing the CSSLP exam. An Associate of ISC2 can then accumulate the necessary work experience to achieve full certification.

The supply of this course by Lumify Work is governed by the booking terms and conditions. Please read the terms and conditions carefully before enrolling in this course, as enrolment in the course is conditional on acceptance of these terms and conditions.

https://www.lumifywork.com/en-nz/courses/certified-secure-software-lifecycle-professional-csslp/