Manuals+ — User Manuals Simplified.

Lumify Work CSSLP Certified Secure Software Lifecycle Professional Instruction Manual

Contents

Lumify Work CSSLP Certified Secure Software Lifecycle Professional

Product Information

Specifications

- Length: 5 days
- Provider: Lumify Work
- Accreditation: ISC2 (International Information System Security Certification Consortium)
- Certification: CSSLP (Certified Secure Software Lifecycle Professional)
- Website:

  https://www.lumifywork.com/en-ph/courses/certified-secure-software-lifecycle-professional-csslp/
- Email:
- Social Media:
    - Facebook: **facebook.com/LumifyWorkPh**
    - LinkedIn: **linkedin.com/company/lumify-work-ph**
    - Twitter: **twitter.com/LumifyWorkPH**
    - YouTube: **youtube.com/@lumifywork**

Why Study This Course?

The CSSLP certification recognizes leading application security skills. It demonstrates advanced technical skills and knowledge in authentication, authorization, and auditing throughout the Software Development Lifecycle (SDLC) using best practices established by cybersecurity experts at ISC2. By obtaining this certification, it showcases your expertise to employers and peers.

Course Content

The course covers the following topics:

1. Secure Software Concepts

- Core Concepts
  - Security Design Principles
2. 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 (ST RM)
  - Ensure Security Requirements Flow Down to Suppliers/Providers
3. Secure Software Architecture and Design
  - Perform Threat Modeling
  - Define the Security Architecture
  - Perform Secure Interface Design
  - Perform Architectural Risk Assessment Model (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
4. Secure Software Implementation
  - Adhere to Relevant Secure Coding Practices (e.g., standards, guidelines, and regulations)

Lumify Work Customized Training

Lumify Work offers the option to deliver and customize this training course for larger groups, saving organizations time, money, and resources. For more information, please contact us at 02 8286 9429.

Product Usage Instructions

Course Enrollment

To enroll in the CSSLP certification course, please follow these steps:

1. Visit the Lumify Work website: **https://www.lumifywork.com/en-ph/courses/certified-secure-software-lifecycle-professional-csslp/**
2. Click on the "Enroll Now" button.
3. Fill out the enrollment form with your personal information.
4. Choose the desired course dates and location.
5. Submit the form and proceed to payment.

Certification Exam

Please note that the certification exam is not included in the course fee. It can be purchased separately. To inquire

about the exam and obtain a quote, please contact us at

FAQ

- Q: What is the duration of the CSSLP certification course?

  A: The course has a duration of 5 days.
- Q: Who is the accrediting body for this course?

  A: The CSSLP certification is accredited by ISC2 (International Information System Security Certification Consortium).
- Q: Can the course be customized for larger groups?

  A: Yes, Lumify Work offers customized training options for larger groups. This can save organizations time, money, and resources. For more information, please contact us at 02 8286 9429.

CYBER SECURITY
Certified Secure Software Lifecycle Professional (CSSLP®)

ISC2 AT LUMIFY WORK
ISC2: The world's leading cyber security and IT security professional organization. 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

LENGTH

- 5 days

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 recognizes leading application security skills. It shows employers and peers you have the advanced technical skills and knowledge necessary for authentication, authorization 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 on a new screen.
https://www.lumifywork.com/en-ph/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 / 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 learned a lot and felt it was important that my goals by attending this course were met. Great job Lumity Work team.

AMANDA NICOL IT SUPPORT SERVICES MANAGER – HEALTH WORLD LIMITED

Secure Software Concepts

- Core Concepts
- Security Design Principles

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

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
- 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)
- 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, acceptance)
- 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 a 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, prioritization, break build criteria)
- Classify and Track Security Errors
- Secure Test Data
- Perform Verification and Validation Testing

Lumify Work

- Customized Training We can also deliver and customise this training course for larger groups saving your organisation time, money and resources.
- For more information, please get in touch with us on 02 8286 9429.

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)

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)

Secure Software Supply Chain

- Implement Software Supply Chain Risk Management
- Analyse the 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))

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

We can also deliver and customise this training course for larger groups – saving your organization time, money, and resources. For more information, please contact us via email on **ph.training@lumifywork.com**

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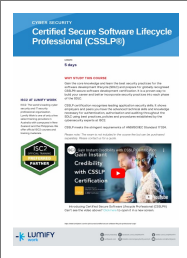
The supply of this course by Lumify Work is governed by the booking terms and conditions. Please read the terms and conditions carefully before enrolling in this course, as enrolment in the cours e is conditional on acceptance of these terms and conditions

https://www.lumifywork.com/en-ph/courses/certified-secure-software-lifecycle-professional-css/p/

Documents / Resources

	Lumify Work CSSLP Certified Secure Software Lifecycle Professional [pdf] Instruction Manual CSSLP Certified Secure Software Lifecycle Professional, CSSLP, Certified Secure Software Lifecycle Professional, Software Lifecycle Professional, Lifecycle Professional

References

- 🔹 **Lumify Work | Lumify Work AU**
- 🌐 **ywork.com**
- 🔹 **Lumify Work | Lumify Work AU**
- ❷ **CSSLP Experience Requirements**
- 🔹 **Lumify Work | Lumify Work AU**
- 🔹 **Associate of ISC2 | Lumify Work PH**
- 🔹 **ISC2 CSSLP & Certified Secure Software Lifecycle Professional | Lumify Work | Lumify Work PH**
- **User Manual**