Certified Secure Software Lifecycle Professional (CSSLP)

Duration 5 days

COURSE DESCRIPTION

The Certified Secure Software Lifecycle Professional (CSSLP) validates that software professionals have the expertise to incorporate security practices – authentication, authorization and auditing – into each phase of the software development lifecycle (SDLC), from software design and implementation to testing and deployment. 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. Successful candidates are competent in the following eight domains:

- Secure Software Concepts
- Secure Software Requirements
- Secure Software Architecture and Design
- Secure Software Implementation
- Secure Software Testing
- Secure Software Lifecycle Management
- Secure Software Deployment, Operations, Maintenance
- Secure Software Supply Chain

COURSE OUTLINE

Domain 1: Secure Software Concepts

- Core Concept
- Security Design

Domain 2: Secure Software Requirements

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

Domain 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
- Evaluate and Select Reusable Secure Design
- Perform Security Architecture and Design Review
- Define Secure Operational Architecture
- Use Secure Architecture and Design Principles, Patterns, and Tools

Domain 4: Secure Software Implementation

- Adhere to Relevant Secure Coding Practices
- Analyzing Code for Security Risks
- Implement Security Controls
- Address Security Risks
- Securely Reuse Third-Party Code or Libraries
- Securely Integrate Components
- Apply Security During the Build Process

Domain 5: Secure Software Testing

- Develop Security Test Cases
- Develop Security Testing Strategy and Plan
- Verify and Validate Documentation
- Identify Undocumented Functionality
- Analyzing Security Implications of Test Results
- Classify and Track Security Errors
- Secure Test Data
- Perform Verification and Validation Testing

Domain 6: Secure Software Lifecycle Management

- Secure Configuration and Version Control
- Define Strategy and Roadmap
- Manage Security Within a Software Development Methodology
- Identify Security Standards and Frameworks
- Define and Develop Security Documentation
- Develop Security Metrics
- Decommission Software
- Report Security Status
- Incorporate Integrated Risk Management (IRM)
- Promote Security Culture in Software Development
- Implement Continuous Improvement

CERTIFICATION

1. Secure Software Concepts	10%
2. Secure Software Requirements	14%
3. Secure Software Architecture and Design	14%
4. Secure Software Implementation	14%
5. Secure Software Testing	14%
6. Secure Software Lifecycle Management	11%
7. Secure Software Deployment, Operations, Maintenance	12%
8. Secure Software Supply Chain	11%

PREREQUISITES

A candidate is required to have a minimum of four years of cumulative paid Software Development Lifecycle (SDLC) professional work experience in one or more of the eight domains of the (ISC)2 CSSLP CBK, or three years of cumulative paid SDLC professional work experience in one or more of the eight domains of the CSSLP CBK with a four-year degree leading to a Baccalaureate, or regional equivalent in Computer Science, Information Technology (IT) or related fields.

WHO SHOULD ATTEND

(ISC)² has an obligation to its membership to maintain the relevancy of the CSSLP. Conducted at regular intervals, the Job Task Analysis (JTA) is a methodical and critical process of determining the tasks that are performed by CSSLP credential holders. The results of the JTA are used to update the examination. This process ensures that candidates are tested on the topic areas relevant to the roles and responsibilities of Today's practicing information security professionals.