Certified Secure Software Lifecycle Professional (CSSLP)

Duration: 5 Days

Course Description:

The Certified Secure Software Lifecycle Professional (CSSLP) course is a comprehensive training program designed to equip learners with the skills and knowledge needed to integrate security into each phase of the Software Development lifecycle (SDLC). It covers essential concepts, from Secure software concepts to the Final disposal of software after its operational life. By delving into topics such as Security design principles, architecture, implementation, testing, and Lifecycle management, learners gain a holistic understanding of how to create and maintain secure software. The CSSLP Certification validates the expertise of professionals in addressing security issues as an integral part of the Software Development process. This course is crucial for software developers, security analysts, and project managers aiming to ensure that security is a priority from the outset, thereby reducing vulnerabilities and compliance issues. Obtaining the CSSLP Certification demonstrates a commitment to security best practices and a high level of professionalism in the field of Software Development.

Target Audience:

The Certified Secure Software Lifecycle Professional (CSSLP) course equips IT professionals with skills for secure Software Development and lifecycle management.

- Software Developers
- Application Security Engineers
- Software Architects
- Security Architects
- Project Managers with a focus on Software Development
- IT Auditors responsible for software process evaluation
- Quality Assurance (QA) Testers implementing security testing
- Security Consultants specialized in software security
- Chief Information Security Officers (CISOs) overseeing software security
- Risk Managers involved in software projects
- System Engineers integrating security into software solutions
- Compliance Analysts ensuring software meets regulations
- Cybersecurity Professionals with a software focus
- Product Owners defining software security requirements
- Supply Chain Managers dealing with software acquisitions
- DevSecOps Specialists integrating security into DevOps practices

Prerequisites:

To successfully undertake training in the Certified Secure Software Lifecycle Professional (CSSLP) course, students should meet the following minimum prerequisites:

- Basic Understanding of Software Development: Familiarity with the software development lifecycle (SDLC) and common software development practices.
- Foundational Knowledge of Security Principles: An understanding of basic cybersecurity concepts, such as confidentiality, integrity, and availability, as well as common security threats and controls.
- Experience in IT or Software Development: At least two years of cumulative, paid work experience in one or more of the eight domains of the (ISC)² CSSLP CBK (Common Body of Knowledge) is recommended. However, candidates who do not yet have the required experience may become an Associate of (ISC)² by successfully passing the CSSLP examination.
- Awareness of Compliance and Regulatory Issues: Some awareness of legal and regulatory issues that pertain to information security, software development, and privacy.
- Communication Skills: Ability to understand and articulate security requirements, risks, and mitigation strategies in both verbal and written forms.

These prerequisites are designed to ensure that participants can derive maximum benefit from the course by having a foundational background upon which to build their CSSLP certification knowledge. However, motivated individuals with a strong desire to learn and a commitment to professional growth in the field of secure software development are encouraged to participate.

Course Objectives:

- Understand core security concepts and design principles to create a robust security posture within the Software Development lifecycle (SDLC).
- Define and integrate software security requirements while ensuring compliance with relevant regulations and data classification standards.
- Develop competence in threat modeling and defining security architecture to mitigate potential risks in software design.
- Learn Secure Coding practices and analyze code for vulnerabilities to maintain code integrity during implementation.
- Devise a comprehensive security testing strategy, including the development of security test cases and analysis of test results for impact.
- Manage secure software lifecycle management by incorporating security in configuration, defining security roadmaps, and promoting a security culture.
- Ensure secure software deployment, operations, maintenance, and disposal adhering to best practices.
- Understand the implications of supply chain risks and learn strategies for secure software acquisition.
- Develop and apply a security-focused strategy for working with suppliers and third-party providers to maintain software security.
- Foster continuous improvement in security practices within Software Development and implement integrated risk management strategies.

Course Outlines:

- 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