1. Course Details:

Course Code : SECR-002
Course Title : CSSLP® (Certified Secure Software Lifecycle Professional) Certification Preparation
Course Duration : 5 Days

2. Course Overview:

- (ISC)² CSSLP training provides a comprehensive review of the knowledge required 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. This training course will help students review and refresh their knowledge and identify areas they need to study for the CSSLP exam.

3. Learning Outcomes:

- Incorporate security requirements in the development of software to produce software that is reliable, resilient and recoverable.
- Understand how to ensure that software security requirements are included in the design of the software, gain knowledge of secure design principles and processes
- Understand the importance of programming concepts that can effectively protect software from vulnerabilities.
- Participants will touch on topics such as software coding vulnerabilities, defensive coding techniques and processes, code analysis and protection, and environmental security considerations that should be factored into software.
- Understand the requirements for software acceptance, paying specific attention to compliance, quality, functionality and assurance.
- Learn about pre- and post-release validation requirements as well as pre-deployment criteria
- Understand the deployment, operations, maintenance and disposal of software from a secure perspective
- Understand how to perform effective assessments on an organization's cyber-supply chain and describe how security applies to the supply chain and software acquisition process

- Understand the importance of supplier sourcing and being able to validate vendor integrity, from third-party vendors to complete outsourcing
- Understand how to manage risk through the adoption of standards and best practices for proper development and testing across the entire lifecycle of products

4. Course Contents:

- Domain 1: Secure Software Concepts
- Domain 2: Secure Software Requirements
- Domain 3: Secure Software Design
- Domain 4: Secure Software Implementation/Programming
- Domain 5: Secure Software Testing
- Domain 6: Secure Lifecycle Management
- Domain 7: Software Deployment, Operations and Maintenance
- Domain 8: Supply Chain and Software Acquisition

5. Our Methodology:

- Make coaching and monitoring innovative and using modern
- Media training also using on the go training by using interactive means and focusing on
- The exercises, practical applications and real situations study.
- Live delivery method, instructor-led training.
- Experienced consultant, trainers, and professional.
- Qualified trainer with high-level experience

6. Attendance Reports:

- Send daily attendance reports to trainingdep
- Send full attendance report to training dep. by the end of thecourse
- Attend 100 % from the course days also providedaily
- Issue attendance certificate for participant who attend minimum 80% from the course duration

7. Pre/Post Reports:

- Pre- assessment before starting training.
- Post assessment after finish training
- Full report for the deferent between Pre-& Post assessment

8. Who Should Attend?

- Software Architect&Engineer
- Software Developer
- Application Security Specialist
- Software Program Manager
- Quality Assurance Tester
- Software Procurement Analyst
- Project Manager
- Security Manager
- IT Director/Manager