CSSLP – Certified Secure Software Lifestyle Professional

LANTEC OF LOUISIANA, LLC
CORPORATE TRAINING CENTER

Days: 5

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 (ISC)^2 CSSLP Common Body of Knowledge (CBK)

Audience: 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

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.

OUTLINE:

LESSON 1 INTRODUCTION

LESSON 2 SECURE SOFTWARE CONCEPTS

- Core Security Concepts
- Security Design Principles

LESSON 3 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 (STRM)
- Ensure Security Requirements Flow Down to Suppliers/Providers

LESSON 4 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

LESSON 5 SECURE SOFTWARE IMPLEMENTATION

- Adhere to Relevant Secure Coding Practices
- Analyze 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

LESSON 6 SECURE SOFTWARE TESTING

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

CSSLP – Certified Secure Software

Lifestyle Professional

LESSON 7 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

LESSON 8 SOFTWARE DEPLOYMENT, OPERATIONS, MAINTENANCE, AND DISPOSAL

- 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
- Perform Information Security Continuous Monitoring (ISCM)
- Support Incident Response
- Perform Patch Management
- Perform Vulnerability Management
- Runtime Protection
- Support Continuity of Operations
- Integrate Service Level Objective (SLO) and Service Level Agreements

LESSON 9 SUPPLY CHAIN AND SOFTWARE ACQUISITION

- Implement Software Supply Chain Risk Management
- Analyze Security of Third-Party Software
- Verify Pedigree and Provenance
- Ensure Supplier Security Requirements in the Acquisition Process
- Support Contractual Requirements