Hewlett Packard Enterprise

CSSLP—Certified Secure Software Lifecycle Professional H0DU5S

HPE course number	H0DU5S
Course length	5 Days
Delivery modes	ILT, VILT
View schedule, local pricing, and register	**View now**
View related courses	**View now**

This Official (ISC)² course provides a comprehensive review of application security concepts and industry best practices, covering the eight domains of the CSSLP CBK: Secure software concepts, security software requirements, secure software design, secure software implementation/coding, secure software testing, software acceptance, software deployment, operations, maintenance, and disposal, supply chain and software acquisition.

Why HPE Education Services?

- IDC MarketScape leader 4 years running for IT education and training*
- Recognized by IDC for leading with global coverage, unmatched technical expertise, and targeted education consulting services*
- Key partnerships with industry leaders OpenStack®, VMware®, Linux®, Microsoft®, ITIL, PMI, CSA, and (ISC)²
- Complete continuum of training delivery options—self-paced eLearning, custom education consulting, traditional classroom, video on-demand instruction, live virtual instructor-led with hands-on lab, dedicated onsite training
- Simplified purchase option with HPE Training Credits

Audience

This course is designed for professionals who demonstrate a globally recognized level of competence, as defined in a common body of knowledge, by assuring security throughout the software lifecycle. They incorporate security when planning, designing, developing, acquiring, testing, deploying, maintaining, and/or managing software to increase its trustworthiness.

The course is intended for students who have at least four years of direct full-time secure software lifecycle professional work experience in one or more of the eight domains of the CSSLP CBK, or three years of direct full-time secure software lifecycle professional work experience in one or more of the eight domains of the CSSLP CBK with a four-year college degree in an information technology discipline. The course builds-on and brings together the holistic view of the topics covered in the everyday environment of an information assurance professional.

Experience in the following professions will greatly enhance the learning environment:

- Software developers
- Engineers and architects
- Product managers
- Project managers
- Software QA
- QA testers
- Business analysts
- Professionals who manage these stakeholders

Course description

In this course you will find that several types of activities are used to reinforce topics and increase knowledge retention. These activities include open-ended questions from the instructor to the students, matching and poll questions, group activities, open/closed questions, and group discussions. This interactive learning technique is based on sound adult learning theories.

*Realize Technology Value with Training, IDC Infographic 2037, Sponsored by HPE, January 2016

Course objectives

- The goal of the security software concepts module is to provide the learner with concepts related to the core software security requirements and foundational design principles as they relate to issues of privacy, governance, risk, and compliance. Learners will understand the software methodologies needed in order to develop software that is secure and resilient to attacks.
- The goal of the security software requirements module is to provide the learner with concepts related to understanding the importance of identifying and developing software with secure requirements. The learner will be able to incorporate security requirements in the development of software in order to produce software that is reliable, resilient, and recoverable.
- The design phase of secure software development is one of the most important phases in the software development lifecycle. The security software design module provides the learner with an understanding of how to ensure that software security requirements are included in the design of the software. Learners will gain knowledge of secure design principles and processes, and be exposed to different architectures and technologies for securing software.
- The security software implementation/coding module provides the learner with an understanding of the importance of programming concepts that can effectively protect software from vulnerabilities.
- Learners 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.
- The security software testing module addresses issues pertaining to proper testing of software for security, including the overall strategies and plans. Learners will gain an understanding of the different types of functional and security testing that should be performed, the criteria for testing, concepts related to impact assessment and corrective actions, and the test data lifecycle.
- The software acceptance module provides an understanding of the requirements for software acceptance, paying specific attention to compliance, quality, functionality, and assurance. Participants will learn about pre- and post-release validation requirements as well as pre-deployment criteria.
- The software deployment, operations, maintenance, and disposal module provides the learner with knowledge pertaining to the deployment, operations, maintenance, and disposal of software from a secure perspective. This is achieved by identifying processes during installation and deployment, operations and maintenance, and disposal that can affect the ability of the software to remain reliable, resilient, and recoverable in its prescribed manner.
- The supply chain and software acquisition module provides the learner with knowledge on how to perform effective assessments on an organization's cyber-supply chain, and describes how security applies to the supply chain and software acquisition process. Learners will understand the importance of supplier sourcing and being able to validate vendor integrity, from third-party vendors to complete outsourcing. Finally, learners will understand how to manage risk through the adoption of standards and best practices for proper development and testing across the entire lifecycle of products.

Benefits to you

This training course will help candidates review and refresh their application security knowledge and help identify areas they need to study for the CSSLP exam and features:

- Official (ISC)² courseware
- Taught by an authorized (ISC)² instructor
- Student handbook
- Collaboration with classmates
- Real-world learning activities and scenarios

Detailed course outline

Domain 1: Secure software concepts	• Core concepts • Security design principles • Privacy • Governance, risk, and compliance • Software development methodologies
Domain 2: Secure software requirements	• Policy decomposition • Data classification and categorization • Functional requirements • Operational requirements
Domain 3: Secure software design	• Design processes • Design considerations • Securing commonly used architecture • Technologies
Domain 4: Secure software implementation/coding	• Declarative vs. imperative (programmatic) security • Vulnerability database/lists • Defensive coding practices and controls • Source code and versioning • Development and build environment • Code/peer review • Code analysis • Anti-tampering techniques
Domain 5: Secure software testing	• Testing artifacts • Testing for security and quality assurance • Types of testing • Impact assessment and corrective action • Test data lifecycle management
Domain 6: Software acceptance	• Pre-release or pre-deployment • Post-release
Domain 7: Software deployment, operations, maintenance, and disposal	• Installation and deployment • Operations and maintenance • Software disposal
Domain 8: Supply chain and software acquisition	• Supplier risk assessment • Supplier sourcing • Software development test • Software delivery, operations, and maintenance • Supplier transitioning

Learn more at
hpe.com/ww/learnsecurity

Follow us:

c04755687, October 2016, Rev. 3

Hewlett Packard
Enterprise