Training: ISC2
ISC2 CSSLP Certification Prep Course

TRAINING GOALS:

Official ISC2 CBK Training Seminar for the CSSLP (Certified Secure Software Lifecycle Professional)

This course is designed for software professionals who 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. Led by an ISC2 authorized instructor, this training seminar provides a comprehensive review of information systems security concepts and industry best practices, covering the following eight domains of the CSSLP Common Body of Knowledge (CBK®)

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

*Each participant in an authorized training **ISC2 CSSLP Certification Prep Course** held in Exclusive Networks will receive a free CSSLP Certification Exam voucher.*

Course objectives

At the end of this course, learners will be able to:

- Discuss the core concepts of software security and the foundational principles that drive construction of resilient software.
- Discuss the security design principles as essential elements for building secure software.
- Discuss software security standards and frameworks, roadmaps and strategies and risk management.
- Explain security in software development methodologies, security metrics and security culture in software development.
- Identify and analyze software requirements pertaining to data privacy, security and compliance

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

with laws and regulations.

- Describe requirement specification and tractability, misuse and abuse cases and flow down of security requirements to supplier.
- Explain secure architecture and design elements and patterns, architectural risk assessment, threat modeling, threat intelligence and attack surface evaluation.
- Explain security architecture and control identification, prioritization and positioning.
- Apply secure coding practices, analyze code for security risks and implement security controls.
- Discuss third-party code and libraries, software composition analysis and security of the build process.
- Discuss security testing strategy plan and analyze security testing methods.
- Discuss validation and verification, security test results and tracking security errors.
- Describe secure software integration and deployment, security data and post-deployment security testing.
- Recognize various security-relevant maintenance activities and discuss planning for the continuity of operations.
- Discuss software supply chain risks and analyze security of third-party software.
- Explain supplier security requirements in the acquisition process and support for contractual requirements.

Intended audience

This course is for individuals planning to pursue the CSSLP certification. The CSSLP is intended for professionals who have a minimum of 4 years of cumulative paid full-time Software Development Lifecycle (SDLC) professional work experience in 1 or more of the 8 domains of the ISC2® CSSLP CBK, or 3 years of cumulative paid full-time SDLC professional work experience in 1 or more of the 8 domains of the CSSLP CBK with a 4-year degree leading to a Baccalaureate, or regional equivalent in Computer Science, Information Technology (IT) or related fields.

Prior to taking this course the learner should have the following experience, skills, or knowledge obtained while serving in the following roles:

- Software Architect
- Software Engineer
- Software Developer
- Application Security Specialist
- Software Program Manager
- Quality Assurance Tester
- Penetration Tester
- Software Procurement Analyst

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

- Project Manager
- Security Manager
- IT Director/Manager

CONSPECT:

- Secure Software Concepts Domain
  - Define core security objectives for software development.
  - Describe the information security triad and explain the main mechanisms of confidentiality, integrity and availability of information.
  - Characterize the relationship between information security and data privacy.
  - Describe accountability, auditing and logging in the context of software security.
  - Explain non-repudiation, digital signatures, benefits of code signing and blockchain.
  - Understand the foundational concepts behind security design principles with respect to secure software development.
- Secure Software Lifecycle and Risk Management Domain
  - Understand and describe OWASP's Software Assurance Maturity Model (OpenSAMM) and Building Security In Maturity Model (BSIMM).
  - Define and recognize security configuration standards and benchmarks.
  - Understand and describe security-focused configuration management processes.
  - Recognize security milestones.
  - Explain and illustrate incorporation of software security practices into the SDLC processes.
  - Discuss security in predictive and adaptive planning for software development.
  - Describe DevOps and DevSecOps.
  - Describe System Security Plan.
  - Recognize security-relevant documentation.
  - Evaluate metrics in software development.
  - Recognize attack surface evaluation for measuring security in software.
  - Describe software decommissioning, end-of-life policy and processes.
  - Discuss data disposition.
  - Explain information system continuous monitoring (ISCM).
  - Describe security information event management (SIEM).
  - Recognize risk management terminology and describe the risk management process.
  - Explain regulations and legal aspects pertaining to intellectual properties and security breaches.
  - Discuss architectural risk assessment.
  - Describe operational risks relevant to integration and deployment environment.

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

- Recognize the importance of personnel training.
- Describe security champions and discuss the importance of security education and guidance.
- Explain retrospectives and continuous improvement in Agile development environments.
- Discuss lessons learned with respect to the processes used to build software.

- Secure Software Requirements Domain
  - Discuss requirements management and identify sources for software security requirements.
  - Recognize functional and nonfunctional requirements and explain the importance of security-focused stories in SCRUM/SCRUM-like methodologies.
  - Analyze misuse/abuse cases and recognize their relevance to known attack patterns.
  - Describe Security Requirements Traceability Matrix (STRM) and discuss how security requirements flow down to suppliers/providers.
  - Analyze security policies and their supporting elements as internal sources for security requirements.
  - Explain compliance requirements and recognize laws, regulations and industry standards as external sources for security requirements.
  - Discuss security standards and frameworks.
  - Describe data governance, explain data ownership, and recognize relevant roles and responsibilities.
  - Describe data classification and explain security labeling and marking.
  - Recognize data types, structured and unstructured.
  - Describe the data lifecycle and explain the process for secure data retention and destruction.
  - Discuss privacy risk, recognize privacy laws and regulations, and explain the requirements for safeguarding personal information.
  - Discuss data anonymization and enumerate various approaches for anonymization.
  - Explain user consent, data retention and data disposition in the context of privacy.
  - Recognize implications of cross-border data transfer and restrictions for the transfer of personal data.
- Secure Software Architecture and Design Domain
  - Understand common threats; describe the threat modeling process, tools and methodologies and explain the process of attack surface evaluation and management.
  - Discuss threat intelligence and describe the sources for cyber threat information.
  - Discuss the process of identification and prioritization of security controls and describe security properties and constraints on the design and constraints imposed by the deployment environment.
  - Describe various architectures and discuss their security-relevant aspects.
  - Describe pervasive computing and IoT, discuss various contactless technologies and discuss their security and privacy aspects.

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

- Explain embedded software and discuss the update challenge and discuss Field-Programmable Gate Array (FPGA) and microcontroller security.
- Explain cloud computing, service models and deployment models, and describe the shared security responsibility model. Discuss mobile applications security.
- Discuss hardware platform concerns, side channel mitigation, speculative execution mitigation, and Hardware Security Modules (HSM).
- Explain cognitive computing, machine learning and artificial intelligence.
- Discuss control systems and their applications in various areas and safety criticality aspects.
- Evaluate security criteria of interfaces, out-of-band management and log interfaces.
- Understand upstream and downstream dependencies, protocol design choices and their security ramifications.
- Describe various authentication and authorization mechanisms; explain credential management and the digital certificate standard.
- Discuss flow controls and data loss prevention; compare and contrast virtual machines and containers.
- Explain the trusted computing base (TCB) and the trusted platform module (TPM).
- Discuss database security, programming language environment, and operating system controls and services.
- Discuss secure architecture and secure design principles, and explain secure design patterns.
- Explain verification of the design, formal and informal secure code reviews and the code inspection process.

- Secure Software Implementation Domain
  - Explain the need for establishing and enforcing secure coding standards.
  - Describe different approaches for implementing security in managed applications.
  - Describe common flaws in software and corresponding mitigation strategies.
  - Discuss input validation, output encoding, authentication, session management, access control, cryptographic practices, error and exception management practices and logging.
  - Explain type safety, memory management and isolation
  - Discuss cryptography, applications to transit and storage, cryptographic agility, cryptographic libraries and encryption algorithm selection.
  - Explain access control, trust zones and function permissions.
  - Explain vulnerability databases and lists.
  - Discuss Common Vulnerabilities and Exposures (CVE), Common Weakness Enumerations (CWE) and Common Attack Pattern Enumeration and Classification (CAPEC).
  - Enumerate OWASP Top 10 Web Application Security Risks.
  - Describe categorization of controls by type and by function.
  - Describe controls to prevent common web application vulnerabilities
  - Describe OWASP Proactive Controls and critical focus areas around building secure

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

software.
- Evaluate the risks associated with using third-party and open-source components and libraries.
- Describe Software Composition Analysis (SCA) and open source management.
- Discuss OWASP Dependency Check and Dependency Track.
- Discuss API integration and evaluate the security aspects.
- Describe system-of-systems.
- Describe the build process, version control, and safeguards used to ensure integrity.
- Discuss anti-tampering techniques as part of software assurance.
- Explain the relation of compiler switches and warnings to the enhancement of security.

- Secure Software Testing Domain
  - Explain functional and nonfunctional security testing, purpose and the phases in penetration testing fuzzing and its variations and limitations.
  - Explain vulnerability scanning and content scanning.
  - Discuss simulation, understand configuration drifts in development environments and describe real user monitoring and synthetic monitoring.
  - Describe fault injection, stress testing and break testing.
  - Describe various types of functional testing, including unit testing, integration testing and regression testing.
  - Describe various types of nonfunctional testing, including scalability, interoperability and performance testing.
  - Describe cryptographic validation and explain Pseudo-Random Number Generators and entropy.
  - Explain test strategy and describe functional and nonfunctional testing.
  - Explain the relationship between use cases and misuse and abuse cases and the importance of creating misuse and abuse cases.
  - Explain test strategy and describe functional and nonfunctional testing.
  - Describe test cases and test harness.
  - Explain black-box and white-box testing, objectives and code coverage.
  - Discuss application security testing (AST) methods and explain their benefits and limitations.
  - Discuss manual code reviews and describe searching for embedded malicious code.
  - Recognize software security-relevant standards, explain crowdsourcing benefits and concerns and discuss bug bounty.
  - Explain the security implications of test results on product management and prioritization of remediation efforts.
  - Explain break-build criteria.
  - Describe the process of tracking security defects.
  - Explain risk scoring, and the Common Vulnerability Scoring System (CVSS).

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

- Explain generation of test data, security of test data, ramifications of using production data in the test environment and database referential integrity and constraints.
- Describe the process of verification and validation testing and explain acceptance testing.
- List various software documentation and explain undocumented functionality.
- Describe OWASP's Application Security Verification Standard (ASVS), its structure and its goals.

- Secure Software Deployment, Operations and Maintenance Domain
  - Explain secure integration, build and deployment.
  - Describe the secure software toolchain.
  - Describe build artifacts and discuss mobile application and platform security.
  - Describe security data, including credentials, keys and certificates and discuss ramifications of failing to protect them in production.
  - Describe vaults used to manage secrets and discuss key vault considerations.
  - Describe the secure bootstrapping process, hardening and the least privilege principle with respect to secure software installation.
  - Explain secure software activation methods and security policy implementation with respect to secure software installation.
  - Describe the Authorization to Operate (ATO) process and the steps involved.
  - Explain risk acceptance.
  - Explain post-deployment verification, issue tracking and testing constraints.
  - Describe security testing automation.
  - Describe the benefits of information security continuous monitoring(ISCM)and list some considerations for its implementation.
  - Describe events, logs and threat intelligence.
  - Explain computer security incidents, incident response and forensics.
  - Describe incident precursors and indicators, monitoring logs and alerts and root-cause analysis.
  - Describe security patch management and explain the timing, prioritization and testing aspects of security patches.
  - Describe vulnerability management and vulnerability scan tools.
  - Explain the operations of web application firewalls.
  - Explain locality of reference, address space layout randomization and data execution prevention.
  - Explain continuity of operations, business impact analysis, data backup and restore and data archiving.
  - Discuss disaster recovery (DR), data residency requirement aspect of DR, resiliency and erasure code.
- Secure Software Supply Chain Domain

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

- Describe the software supply chain.
- Recognize participants in the supply chain.
- Explain software supply chain risk management.
- Explain security risks associated with third party/open source code and recognize OWASP's Software Component Verification Standard (SCVS).
- Describe software supply chain attacks.
- Explain the risks associated with peer-to-peer applications and file sharing.
- Explain code repository and build environment security.
- Explain cryptographically hashed, digitally signed components.
- Describe security in the acquisition process and audit of security policy compliance.
- Explain third-party vulnerability/incident notification and reporting and maintenance and support structure.
- Explain commercial and open-source software licenses.
- Explain vendor/supplier security track record in acquisition and the right-to-audit clause in contracts.
- Explain contractual requirements for intellectual property(IP) ownership inout sourcing relationships, code escrow, liability, warranty and service-level agreements (SLAs).

- Applied Scenario Activities
  - Apply security through the SDLC via animated video-based scenarios and corresponding activities.

REQUIREMENTS:

Candidates for CSSLP 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 ISC2 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.

If you don't have the required experience to become a CSSLP, you may become an Associate of ISC2 by successfully passing the CSSLP examination. You will then have five years to earn the four years required experience.

Part-time work and internships may also count towards your experience.

Valid experience includes information systems security-related work performed in the Software Development Lifecycle (SDLC), or work that requires application security knowledge and involves direct application of that knowledge. Experience must fall within one or more of the eight domains of the ISC2 CSSLP CBK:

- Domain 1.Secure Software Concepts
- Domain 2. Secure Software Requirements

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

- Domain 3. Secure Software Architecture and Design
- Domain 4. Secure Software Implementation
- Domain 5. Secure Software Testing
- Domain 6. Secure Software Lifecycle Management
- Domain 7. Secure Software Deployment, Operations, Maintenance
- Domain 8. Secure Software Supply Chain

More information https://www.isc2.org/Certifications/CSSLP/Experience-Requirements

Difficulty level



CERTIFICATE:

The participants will obtain certificates signed by ISC2 (course completion).

In order to complete the course, receive a certificate of completion and earn ISC2 continuing professional education (CPE) credits learners must:

- Complete all learning activities within the course.
- Complete a course evaluation.
- Score 70% or higher on the final assessment.

An electronic Certificate of Completion will be provided once you have completed the course by meeting all the requirements. We recommend that you download and retain the certificate of completion as proof of credits earned.

This course will help prepare you also for the CSSLP certification exam available at Pearson VUE test centers.

*Each participant in an authorized training **ISC2 CSSLP Certification Prep Course** held in Exclusive Networks will receive a free CSSLP Certification Exam voucher.*

TRAINER:

ISC2 Authorized Instructor

ADDITIONAL INFORMATION:

Participating in this training you get 40 CPE (Continuing Professional Education) credits.

CPE credits for ISC2 credentials must be self-reported by members and associates through the ISC2

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310

CPE Portal accessible via www.isc2.org using your member login credentials.

CPE credits earned for this course may be eligible for continuing professional education credits for non-ISC2 certifications. Please visit the continuing education requirements established by the credentialing organization for eligibility.

For specific questions related to your CPE credits or the CPE portal please contact member support - membersupport@isc2.org.

The Official ISC2 CBK Training Seminar for Certified Secure Software Lifecycle Professional (CSSLP) has earned ACE CREDIT. Students who complete the course can apply for two hours of lower division credit at participating universities and colleges. For more information https://www.acenet.edu/national-guide/Pages/default.aspx

Exclusive Networks Deutschland GmbH
Rahel-Hirsch-Straße 10 / 3. Stock, 10557 Berlin
Tel: +49 303251310