CSSLP®

Certified Secure
Software Lifecycle Professional

An (ISC)² Certification

Domain Refresh

Effective Date: September 15, 2020

*Please note: The **CSSLP Exam Outline** is the official document outlining the domains, weights and subdomains of the certification exam. This document is intended as a supplementary resource only.*

CSSLP Domain Refresh

On September 15, 2020, the domains for the (ISC)² Certified Secure Software Lifecycle Professional (CSSLP®) credential exam were refreshed and the current CSSLP Exam Outline is available on our website.

The content of the CSSLP has been refreshed to reflect the most pertinent issues that secure software professionals currently face, along with the best practices for mitigating those issues. Some topics have been updated while others have been realigned. The result is an exam that most accurately reflects both the deep knowledge of the security practices in each phase of the software development lifecycle (SDLC), as well as the hands-on experience with these practices, that secure software professionals should have.

As a result of the content refresh, the domain and subdomain names have been updated to describe the topics accurately. The weights for the domains have also changed.
Please see the comparison table on the next page.

Domain Comparison

Prior to September 15, 2020	Effective September 15, 2020
Domain 1: Secure Software Concepts	**Domain 1:** Secure Software Concepts
• Core Concepts • Security Design Principles	• Core Concepts • Security Design Principles
Exam Weight: 13%	**Exam Weight: 10%**

Prior to September 15, 2020	Effective September 15, 2020
Domain 2: Secure Software Requirements	**Domain 2:** Secure Software Requirements
• Identify Security Requirements • Interpret Data Classification Requirements • Identify Privacy Requirements • Develop Misuse and Abuse Cases • Include Security in Software Requirements Specifications • Develop Security Requirement Traceability Matrix	• **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**
Exam Weight: 14%	**Exam Weight: 14%**

Prior to September 15, 2020	Effective September 15, 2020
Domain 3: Secure Software Design	**Domain 3:** **Secure Software Architecture and Design**
• Perform Threat Modeling • Define the Security Architecture • Performing Secure Interface Design • Performing Architectural Risk Assessment • Modeling (Non-Functional) Security Properties and Constraints • Model and Classify Data • Evaluate and Select Reusable Secure Design • Perform Design Security Review • Design Secure Assembly Architecture for Component-Based Systems • Use Security Enhancing Architecture and Design Tools • Use Secure Design Principles and Patterns	• Perform Threat Modeling • Define the Security Architecture • Perform Secure Interface Design • Perform 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**
Exam Weight: 16%	**Exam Weight: 14%**

Prior to September 15, 2020	Effective September 15, 2020
Domain 4: Secure Software Implementation/ Programming	**Domain 4:** **Secure Software Implementation**
• Follow Secure Coding Practices • Analyze Code for Security Vulnerabilities • Implement Security Controls • Fix Security Vulnerabilities • Look for Malicious Code • Securely Reuse Third Party Code or Libraries • Securely Integrate Components • Apply Security During the Build Process • Debug Security Errors	• **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
Exam Weight: 16%	**Exam Weight: 14%**

Prior to September 15, 2020	Effective September 15, 2020
Domain 5: Secure Software Testing	**Domain 5:** Secure Software Testing
• Develop Security Test Cases • Develop Security Testing Strategy and Plan • Identify Undocumented Functionality • Interpret Security Implications of Test Results • Classify and Track Security Errors • Secure Test Data • Develop or Obtain Security Data • Perform Verification and Validation 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
Exam Weight: 14%	**Exam Weight: 14%**

Prior to September 15, 2020	Effective September 15, 2020
Domain 6: Secure Lifecycle Management	**Domain 6:** **Secure Software Lifecycle Management**
• Secure Configuration and Version Control • Establish Security Milestones • Choose a Secure Software Methodology • Identify Security Standards and Frameworks • Create Security Documentation • Develop Security Metrics • Decommission Software • Report Security Status • Support Governance, Risk, and Compliance (GRC)	• 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**
Exam Weight: 10%	**Exam Weight: 11%**

Prior to September 15, 2020	Effective September 15, 2020
Domain 7: Software Deployment, Operations, and Maintenance	**Domain 7:** **Secure Software Deployment, Operations, Maintenance**
• Perform Implementation 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 Security Monitoring • Support Incident Response • Support Patch and Vulnerability Management • Support Continuity of Operations	• **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 Objectives (SLO) and Service Level Agreements (SLA)**
Exam Weight: 9%	**Exam Weight: 12%**

Prior to September 15, 2020	Effective September 15, 2020
Domain 8: Supply Chain and Software Acquisition	**Domain 8:** **Secure Software Supply Chain**
• Analyze Security of Third Party Software • Verify Pedigree and Provenance • Provide Security Support to the Acquisition Process	• **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**
Exam Weight: 8%	**Exam Weight: 11%**

Additional Examination Information

Supplementary References

Candidates are encouraged to supplement their education and experience by reviewing relevant resources that pertain to the CBK and identifying areas of study that may need additional attention.

View the full list of supplementary references at www.isc2.org/certifications/References.

Examination Policies and Procedures

(ISC)² recommends that CSSLP candidates review exam policies and procedures prior to registering for the examination. Read the comprehensive breakdown of this important information at www.isc2.org/Register-for-Exam.

Legal Info

For any questions related to (ISC)²'s legal policies, please contact the (ISC)² Legal Department at legal@isc2.org.

Any Questions?

(ISC)² Americas

Tel: +1.866.331.ISC2 (4722)

Email: membersupport@isc2.org

(ISC)² Asia-Pacific

Tel: +852.2850.6951

Email: membersupportapac@isc2.org

(ISC)² EMEA

Tel: +44.203.960.7800

Email: membersupportemea@isc2.org