EDUSUM

#1 Online Certification Guide

CSSLP

ISC2 CSSLP

A Success Guide to Prepare-
ISC2 Secure Software Lifecycle Professional

edusum.com

Table of Contents

Introduction to CSSLP Exam on ISC2 Secure Software Lifecycle Professional

Use this quick start guide to collect all the information about ISC2 CSSLP Certification exam. This study guide provides a list of objectives and resources that will help you prepare for items on the ISC2 Secure Software Lifecycle Professional (CSSLP) exam. The Sample Questions will help you identify the type and difficulty level of the questions and the Practice Exams will make you familiar with the format and environment of an exam. You should refer this guide carefully before attempting your actual ISC2 Certified Secure Software Lifecycle Professional (CSSLP) certification exam.

The ISC2 CSSLP certification is mainly targeted to those candidates who want to build their career in Cybersecurity domain. The ISC2 Certified Secure Software Lifecycle Professional (CSSLP) exam verifies that the candidate possesses the fundamental knowledge and proven skills in the area of ISC2 CSSLP.

ISC2 CSSLP Certification Details:

Exam Name	ISC2 Certified Secure Software Lifecycle Professional (CSSLP)
Exam Code	CSSLP
Exam Price	$549 (USD)
Duration	240 min
Number of Questions	175
Passing Score	700/1000
Schedule Exam	Pearson VUE
Sample Questions	ISC2 CSSLP Sample Questions
Practice Exam	**ISC2 CSSLP Certification Practice Exam**

ISC2 CSSLP Exam Syllabus:

Topic	Details	Weights
Secure Software Concepts	- Core concepts - Security design principles	13%
Secure Software Requirements	- Identify security requirements - Interpret data classification requirements - Identify privacy requirements - Develop misuse and abuse cases - Include security in software requirement specifications - Develop security requirement traceability matrix	14%
Secure Software Design	- 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 design security review - Design secure assembly architecture for component-based systems - Use security enhancing architecture and design tools - Use secure design principles and patterns	16%
Secure Software Implementation/Programming	- 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	16%

Topic	Details	Weights
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 test data - Perform verification and validation testing (e.g., IV&V)	14%
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)	10%
Software Deployment, Operations and 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 (e.g., managing error logs, audits, meeting SLAs, CIA metrics) - Support incident response - Support patch and vulnerability management - Support continuity of operations	9%
Supply Chain and Software Acquisition	- Analyze security of third party software - Verify pedigree and provenance - Provide security support to the acquisition process	8%

CSSLP Sample Questions:

01. The amount of time by which business operations need to be restored to service levels as expected by the business when there is a security breach or disaster is known as

a) Maximum tolerable downtime (MTD)
b) Mean time before failure (MTBF)
c) Minimum security baseline (MSB)
d) Recovery time objective (RTO)

02. Which of the following legal instruments assures the confidentiality of software programs, processing logic, database schema, and internal organizational business processes and client lists?
a) Noncompete agreements
b) Nondisclosure agreements (NDA)
c) Service level agreements (SLA)
d) Trademarks

03. In which of the following software development methodologies does unit testing enable collective code ownership and is critical to assure software assurance?
a) Waterfall
b) Agile
c) Spiral
d) Prototyping

04. Certificate authority, registration authority, and certificate revocation lists are all part of which of the following?
a) Advanced encryption standard (AES)
b) Steganography
c) Public key infrastructure (PKI)
d) Lightweight directory access protocol (LDAP)

05. Developing software to monitor its functionality and report when the software is down and unable to provide the expected service to the business is a protection to assure which of the following?
a) Confidentiality
b) Integrity
c) Authentication
d) Availability

06. When reporting a security defect in the software, which of the following also needs to be reported so that variance from the intended behavior of the software can be determined?
a) Defect identifier
b) Title
c) Expected results
d) Tester name

07. As a means to assure the confidentiality of copyright information, the security analyst identifies the requirement to embed information inside another digital audio, video, or image signal. This is commonly referred to as
a) Encryption
b) Hashing
c) Licensing
d) Watermarking

08. A means of restricting access to objects based on the identity of subjects and/or groups to which they belong is the definition of
a) Nondiscretionary access control (NDAC)
b) Discretionary access control (DAC)
c) Mandatory access control (MAC)
d) Rule-based access control

09. The first step in the incident response process of a reported breach is to
a) Research the validity of the alert or event further
b) Notify management of the security breach
c) Inform potentially affected customers of a potential breach
d) Conduct an independent third party evaluation to investigate the reported breach

10. When the code is not allowed to access memory at arbitrary locations that are out of range of the memory address space that belongs to the object's publicly exposed fields, it is referred to as which of the following types of code?
a) Object code
b) Type safe code
c) Obfuscated code
d) Source code

Answers to CSSLP Exam Questions:

Question: 01 Answer: d	Question: 02 Answer: b	Question: 03 Answer: b	Question: 04 Answer: c	Question: 05 Answer: d
Question: 06 Answer: c	Question: 07 Answer: d	Question: 08 Answer: b	Question: 09 Answer: a	Question: 10 Answer: b

Note: If you find any typo or data entry error in these sample questions, we request you to update us by commenting on this page or write an email on feedback@edusum.com