EDUSUM

#1 Online Certification Guide

CISSP-ISSMP

ISSMP

A Success Guide to Prepare-
ISC2 Information Systems Security Management Professional

edusum.com

Table of Contents

Introduction to CISSP-ISSMP Exam on ISC2 Information Systems Security Management Professional

Use this quick start guide to collect all the information about ISC2 CISSP-ISSMP Certification exam. This study guide provides a list of objectives and resources that will help you prepare for items on the ISC2 Information Systems Security Management Professional (CISSP-ISSMP) 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 Information Systems Security Management Professional (CISSP-ISSMP) certification exam.

The ISC2 CISSP-ISSMP certification is mainly targeted to those candidates who want to build their career in Cybersecurity domain. The ISC2 Information Systems Security Management Professional (CISSP-ISSMP) exam verifies that the candidate possesses the fundamental knowledge and proven skills in the area of ISC2 ISSMP.

ISC2 CISSP-ISSMP Certification Details:

Exam Name	ISC2 Information Systems Security Management Professional (CISSP-ISSMP)
Exam Code	CISSP-ISSMP
Exam Price	$399 (USD)
Duration	180 minutes
Number of Questions	125
Passing Score	700/1000
Schedule Exam	Pearson VUE
Sample Questions	ISC2 CISSP-ISSMP Sample Questions
Practice Exam	**ISC2 CISSP-ISSMP Certification Practice Exam**

ISC2 CISSP-ISSMP Exam Syllabus:

Topic	Details	Weights
Identity and Access Management Architecture	- Design identity management and lifecycle - Design access control management and lifecycle	19%
Security Operations Architecture	- Determine security operation capability requirements and strategy - Design continuous security monitoring (e.g., SIEM, insider threat, enterprise log management, cyber crime, advanced persistent threat) - Design continuity, availability and recovery solutions - Design security operations (e.g., interoperability, scalability, availability, supportability) - Integrate physical security controls - Design incident management capabilities - Security communications and networks	17%
Infrastructure Security	- Determine infrastructure security capability requirements and strategy - Design layer 2/3 architecture (e.g., access control segmentation, out-of-band management, OSI layers) - Secure common services (e.g., wireless, email, VoIP, unified communications) - Architect detective, deterrent, preventative and control systems - Architect infrastructure monitoring - Design integrated cryptographic solutions (e.g., Public Key Infrastructure (PKI), identity system integration)	19%
Architect for Governance, Compliance and Risk Management	- Architect for governance and compliance - Design threat and risk management capabilities - Architect security solutions for off-site data use and storage - Operating environment (e.g., virtualization, cloud computing)	16%
Security Architecture Modeling	- Identify security architecture approach (e.g., reference architectures, build guides, blueprints, patterns) - Verify and validate design (e.g., POT, FAT, regression)	14%

Topic	Details	Weights
Architect for Application Security	- Review software development lifecycle (SDLC) integration of application security architecture (e.g., requirements traceability matrix, security architecture documentation, secure coding) - Review application security (e.g., custom, commercial off-the-shelf (COTS), in-house cloud) - Determine application security capability requirements and strategy (e.g., open source, cloud service providers, SaaS/IaaS providers) - Design application cryptographic solutions (e.g., cryptographic API selection, PRNG selection, software-based key management) - Evaluate application controls against existing threats and vulnerabilities - Determine and establish application security approaches for all system components (mobile, web and thick client applications; proxy, application and database services)	15%

CISSP-ISSMP Sample Questions:

01. Software Development Life Cycle (SDLC) is a logical process used by programmers to develop software. Which of the following SDLC phases meets the audit objectives defined below: System and data are validated.System meets all user requirements. System meets all control requirements.
a) Programming and training
b) Evaluation and acceptance
c) Definition
d) Initiation

02. Which of the following are known as the three laws of OPSEC?
(Choose three.)
a) If you don't know the threat, how do you know what to protect?
b) If you don't know what to protect, how do you know you are protecting it?
c) If you are not protecting it (the critical and sensitive information), the adversary wins!
d) If you don't know about your security resources you cannot protect your network.

03. Joseph works as a Software Developer for Web Tech Inc. He wants to protect the algorithms and the techniques of programming that he uses in developing an application. Which of the following laws are used to protect a part of software?
a) Code Security law
b) Trademark laws
c) Copyright laws
d) Patent laws

04. How many change control systems are there in project management?
a) 3
b) 4
c) 2
d) 1

05. Which of the following statements are true about a hot site?
(Choose two.)
a) It can be used within an hour for data recovery.
b) It is cheaper than a cold site but more expensive than a worm site.
c) It is the most inexpensive backup site.
d) It is a duplicate of the original site of the organization, with full computer systems as well as near-complete backups of user data.

06. Which of the following is the default port for Simple Network Management Protocol (SNMP)?
a) TCP port 80
b) TCP port 25
c) UDP port 161
d) TCP port 110

07. Against which of the following does SSH provide protection?
(Choose two.)
a) IP spoofing
b) Broadcast storm
c) Password sniffing
d) DoS attack

08. Which of the following deals is a binding agreement between two or more persons that is enforceable by law?
a) Outsource
b) Proposal
c) Contract
d) Service level agreement

09. What are the steps related to the vulnerability management program?
(Choose three.)
a) Maintain and Monitor
b) Organization Vulnerability
c) Define Policy
d) Baseline the Environment

10. Which of the following security models dictates that subjects can only access objects through applications?
a) Biba-Clark model
b) Bell-LaPadula
c) Clark-Wilson
d) Biba model

Answers to CISSP-ISSMP Exam Questions:

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

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