EDUSUM

#1 Online Certification Guide

CISSP

ISC2 CISSP Certification

A Success Guide to Prepare-
ISC2 Information Systems Security Professional

edusum.com

Table of Contents

Introduction to CISSP Exam on ISC2 Information Systems Security Professional

Use this quick start guide to collect all the information about ISC2 CISSP 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 Professional (CISSP) 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 Information Systems Security Professional (CISSP) certification exam.

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

ISC2 CISSP Certification Details:

Exam Name	ISC2 Certified Information Systems Security Professional (CISSP)
Exam Code	CISSP
Exam Price	$599 (USD)
Duration	360 minutes
Number of Questions	250
Passing Score	700/1000
Schedule Exam	Pearson VUE
Sample Questions	ISC2 CISSP Sample Questions
Practice Exam	**ISC2 CISSP Certification Practice Exam**

ISC2 CISSP Exam Syllabus:

Topic	Details	Weights
Security and Risk Management	- Confidentiality, integrity and availability concepts - Security governance principles - Compliance - Legal and regulatory issues - Professional ethics - Security policies, standards, procedures and guidelines	16%
Asset Security	- Information and asset classification - Ownership (e.g., data owners, system owners) - Protect privacy - Appropriate retention - Data security controls - Handling requirements (e.g., markings, labels, storage)	10%
Security Engineering	- Engineering processes using secure design principles - Fundamental concepts of security models - Security evaluation models - Security capabilities of information systems - Security architectures, designs and solution elements vulnerabilities - Web-based systems vulnerabilities - Mobile systems vulnerabilities - Embedded devices and cyber-physical systems vulnerabilities - Cryptography - Site and facility design secure principles - Physical security	12%
Communication and Network Security	- Secure network architecture design (e.g., IP & non-IP protocols, segmentation) - Secure network components - Secure communication channels - Network attacks	12%
Identity and Access Management	- Physical and logical assets control - Identification and authentication of people and devices - Identity as a service (e.g., cloud identity) - Third-party identity services (e.g., on-premise) - Access control attacks - Identity and access provisioning lifecycle (e.g., provisioning review)	13%

Topic	Details	Weights
Security Assessment and Testing	- Assessment and test strategies - Security process data (e.g., management and operational controls) - Security control testing - Test outputs (e.g., automated, manual) - Security architecture vulnerabilities	11%
Security Operations	- Investigations support and requirements - Logging and monitoring activities - Provisioning of resources - Foundational security operations concepts - Resource protection techniques - Incident management - Preventative measures - Patch and vulnerability management - Change management processes - Recovery strategies - Disaster recovery processes and plans - Business continuity planning and exercises - Physical security - Personnel safety concerns	16%
Software Development Security	- Security in the software development lifecycle - Development environment security controls - Software security effectiveness - Acquired software security impact	10%

CISSP Sample Questions:

01. The process for developing an ISCM strategy and implementing an ISCM program is?
a) Define, analyze, implement, establish, respond, review and update
b) Analyze, implement, define, establish, respond, review and update
c) Define, establish, implement, analyze, respond, review and update
d) Implement, define, establish, analyze, respond, review and update

02. What are the seven main categories of access control?
a) Detective, corrective, monitoring, logging, recovery, classification, and directive
b) Directive, deterrent, preventative, detective, corrective, compensating, and recovery
c) Authorization, identification, factor, corrective, privilege, detective, and directive
d) Identification, authentication, authorization, detective, corrective, recovery, and directive

03. Ann installs a new Wireless Access Point (WAP) and users are able to connect to it. However, once connected, users cannot access the Internet. Which of the following is the MOST likely cause of the problem?
a) The signal strength has been degraded and latency is increasing hop count.
b) An incorrect subnet mask has been entered in the WAP configuration.
c) The signal strength has been degraded and packets are being lost.
d) Users have specified the wrong encryption type and packets are being rejected.

04. Qualitative risk assessment is earmarked by which of the following?
a) Ease of implementation and it can be completed by personnel with a limited understanding of the risk assessment process
b) Can be completed by personnel with a limited understanding of the risk assessment process and uses detailed metrics used for calculation of risk
c) Detailed metrics used for calculation of risk and ease of implementation
d) Can be completed by personnel with a limited understanding of the risk assessment process and detailed metrics used for the calculation of risk

05. Which of the following security models is primarily concerned with how the subjects and objects are created and how subjects are assigned rights or privileges?
a) Bell–LaPadula
b) Biba-Integrity
c) Chinese Wall
d) Graham–Denning

06. Before applying a software update to production systems, it is MOST important that
a) Full disclosure information about the threat that the patch addresses is available
b) The patching process is documented
c) The production systems are backed up
d) An independent third party attests the validity of the patch

07. While an Enterprise Security Architecture (ESA) can be applied in many different ways, it is focused on a few key goals. Identify the proper listing of the goals for the ESA:
a) It represents a simple, long term view of control, it provides a unified vision for common security controls, it leverages existing technology investments, it provides a fixed approach to current and future threats and also the needs of peripheral functions
b) It represents a simple, long term view of control, it provides a unified vision for common security controls, it leverages new technology investments, it provides a flexible approach to current and future threats and also the needs of core functions
c) It represents a complex, short term view of control, it provides a unified vision for common security controls, it leverages existing technology investments, it provides a flexible approach to current and future threats and also the needs of core functions
d) It represents a simple, long term view of control, it provides a unified vision for common security controls, it leverages existing technology investments, it provides a flexible approach to current and future threats and also the needs of core functions

08. Technical evaluation of assurance to ensure that security requirements have been met is known as?
a) Accreditation
b) Certification
c) Validation
d) Verification

09. A potential vulnerability of the Kerberos authentication server is
a) Single point of failure
b) Asymmetric key compromise
c) Use of dynamic passwords
d) Limited lifetimes for authentication credentials

10. Which of the following can BEST be used to capture detailed security requirements?
a) Threat modeling, covert channels, and data classification
b) Data classification, risk assessments, and covert channels
c) Risk assessments, covert channels, and threat modeling
d) Threat modeling, data classification, and risk assessments

Answers to CISSP Exam Questions:

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

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