EDUSUM

CISSP-ISSAP

ISC2 CISSP-ISSAP Certification

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

_____

Table of Contents

_____

_____

Introduction to CISSP-ISSAP Exam on ISC2 Information Systems Security Architecture Professional

Use this quick start guide to collect all the information about ISC2 CISSP-ISSAP 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 Architecture Professional (CISSP-ISSAP) 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 Architecture Professional (CISSP-ISSAP) certification exam.

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

ISC2 CISSP-ISSAP Certification Details:

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

_____

ISC2 CISSP-ISSAP 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-ISSAP Sample Questions:

01. Which of the following protocols uses public-key cryptography to authenticate the remote computer?
a) SSH
b) Telnet
c) SCP
d) SSL

02. You work as a Network Administrator of a TCP/IP network. You are having DNS resolution problem. Which of the following utilities will you use to diagnose the problem?
a) TRACERT
b) PING
c) IPCONFIG
d) NSLOOKUP

03. Which of the following describes the acceptable amount of data loss measured in time?
a) Recovery Consistency Objective (RCO)
b) Recovery Time Objective (RTO)
c) Recovery Point Objective (RPO)
d) Recovery Time Actual (RTA)

_____

04. Which of the following statements about Discretionary Access Control List (DACL) is true?
a) It specifies whether an audit activity should be performed when an object attempts to access a resource.
b) It is a unique number that identifies a user, group, and computer account.
c) It is a list containing user accounts, groups, and computers that are allowed (or denied) access to the object.
d) It is a rule list containing access control entries.

05. In which of the following access control models, owner of an object decides who is allowed to access the object and what privileges they have?
a) Access Control List (ACL)
b) Mandatory Access Control (MAC)
c) Role Based Access Control (RBAC)
d) Discretionary Access Control (DAC)

06. Which of the following attacks can be overcome by applying cryptography?
a) Web ripping
b) DoS
c) Sniffing
d) Buffer overflow

07. Which of the following types of firewall functions at the Session layer of OSI model?
a) Circuit-level firewall
b) Application-level firewall
c) Packet filtering firewall
d) Switch-level firewall

08. The network you administer allows owners of objects to manage the access to those objects via access control lists. This is an example of what type of access control?
a) RBAC
b) MAC
c) CIA
d) DAC

09. Which of the following are examples of physical controls used to prevent unauthorized access to sensitive materials?
a) Thermal alarm systems
b) Security Guards
c) Closed circuit cameras
d) Encryption

10. In which of the following network topologies does the data travel around a loop in a single direction and pass through each device?
a) Ring topology
b) Tree topology
c) Star topology
d) Mesh topology

_____

_____

Answers to CISSP-ISSAP Exam Questions:

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

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