EDUSUM

#1 Online Certification Guide

CAP

ISC2 CAP certification

A Success Guide to Prepare-
ISC2 Authorization Professional

edusum.com

Table of Contents

Introduction to CAP Exam on ISC2 Authorization Professional

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

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

ISC2 CAP Certification Details:

Exam Name	ISC2 Certified Authorization Professional (CAP)
Exam Code	CAP
Exam Price	$419 (USD)
Duration	180 min
Number of Questions	125
Passing Score	700/1000
Schedule Exam	Pearson VUE
Sample Questions	ISC2 CAP Sample Questions
Practice Exam	**ISC2 CAP Certification Practice Exam**

ISC2 CAP Exam Syllabus:

Topic	**Details**	**Weights**
Risk Management Framework (RMF)	- Describe the RMF - Describe and distinguish between the RMF steps - Identify roles and define responsibilities - Understand and describe how the RMF process relates to the organizational structure - Understand the relationship between the RMF and System Development Life Cycle (SDLC) - Understand legal, regulatory and other security requirements	20%
Categorization of Information Systems	- Categorize the system - Describe the information system (including the security authorization boundaries) - Register the system	8%
Selection of Security Controls	- Identify and document (inheritable) controls - Select, tailor and document security controls - Develop security control monitoring strategy - Review and approve security plan	13%
Security Control Implementation	- Implement selected security controls - Document security control implementation	10%
Security Control Assessment	- Prepare for security control assessment - Develop security control assessment plan - Assess security control effectiveness - Develop initial security assessment report (SAR) - Review interim SAR and perform initial remediation actions - Develop final SAR and optional addendum	19%
Information System Authorization	- Develop plan of action and milestones (POAM) (e.g., resources, schedule, requirements) - Assemble security authorization package - Determine risk - Determine the acceptability of risk - Obtain security authorization decision	13%
Monitoring of Security Controls	- Determine security impact of changes to system and environment - Perform ongoing security control assessments (e.g., continuous monitoring, internal and external assessments) - Conduct ongoing remediation actions (resulting from incidents, vulnerability scans, audits, vendor updates, etc.) - Update key documentation (e.g., SP, SAR, POAM) - Perform periodic security status reporting - Perform ongoing risk determination and acceptanc - Decommission and remove system	17%

CAP Sample Questions:

01. According to the Risk Management Framework (RMF), which role has a primary responsibility to report the security status of the information system to the authorizing official (AO) and other appropriate organizational officials on an ongoing basis in accordance with the monitoring strategy?
a) Information system security officer (ISSO)
b) Common control provider
c) Independent assessor
d) Senior information assurance officer (SIAO)

02. Which authorization approach considers time elapsed since the authorization results were produced, the environment of operation, the criticality/sensitivity of the information, and the risk tolerance of the other organization?
a) Leveraged
b) Single
c) Joint
d) Site specific

03. When should the information system owner document the information system and authorization boundary description in the security plan?
a) After security controls are implemented
b) While assembling the authorization package
c) After security categorization
d) When reviewing the security control assessment plan

04. Information developed from Federal Information Processing Standard (FIPS) 199 may be used as an input to which authorization package document?
a) Security assessment report (SAR)
b) System security plan (SSP)
c) Plan of actions and milestones (POA&M)
d) Authorization decision document

05. Why is security control volatility an important consideration in the development of a security control monitoring strategy?
a) It identifies needed security control monitoring exceptions.
b) It indicates a need for compensating controls.
c) It establishes priority for security control monitoring.
d) It provides justification for revisions to the configuration management and control plan.

06. System authorization is now used to refer to which of the following terms?
a) System security declaration
b) Certification and accreditation
c) Security test and evaluation
d) Continuous monitoring

07. Documenting the description of the system in the system security plan is the primary responsibility of which Risk Management Framework (RMF) role?
a) Authorizing official (AO)
b) Information owner
c) Information system security officer (ISSO)
d) Information system owner

08. When an authorizing official (AO) submits the security authorization decision, what responses should the information system owner (ISO) expect to receive?
a) Authorized to operate (ATO) or denial authorization to operate (DATO), the conditions for the authorization placed on the information system and owner, and the authorization termination date
b) Authorized to Operate (ATO) or Denial Authorization to Operate (DATO), the list of security controls accessed, and an system contingency plan
c) Authorized to operate (ATO) or denial authorization to operate (DATO), and the conditions for the authorization placed on the information system and owner
d) A plan of action and milestones (POA&M), the conditions for the authorization placed on the information system and owner, and the authorization termination date

09. Who determines the required level of independence for security control assessors?
a) Information system owner (ISO)
b) Information system security manager (ISSM)
c) Authorizing official (AO)
d) Information system security officer (ISSO)

10. What key information is used by the authorizing official (AO) to assist with the risk determination of an information system (IS)?
a) Security authorization package (SAP)
b) Plan of action and milestones (POA&M)
c) Security plan (SP)
d) Interconnection security agreement (ISA)

Answers to CAP Exam Questions:

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