



ISC2 CISSP-ISSEP

ISC2 ISSEP Certification Questions & Answers

Exam Summary – Syllabus – Questions

CISSP-ISSEP

[ISC2 Information Systems Security Engineering Professional \(CISSP-ISSEP\)](#)

125 Questions Exam – 700/1000 Cut Score – Duration of 180 minutes

Table of Contents:

Know Your CISSP-ISSEP Certification Well:.....	2
ISC2 CISSP-ISSEP Certification Details:	2
CISSP-ISSEP Syllabus:	3
Systems Security Engineering Foundations - 25%.....	3
Risk Management - 14%	3
Security Planning and Design - 30%.....	4
Systems Implementation, Verification and Validation - 14%	4
Secure Operations, Change Management and Disposal - 17%	5
ISC2 CISSP-ISSEP Sample Questions:.....	5
Study Guide to Crack ISC2 CISSP-ISSEP Exam:.....	9

Know Your CISSP-ISSEP Certification Well:

The CISSP-ISSEP is best suitable for candidates who want to gain knowledge in the ISC2 Cybersecurity. Before you start your CISSP-ISSEP preparation you may struggle to get all the crucial ISSEP materials like CISSP-ISSEP syllabus, sample questions, study guide.

But don't worry the CISSP-ISSEP PDF is here to help you prepare in a stress free manner.

The PDF is a combination of all your queries like-

- What is in the CISSP-ISSEP syllabus?
- How many questions are there in the CISSP-ISSEP exam?
- Which Practice test would help me to pass the CISSP-ISSEP exam at the first attempt?

Passing the CISSP-ISSEP exam makes you ISC2 Information Systems Security Engineering Professional (CISSP-ISSEP). Having the ISSEP certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

ISC2 CISSP-ISSEP Certification Details:

Exam Name	ISC2 Information Systems Security Engineering Professional (CISSP-ISSEP)
Exam Code	CISSP-ISSEP
Exam Price	\$599 (USD)
Duration	180 mins
Number of Questions	125
Passing Score	700/1000
Schedule Exam	Pearson VUE
Sample Questions	ISC2 CISSP-ISSEP Sample Questions
Practice Exam	ISC2 CISSP-ISSEP Certification Practice Exam

CISSP-ISSEP Syllabus:

Topic	Details
Systems Security Engineering Foundations - 25%	
Apply systems security engineering fundamentals	<ul style="list-style-type: none"> - Understand systems security engineering trust concepts and hierarchies - Identify the relationships between systems and security engineering processes - Apply structural security design principles
Execute systems security engineering processes	<ul style="list-style-type: none"> - Identify organizational security authority - Identify system security policy elements - Integrate design concepts (e.g., open, proprietary, modular)
Integrate with applicable system development methodology	<ul style="list-style-type: none"> - Integrate security tasks and activities - Verify security requirements throughout the process - Integrate software assurance method
Perform technical management	<ul style="list-style-type: none"> - Perform project planning processes - Perform project assessment and control processes - Perform decision management processes - Perform risk management processes - Perform configuration management processes - Perform information management processes - Perform measurement processes - Perform Quality Assurance (QA) processes - Identify opportunities for security process automation
Participate in the acquisition process	<ul style="list-style-type: none"> - Prepare security requirements for acquisitions - Participate in selection process - Participate in Supply Chain Risk Management (SCRM) - Participate in the development and review of contractual documentation
Design Trusted Systems and Networks (TSN)	
Risk Management - 14%	
Apply security risk management principles	<ul style="list-style-type: none"> - Align security risk management with Enterprise Risk Management (ERM) - Integrate risk management throughout the lifecycle
Address risk to system	<ul style="list-style-type: none"> - Establish risk context - Identify system security risks

Topic	Details
	<ul style="list-style-type: none"> - Perform risk analysis - Perform risk evaluation - Recommend risk treatment options - Document risk findings and decisions
Manage risk to operations	<ul style="list-style-type: none"> - Determine stakeholder risk tolerance - Identify remediation needs and other system changes - Determine risk treatment options - Assess proposed risk treatment options - Recommend risk treatment options
Security Planning and Design - 30%	
Analyze organizational and operational environment	<ul style="list-style-type: none"> - Capture stakeholder requirements - Identify relevant constraints and assumptions - Assess and document threats - Determine system protection needs - Develop Security Test Plans (STP)
Apply system security principles	<ul style="list-style-type: none"> - Incorporate resiliency methods to address threats - Apply defense-in-depth concepts - Identify fail-safe defaults - Reduce Single Points of Failure (SPOF) - Incorporate least privilege concept - Understand economy of mechanism - Understand Separation of Duties (SoD) concept
Develop system requirements	<ul style="list-style-type: none"> - Develop system security context - Identify functions within the system and security Concept of Operations (CONOPS) - Document system security requirements baseline - Analyze system security requirements
Create system security architecture and design	<ul style="list-style-type: none"> - Develop functional analysis and allocation - Maintain traceability between specified design and system requirements - Develop system security design components - Perform trade-off studies - Assess protection effectiveness
Systems Implementation, Verification and Validation - 14%	
Implement, integrate and deploy security solutions	<ul style="list-style-type: none"> - Perform system security implementation and integration - Perform system security deployment activities

Topic	Details
Verify and validate security solutions	<ul style="list-style-type: none"> - Perform system security verification - Perform security validation to demonstrate security controls meet stakeholder security requirements
Secure Operations, Change Management and Disposal - 17%	
Develop secure operations strategy	<ul style="list-style-type: none"> - Specify requirements for personnel conducting operations - Contribute to the continuous communication with stakeholders for security relevant aspects of the system
Participate in secure operations	<ul style="list-style-type: none"> - Develop continuous monitoring solutions and processes - Support the Incident Response (IR) process - Develop secure maintenance strategy
Participate in change management	<ul style="list-style-type: none"> - Participate in change reviews - Determine change impact - Perform verification and validation of changes - Update risk assessment documentation
Participate in the disposal process	<ul style="list-style-type: none"> - Identify disposal security requirements - Develop secure disposal strategy - Develop decommissioning and disposal procedures - Audit results of the decommissioning and disposal process

ISC2 CISSP-ISSEP Sample Questions:

Question: 1

Which of the following types of CNSS issuances establishes criteria, and assigns responsibilities?

- a) Advisory memoranda
- b) Directives
- c) Instructions
- d) Policies

Answer: d

Question: 2

NIST SP 800-53A defines three types of interview depending on the level of assessment conducted. Which of the following NIST SP 800-53A interviews consists of informal and ad hoc interviews?

- a) Abbreviated
- b) Significant
- c) Substantial
- d) Comprehensive

Answer: a**Question: 3**

Which of the following DoD directives defines DITSCAP as the standard C&A process for the Department of Defense?

- a) DoD 5200.22-M
- b) DoD 8910.1
- c) DoD 5200.40
- d) DoD 8000.1

Answer: c**Question: 4**

Which of the following configuration management system processes keeps track of the changes so that the latest acceptable configuration specifications are readily available?

- a) Configuration Identification
- b) Configuration Verification and Audit
- c) Configuration Status and Accounting
- d) Configuration Control

Answer: c

Question: 5

Which of the following principles are defined by the IATF model?

(Choose two.)

- a) The degree to which the security of the system, as it is defined, designed, and implemented, meets the security needs.
- b) The problem space is defined by the customer's mission or business needs
- c) The systems engineer and information systems security engineer define the solution space, which is driven by the problem space.
- d) Always keep the problem and solution spaces separate.

Answer: b, c, d

Question: 6

In which of the following DIACAP phases is residual risk analyzed?

- a) Phase 2
- b) Phase 3
- c) Phase 5
- d) Phase 1
- e) Phase 4

Answer: e

Question: 7

Which of the following DITSCAP/NIACAP model phases is used to show the required evidence to support the DAA in accreditation process and conclude in an Approval To Operate (ATO)?

- a) Verification
- b) Validation
- c) Post accreditation
- d) Definition

Answer: b

Question: 8

You work as an ISSE for BlueWell Inc. You want to break down user roles, processes, and information until ambiguity is reduced to a satisfactory degree.

Which of the following tools will help you to perform the above task?

- a) PERT Chart
- b) Gantt Chart
- c) Functional Flow Block Diagram
- d) Information Management Model (IMM)

Answer: d

Question: 9

Which of the following federal laws are related to hacking activities?

(Choose three.)

- a) 18 U.S.C. 1030
- b) 18 U.S.C. 1029
- c) 18 U.S.C. 2510
- d) 18 U.S.C. 1028

Answer: a, b, c

Question: 10

Which of the following is NOT an objective of the security program?

- a) Security education
- b) Information classification
- c) Security organization
- d) Security plan

Answer: d

Study Guide to Crack ISC2 CISSP-ISSEP Exam:

- Getting details of the CISSP-ISSEP syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the CISSP-ISSEP exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the ISC2 provided training for CISSP-ISSEP exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the CISSP-ISSEP sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on CISSP-ISSEP practice tests is must. Continuous practice will make you an expert in all syllabus areas.

Reliable Online Practice Test for CISSP-ISSEP Certification

Make EduSum.com your best friend during your ISC2 Information Systems Security Engineering Professional exam preparation. We provide authentic practice tests for the CISSP-ISSEP exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual CISSP-ISSEP exam. We guarantee you 100% success in your first exam attempt if you continue practicing regularly. Don't bother if you don't get 100% marks in initial practice exam attempts. Just utilize the result section to know your strengths and weaknesses and prepare according to that until you get 100% with our practice tests. Our evaluation makes you confident, and you can score high in the CISSP-ISSEP exam.

Start Online practice of CISSP-ISSEP Exam by visiting URL
<https://www.edusum.com/isc2/cissp-issep-isc2-information-systems-security-engineering-professional>