ISC2 CISSP-ISSMP

ISC2 ISSMP Certification Questions & Answers

Exam Summary – Syllabus –Questions

CISSP-ISSMP
ISC2 Information Systems Security Management Professional (CISSP-ISSMP)
125 Questions Exam – 700/1000 Cut Score – Duration of 180 minutes

Table of Contents:

Know Your CISSP-ISSMP Certification Well:

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

But don't worry the CISSP-ISSMP 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-ISSMP syllabus?
- How many questions are there in the CISSP-ISSMP exam?
- Which Practice test would help me to pass the CISSP-ISSMP exam at the first attempt?

Passing the CISSP-ISSMP exam makes you . Having the ISSMP 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-ISSMP ISSMP Certification Details:

Exam Name	ISC2 Information Systems Security Management Professional (CISSP-ISSMP)
Exam Code	CISSP-ISSMP
Exam Price	$599 (USD)
Duration	180 mins
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**

CISSP-ISSMP Syllabus:

Topic	Details
Leadership and Business Management - 22%	
Establish Security's Role in Organizational Culture, Vision, and Mission	- Define information security program vision and mission - Align security with organizational goals, objectives, and values - Explain business processes and their relationships - Describe the relationship between organizational culture and security
Align Security Program with Organizational Governance	- Identify and navigate organizational governance structure - Recognize roles of key stakeholders - Recognize sources and boundaries of authorization - Negotiate organizational support for security initiatives
Define and Implement Information Security Strategies	- Identify security requirements from business initiatives - Evaluate capacity and capability to implement security strategies - Manage implementation of security strategies - Review and maintain security strategies - Describe security engineering theories, concepts, and methods
Define and Maintain Security Policy Framework	- Determine applicable external standards - Manage data classification - Establish internal policies - Obtain organizational support for policies - Develop procedures, standards, guidelines, and baselines - Ensure periodic review of security policy framework
Manage Security Requirements in Contracts and Agreements	- Evaluate service management agreements (e.g., risk, financial) - Govern managed services (e.g., infrastructure, cloud services) - Manage impact of organizational change (e.g., mergers and acquisitions, outsourcing) - Monitor and enforce compliance with contractual agreements
Oversee Security Awareness and Training Programs	- Promote security programs to key stakeholders - Identify training needs by target segment - Monitor and report on effectiveness of security awareness and training programs
Define, Measure, and Report Security Metrics	- Identify Key Performance Indicators (KPI) - Relate KPIs to the risk position of the organization

Topic	Details
	- Use metrics to drive security program development and operations
Prepare, Obtain, and Administer Security Budget	- Manage and report financial responsibilities - Prepare and secure annual budget - Adjust budget based on evolving risks
Manage Security Programs	- Build cross-functional relationships - Identify communication bottlenecks and barriers - Define roles and responsibilities - Resolve conflicts between security and other stakeholders - Determine and manage team accountability
Apply Product Development and Project Management Principles	- Describe project lifecycle - Identify and apply appropriate project management methodology - Analyze time, scope, and cost relationship
Systems Lifecycle Management - 19%	
Manage Integration of Security into System Development Lifecycle (SDLC)	- Integrate information security gates (decision points) and milestones into lifecycle - Implement security controls into system lifecycle - Oversee configuration management processes
Integrate New Business Initiatives and Emerging Technologies into the Security Architecture	- Participate in development of business case for new initiatives to integrate security - Address impact of new business initiatives on security
Define and Oversee Comprehensive Vulnerability Management Programs (e.g., vulnerability scanning, penetration testing, threat analysis)	- Classify assets, systems, and services based on criticality to business - Prioritize threats and vulnerabilities - Oversee security testing - Mitigate or remediate vulnerabilities based on risk
Manage Security Aspects of Change Control	- Integrate security requirements with change control process - Identify stakeholders - Oversee documentation and tracking - Ensure policy compliance

Topic	Details
Risk Management - 18%	
Develop and Manage a Risk Management Program	- Communicate risk management objectives with risk owners and other stakeholders - Understand principles for defining risk tolerance - Determine scope of organizational risk program - Obtain and verify organizational asset inventory - Analyze organizational risk management requirements - Determine the impact and likelihood of threats and vulnerabilities - Determine countermeasures, compensating and mitigating controls - Recommend risk treatment options and when to apply them
Conduct Risk Assessments (RA)	- Identify risk factors - Manage supplier, vendor, and third-party risk - Understand supply chain security management - Conduct Business Impact Analysis (BIA) - Manage risk exceptions - Monitor and report on risk - Perform cost–benefit analysis
Threat Intelligence and Incident Management - 17%	
Establish and Maintain Threat Intelligence Program	- Synthesize relevant data from multiple threat intelligence sources - Conduct baseline analysis - Review anomalous behavior patterns for potential concerns - Conduct threat modeling - Identify ongoing attacks - Correlate related attacks - Create actionable alerting to appropriate resources
Establish and Maintain Incident Handling and Investigation Program	- Develop program documentation - Establish incident response case management process - Establish Incident Response Team (IRT) - Understand and apply incident management methodologies - Establish and maintain incident handling process - Establish and maintain investigation process - Quantify and report financial and operational impact of incidents and investigations to stakeholders - Conduct Root Cause Analysis (RCA)

Topic	Details
Contingency Management - 10%	
Oversee Development of Contingency Plans (CP)	- Analyze challenges related to the Business Continuity (BC) process (e.g., time, resources, verification) - Analyze challenges related to the Disaster Recovery (DR) process (e.g., time, resources, verification) - Analyze challenges related to the Continuity of Operations Plan (COOP) - Coordinate with key stakeholders - Define internal and external incident communications plans - Define incident roles and responsibilities - Determine organizational drivers and policies - Reference Business Impact Analysis (BIA) - Manage third-party dependencies - Prepare security management succession plan
Guide Development of Recovery Strategies	- Identify and analyze alternatives - Recommend and coordinate recovery strategies - Assign recovery roles and responsibilities
Maintain Business Continuity Plan (BCP), Continuity of Operations Plan (COOP), and Disaster Recovery Plan (DRP)	- Plan testing, evaluation, and modification - Determine survivability and resiliency capabilities - Manage plan update process
Manage Recovery Process	- Declare disaster - Implement plan - Restore normal operations - Gather lessons learned - Update plan based on lessons learned
Law, Ethics, and Security Compliance Management - 14%	
Understand the Impact of Laws that Relate to Information Security	- Understand global privacy laws - Understand legal jurisdictions the organization operates within (e.g., trans-border data flow) - Understand export laws - Understand intellectual property laws - Understand industry regulations affecting the organization - Advise on potential liabilities
Understand Management Issues as Related to the (ISC)2 Code of Ethics	

Topic	Details
Validate Compliance in Accordance with Applicable Laws, Regulations, and Industry Best Practices	- Obtain leadership buy-in - Select compliance framework(s) - Implement validation procedures outlined in framework(s) - Define and utilize security compliance metrics to report control effectiveness and potential areas of improvement
Coordinate with Auditors, and Assist with the Internal and External Audit Process	- Prepare - Schedule - Perform audit - Evaluate findings - Formulate response - Validate implemented mitigation and remediation actions
Document and Manage Compliance Exceptions	

ISC2 CISSP-ISSMP Sample Questions:

Question: 1

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

Answer: d

Question: 2

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.

Answer: a, d

Question: 3

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

Answer: a, c, d

Question: 4

Against which of the following does SSH provide protection?

(Choose two.)

a) IP spoofing
b) Broadcast storm
c) Password sniffing
d) DoS attack

Answer: a, c

Question: 5

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.

Answer: a, b, c

Question: 6

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

Answer: c

Question: 7

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

Answer: b

Question: 8

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

Answer: c

Question: 9

How many change control systems are there in project management?

a) 3
b) 4
c) 2
d) 1

Answer: b

Question: 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

Answer: c

Study Guide to Crack ISC2 ISSMP CISSP-ISSMP Exam:

- Getting details of the CISSP-ISSMP 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-ISSMP 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-ISSMP 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-ISSMP 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-ISSMP practice tests is must. Continuous practice will make you an expert in all syllabus areas.

Reliable Online Practice Test for CISSP-ISSMP Certification

Make EduSum.com your best friend during your ISC2 Information Systems Security Management Professional exam preparation. We provide authentic practice tests for the CISSP-ISSMP exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual CISSP-ISSMP 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-ISSMP exam.

Start Online practice of CISSP-ISSMP Exam by visiting URL
https://www.edusum.com/isc2/cissp-issmp-isc2-information-systems-security-management-professional