ISC2 CISSP-ISSMP

ISC2 ISSMP Certification Questions & Answers

Exam Summary – Syllabus –Questions

CISSP-ISSMP
ISC2 Information Systems Security Management Professional
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 Strategy and Implementation. 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 ISC2 Information Systems Security Management Professional. 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 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 - 20%	
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 - Define security's relationship to the overall business processes - Define the relationship between organizational culture and security
Align Security Program with Organizational Governance	- Identify and navigate organizational governance structure - Validate roles of key stakeholders - Validate sources and boundaries of authorization - Advocate and obtain 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 - Prescribe security architecture and engineering theories, concepts and methods
Define and maintain security policy framework Determine applicable external standards	- Determine applicable external standards - Determine data classification and protection requirements - Establish internal policies - Advocate and 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)

Topic	Details
	- Ensure that appropriate regulatory compliance statements and requirements are included in contractual agreements - Monitor and enforce compliance with contractual agreements
Manage security awareness and training programs	- Promote security programs to key stakeholders - Identify needs and implement training programs 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) - Associate Key Performance Indicators (KPI) to the risk posture of the organization - Use metrics to drive security program development and operations
Prepare, Obtain and Administer Security Budget	- Prepare and secure annual budget - Adjust budget based on evolving risks and threat landscape - Manage and report financial responsibilities
Manage Security Programs	- Define roles and responsibilities - Determine and manage team accountability - Build cross-functional relationships - Resolve conflicts between security and other stakeholders - Identify communication bottlenecks and barriers - Integrate security controls into human resources processes
Apply Product Development and Project Management Principles	- Incorporate security into project lifecycle - Identify and apply appropriate project management methodology - Analyze project time, scope and cost relationship
Systems Lifecycle Management - 18%	
Manage integration of security into Systems	- Integrate information security gates (decision points) and requirements into lifecycle - Implement security controls into system lifecycle

Topic	Details
Development Life Cycle (SDLC)	- Oversee security configuration management (CM) processes
Integrate New Business Initiatives and Emerging Technologies into the Security Architecture	- Integrate security into new business initiatives and emerging technologies - Address impact of new business initiatives on security posture
Define and Oversee Comprehensive Vulnerability Management Programs (e.g., vulnerability scanning, penetration testing, threat analysis)	- Identify, classify and prioritize assets, systems and services based on criticality to business - Prioritize threats and vulnerabilities - Manage security testing - Manage mitigation and/or remediation of vulnerabilities based on risk
Manage Security Aspects of Change Control	- Integrate security requirements with change control process - Identify and coordinate with the stakeholders - Manage documentation and tracking - Ensure policy compliance (e.g., continuous monitoring)
Risk Management - 19%	
Develop and Manage a Risk Management Program	- Identify risk management program objectives - Communicate and agree on risk management objectives with risk owners and other stakeholders - Determine scope of organizational risk program - Identify organizational security risk tolerance/appetite - Obtain and verify organizational asset inventory - Analyze organizational risks - Determine countermeasures, compensating and mitigating controls - Perform cost-benefit analysis (CBA) of risk treatment options

Topic	Details
Conduct Risk Assessments	- Identify risk factors
Manage security risks within the supply chain (e.g., supplier, vendor, third-party risk)	- Identify supply chain security risk requirements - Integrate supply chain security risks into organizational risk management - Validate security risk control within the supply chain - Monitor and review the supply chain security risks
Threat Intelligence and Incident Management - 17%	
Establish and Maintain Threat Intelligence Program	- Aggregate threat data from multiple threat intelligence sources - Conduct baseline analysis of network traffic, data and user behavior - Detect and analyze anomalous behavior patterns for potential concerns - Conduct threat modeling - Identify and categorize an attack - Correlate related security event and threat data - 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 - 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)
Contingency Management - 15%	
Facilitate development of contingency plans	- Identify and analyze factors related to the Continuity of Operations Plan (COOP) - Identify and analyze factors related to the business continuity plan (BCP) (e.g., time, resources, verification) - Identify and analyze factors related to the disaster

Topic	Details
	recovery plan (DRP) (e.g., time, resources, verification) - Coordinate contingency management plans with key stakeholders - Define internal and external crisis communications plans - Define and communicate contingency roles and responsibilities - Identify and analyze contingency impact on business processes and priorities - Manage third-party contingency dependencies - Prepare security management succession plan
Develop recovery strategies	- Identify and analyze alternatives - Recommend and coordinate recovery strategies - Assign recovery roles and responsibilities
Maintain contingency plan, Continuity of Operations Plan (COOP), business continuity plan (BCP) and disaster recovery plan (DRP)	- Plan testing, evaluation and modification - Determine survivability and resiliency capabilities - Manage plan update process
Manage disaster response and recovery process	- Declare disaster - Implement plan - Restore normal operations - Gather lessons learned - Update plan based on lessons learned
Law, Ethics and Security Compliance Management - 11%	
Identify the impact of laws and regulations that relate to information security	- Identify applicable privacy laws - Identify legal jurisdictions the organization and users operate within (e.g., trans-border data flow) - Identify export laws - Identify intellectual property (IP) laws - Identify applicable industry regulations - Identify and advise on non-compliance risks

Topic	Details
Adhere to the (ISC)2 Code of Ethics as related to management issues	
Validate compliance in accordance with applicable laws, regulations and industry best practices	- Inform and advise senior management - Evaluate and select compliance framework(s) - Implement the compliance framework(s) - Define and monitor compliance metrics
Coordinate with auditors and regulators in support of the internal and external audit processes	- Plan - Schedule - Coordinate audit activities - Evaluate and validate findings - Formulate response - Validate implemented mitigation and remediation actions
Document and Manage Compliance Exceptions	- Identify and document compensating controls and workarounds - Report and obtain authorized approval of risk waiver

ISC2 CISSP-ISSMP Sample Questions:

Question: 1

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: 2

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: 3

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

Question: 4

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: 5

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: 6

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: 7

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: 8

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: 9

How many change control systems are there in project management?

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

Answer: b

Question: 10

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

Study Guide to Crack ISC2 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