EDUSUM

#1 Online Certification Guide

ISC2 CISSP

ISC2 CISSP Certification Questions & Answers

Exam Summary – Syllabus –Questions

CISSP

ISC2 Certified Information Systems Security Professional (CISSP)

100-150 Questions Exam – 700/1000 Cut Score – Duration of 180 minutes

Table of Contents:

Know Your CISSP Certification Well:

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

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

Passing the CISSP exam makes you ISC2 Certified Information Systems Security Professional (CISSP). Having the CISSP 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 Certification Details:

Exam Name	ISC2 Certified Information Systems Security Professional (CISSP)
Exam Code	CISSP
Exam Price	$699 (USD)
Duration	180 mins
Number of Questions	100-150
Passing Score	700/1000
Schedule Exam	**Pearson VUE**
Sample Questions	**ISC2 CISSP Sample Questions**
Practice Exam	**ISC2 CISSP Certification Practice Exam**

CISSP Syllabus:

Topic	Details
Security and Risk Management - 15%	
Understand and apply concepts of confidentiality, integrity and availability	
Evaluate and apply security governance principles	- Alignment of security function to business strategy, goals, mission, and objectives - Organizational processes (e.g., acquisitions, divestitures, governance committees) - Organizational roles and responsibilities - Security control frameworks - Due care/due diligence
Determine compliance requirements	- Contractual, legal, industry standards, and regulatory requirements - Privacy requirements
Understand legal and regulatory issues that pertain to information security in a global context	- Cyber crimes and data breaches - Licensing and intellectual property requirements - Import/export controls - Trans-border data flow - Privacy
Understand, adhere to, and promote professional ethics	- (ISC)² Code of Professional Ethics - Organizational code of ethics
Develop, document, and implement security policy, standards, procedures, and guidelines	
Identify, analyze, and prioritize Business Continuity (BC) requirements	- Develop and document scope and plan - Business Impact Analysis (BIA)
Contribute to and enforce personnel security policies and procedures	- Candidate screening and hiring - Employment agreements and policies - Onboarding and termination processes - Vendor, consultant, and contractor agreements and controls - Compliance policy requirements - Privacy policy requirements
Understand and apply risk management concepts	- Identify threats and vulnerabilities - Risk assessment/analysis - Risk response - Countermeasure selection and

	implementation - Applicable types of controls (e.g., preventive, detective, corrective) - Security Control Assessment (SCA) - Monitoring and measurement - Asset valuation - Reporting - Continuous improvement - Risk frameworks
Understand and apply threat modeling concepts and methodologies	- Threat modeling methodologies - Threat modeling concepts
Apply risk-based management concepts to the supply chain	- Risks associated with hardware, software, and services - Third-party assessment and monitoring - Minimum security requirements - Service-level requirements
Establish and maintain a security awareness, education, and training program	- Methods and techniques to present awareness and training - Periodic content reviews - Program effectiveness evaluation
Asset Security - 10%	
Identify and classify information and assets	- Data classification - Asset Classification
Determine and maintain information and asset ownership	
Protect privacy	- Data owners - Data processers - Data remanence - Collection limitation
Ensure appropriate asset retention	
Determine data security controls	- Understand data states - Scoping and tailoring - Standards selection - Data protection methods
Establish information and asset handling requirements	
Security Architecture and Engineering - 13%	
Implement and manage engineering processes using secure design principles	

Understand the fundamental concepts of security models	
Select controls based upon systems security requirements	
Understand security capabilities of information systems (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)	
Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements	- Client-based systems - Server-based systems - Database systems - Cryptographic systems - Industrial Control Systems (ICS) - Cloud-based systems - Distributed systems - Internet of Things (IoT)
Assess and mitigate vulnerabilities in web-based systems	
Assess and mitigate vulnerabilities in mobile systems	
Assess and mitigate vulnerabilities in embedded devices	
Apply cryptography	- Cryptographic life cycle (e.g., key management, algorithm selection) - Cryptographic methods (e.g., symmetric, asymmetric, elliptic curves) - Public Key Infrastructure (PKI) - Key management practices - Digital signatures - Non-repudiation - Integrity (e.g., hashing) - Understand methods of cryptanalytic attacks - Digital Rights Management (DRM)
Apply security principles to site and facility design	
Implement site and facility security controls	- Wiring closets/intermediate distribution facilities - Server rooms/data centers - Media storage facilities - Evidence storage

	- Restricted and work area security - Utilities and Heating, Ventilation, and Air Conditioning (HVAC) - Environmental issues - Fire prevention, detection, and suppression
Communication and Network Security - 14%	
Implement secure design principles in network architectures	- Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) models - Internet Protocol (IP) networking - Implications of multilayer protocols - Converged protocols - Software-defined networks - Wireless networks
Secure network components	- Operation of hardware - Transmission media - Network Access Control (NAC) devices - Endpoint security - Content-distribution networks
Implement secure communication channels according to design	- Voice - Multimedia collaboration - Remote access - Data communications - Virtualized networks
Identity and Access Management (IAM) - 13%	
Control physical and logical access to assets	- Information - Systems - Devices - Facilities
Manage identification and authentication of people, devices, and services	- Identity management implementation - Single/multi-factor authentication - Accountability - Session management - Registration and proofing of identity - Federated Identity Management (FIM) - Credential management systems
Integrate identity as a third-party service	- On-premise - Cloud - Federated

Implement and manage authorization mechanisms	- Role Based Access Control (RBAC) - Rule-based access control - Mandatory Access Control (MAC) - Discretionary Access Control (DAC) - Attribute Based Access Control (ABAC)
Manage the identity and access provisioning lifecycle	- User access review - System account access review - Provisioning and deprovisioning
Security Assessment and Testing - 12%	
Design and validate assessment, test, and audit strategies	- Internal - External - Third-party
Conduct security control testing	- Vulnerability assessment - Penetration testing - Log reviews - Synthetic transactions - Code review and testing - Misuse case testing - Test coverage analysis - Interface testing
Collect security process data (e.g., technical and administrative)	- Account management - Management review and approval - Key performance and risk indicators - Backup verification data - Training and awareness - Disaster Recovery (DR) and Business Continuity (BC)
Analyze test output and generate report	
Conduct or facilitate security audits	- Internal - External - Third-party
Security Operations - 13%	
Understand and support investigations	- Evidence collection and handling - Reporting and documentation - Investigative techniques - Digital forensics tools, tactics, and procedures
Understand requirements for investigation types	- Administrative - Criminal - Civil

	- Regulatory - Industry standards
Conduct logging and monitoring activities	- Intrusion detection and prevention - Security Information and Event Management (SIEM) - Continuous monitoring - Egress monitoring
Securely provisioning resources	- Asset inventory - Asset management - Configuration management
Understand and apply foundational security operations concepts	- Need-to-know/least privileges - Separation of duties and responsibilities - Privileged account management - Job rotation - Information lifecycle - Service Level Agreements (SLA)
Apply resource protection techniques	- Media management - Hardware and software asset management
Conduct incident management	- Detection - Response - Mitigation - Reporting - Recovery - Remediation - Lessons learned
Operate and maintain detective and preventative measures	- Firewalls - Intrusion detection and prevention systems - Whitelisting/blacklisting - Third-party provided security services - Sandboxing - Honeypots/honeynets - Anti-malware
Implement and support patch and vulnerability management	
Understand and participate in change management processes	
Implement recovery strategies	- Backup storage strategies - Recovery site strategies - Multiple processing sites - System resilience, high availability, Quality of Service (QoS), and fault tolerance

Implement Disaster Recovery (DR) processes	- Response - Personnel - Communications - Assessment - Restoration - Training and awareness
Test Disaster Recovery Plans (DRP)	- Read-through/tabletop - Walkthrough - Simulation - Parallel - Full interruption
Participate in Business Continuity (BC) planning and exercises	
Implement and manage physical security	- Perimeter security controls - Internal security controls
Address personnel safety and security concerns	- Travel - Security training and awareness - Emergency management - Duress
Software Development Security - 10%	
Understand and integrate security in the Software Development Life Cycle (SDLC)	- Development methodologies - Maturity models - Operation and maintenance - Change management - Integrated product team
Identify and apply security controls in development environments	- Security of the software environments - Configuration management as an aspect of secure coding - Security of code repositories
Assess the effectiveness of software security	- Auditing and logging of changes - Risk analysis and mitigation
Assess security impact of acquired software	
Define and apply secure coding guidelines and standards	- Security weaknesses and vulnerabilities at the source-code level - Security of application programming interfaces - Secure coding practices

ISC2 CISSP Sample Questions:

Question: 1

While an Enterprise Security Architecture (ESA) can be applied in many different ways, it is focused on a few key goals. Identify the proper listing of the goals for the ESA:

a) It represents a simple, long term view of control, it provides a unified vision for common security controls, it leverages existing technology investments, it provides a fixed approach to current and future threats and also the needs of peripheral functions
b) It represents a simple, long term view of control, it provides a unified vision for common security controls, it leverages new technology investments, it provides a flexible approach to current and future threats and also the needs of core functions
c) It represents a complex, short term view of control, it provides a unified vision for common security controls, it leverages existing technology investments, it provides a flexible approach to current and future threats and also the needs of core functions
d) It represents a simple, long term view of control, it provides a unified vision for common security controls, it leverages existing technology investments, it provides a flexible approach to current and future threats and also the needs of core functions

Answer: d

Question: 2

Ann installs a new Wireless Access Point (WAP) and users are able to connect to it. However, once connected, users cannot access the Internet. Which of the following is the MOST likely cause of the problem?

a) The signal strength has been degraded and latency is increasing hop count.
b) An incorrect subnet mask has been entered in the WAP configuration.
c) The signal strength has been degraded and packets are being lost.
d) Users have specified the wrong encryption type and packets are being rejected.

Answer: b

Question: 3

Technical evaluation of assurance to ensure that security requirements have been met is known as?

a) Accreditation
b) Certification
c) Validation
d) Verification

Answer: b

Question: 4

The process for developing an ISCM strategy and implementing an ISCM program is?

a) Define, analyze, implement, establish, respond, review and update
b) Analyze, implement, define, establish, respond, review and update
c) Define, establish, implement, analyze, respond, review and update
d) Implement, define, establish, analyze, respond, review and update

Answer: c

Question: 5

Qualitative risk assessment is earmarked by which of the following?

a) Ease of implementation and it can be completed by personnel with a limited understanding of the risk assessment process
b) Can be completed by personnel with a limited understanding of the risk assessment process and uses detailed metrics used for calculation of risk
c) Detailed metrics used for calculation of risk and ease of implementation
d) Can be completed by personnel with a limited understanding of the risk assessment process and detailed metrics used for the calculation of risk

Answer: a

Question: 6

Which of the following can BEST be used to capture detailed security requirements?

a) Threat modeling, covert channels, and data classification
b) Data classification, risk assessments, and covert channels
c) Risk assessments, covert channels, and threat modeling
d) Threat modeling, data classification, and risk assessments

Answer: d

Question: 7

What are the seven main categories of access control?

a) Detective, corrective, monitoring, logging, recovery, classification, and directive
b) Directive, deterrent, preventative, detective, corrective, compensating, and recovery
c) Authorization, identification, factor, corrective, privilege, detective, and directive
d) Identification, authentication, authorization, detective, corrective, recovery, and directive

Answer: b

Question: 8

Which of the following security models is primarily concerned with how the subjects and objects are created and how subjects are assigned rights or privileges?

a) Bell–LaPadula
b) Biba-Integrity
c) Chinese Wall
d) Graham–Denning

Answer: d

Question: 9

Before applying a software update to production systems, it is MOST important that

a) Full disclosure information about the threat that the patch addresses is available
b) The patching process is documented
c) The production systems are backed up
d) An independent third party attests the validity of the patch

Answer: c

Question: 10

A potential vulnerability of the Kerberos authentication server is

a) Single point of failure
b) Asymmetric key compromise
c) Use of dynamic passwords
d) Limited lifetimes for authentication credentials

Answer: a

Study Guide to Crack ISC2 CISSP Exam:

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