ISC2 CISSP

ISC2 CISSP Certification Questions & Answers

Get Instant Access to Vital Exam Acing Materials | Study Guide | Sample Questions | Practice Test

CISSP

ISC2 Certified Information Systems Security Professional (CISSP)

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




EDUSUM

#1 Online Certification Guide

Table of Contents:

Discover More about the CISSP Certification

Are you interested in passing the ISC2 CISSP exam? First discover, who benefits from the CISSP certification. The CISSP is suitable for a candidate if he wants to learn about Cybersecurity. Passing the CISSP exam earns you the ISC2 Certified Information Systems Security Professional (CISSP) title.

While preparing for the CISSP exam, many candidates struggle to get the necessary materials. But do not worry; your struggling days are over. The CISSP PDF contains some of the most valuable preparation tips and the details and instant access to useful **CISSP study materials just at one click.**

ISC2 CISSP Certification Details:

Exam Name	ISC2 Certified Information Systems Security Professional (CISSP)
Exam Code	CISSP
Exam Price	$499 (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, adhere to, and promote professional ethics	- (ISC)2 Code of Professional Ethics - Organizational code of ethics
Understand and apply security concepts	- Confidentiality, integrity, and availability, authenticity and nonrepudiation

Evaluate and apply security governance principles	- Alignment of the 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 and other requirements	- Contractual, legal, industry standards, and regulatory requirements - Privacy requirements
Understand legal and regulatory issues that pertain to information security in a holistic context	- Cybercrimes and data breaches - Licensing and Intellectual Property (IP) requirements - Import/export controls - Transborder data flow - Privacy
Understand requirements for investigation types (i.e., administrative, criminal, civil, regulatory, industry standards)	
Develop, document, and implement security policy, standards, procedures, and guidelines	
Identify, analyze, and prioritize Business Continuity (BC) requirements	- Business Impact Analysis (BIA) - Develop and document the scope and the plan
Contribute to and enforce personnel security policies and procedures	- Candidate screening and hiring - Employment agreements and policies - Onboarding, transfers, 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) - Control assessments (security and privacy) - Monitoring and measurement - Reporting - Continuous improvement (e.g., Risk maturity modeling) - Risk frameworks
Understand and apply threat modeling concepts and methodologies	
Apply Supply Chain Risk Management (SCRM) concepts	- 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 (e.g., social engineering, phishing, security champions, gamification) - Periodic content reviews - Program effectiveness evaluation
Asset Security - 10%	
Identify and classify information and assets	- Data classification - Asset Classification
Establish information and asset handling requirements	

Provision resources securely	- Information and asset ownership - Asset inventory (e.g., tangible, intangible) - Asset management
Manage data lifecycle	- Data roles (i.e., owners, controllers, custodians, processors, users/subjects) - Data collection - Data location - Data maintenance - Data retention - Data remanence - Data destruction
Ensure appropriate asset retention (e.g., End-of-Life (EOL), End-of-Support (EOS))	
Determine data security controls and compliance requirements	- Data states (e.g., in use, in transit, at rest) - Scoping and tailoring - Standards selection - Data protection methods (e.g., Digital Rights Management (DRM), Data Loss Prevention (DLP), Cloud Access Security Broker (CASB))
Security Architecture and Engineering - 13%	
Research, implement and manage engineering processes using secure design principles	- Threat modeling - Least privilege - Defense in depth - Secure defaults - Fail securely - Separation of Duties (SoD) - Keep it simple - Zero Trust - Privacy by design - Trust but verify - Shared responsibility

Understand the fundamental concepts of security models (e.g., Biba, Star Model, Bell-LaPadula)	
Select controls based upon systems security requirements	
Understand security capabilities of information systems (IS) (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 (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS)) - Distributed systems - Internet of Things (IoT) - Microservices - Containerization - Serverless - Embedded systems - High-Performance Computing (HPC) systems - Edge computing systems - Virtualized systems

Select and determine cryptographic solutions	- Cryptographic life cycle (e.g., keys, algorithm selection) - Cryptographic methods (e.g., symmetric, asymmetric, elliptic curves, quantum) - Public Key Infrastructure (PKI) - Key management practices - Digital signatures and digital certificates - Non-repudiation - Integrity (e.g., hashing)
Understand methods of cryptanalytic attacks	- Brute force - Ciphertext only - Known plaintext - Frequency analysis - Chosen ciphertext - Implementation attacks - Side-channel - Fault injection - Timing - Man-in-the-Middle (MITM) - Pass the hash - Kerberos exploitation - Ransomware
Apply security principles to site and facility design	
Design 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 - Power (e.g., redundant, backup)

Communication and Network Security - 13%	
Assess and implement secure design principles in network architectures	- Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) models - Internet Protocol (IP) networking (e.g., Internet Protocol Security (IPSec), Internet Protocol (IP) v4/6) - Secure protocols - Implications of multilayer protocols - Converged protocols (e.g., Fiber Channel Over Ethernet (FCoE), Internet Small Computer Systems Interface (iSCSI), Voice over Internet Protocol (VoIP)) - Micro-segmentation (e.g., Software Defined Networks (SDN), Virtual eXtensible Local Area Network (VXLAN), Encapsulation, Software-Defined Wide Area Network (SD WAN)) - Wireless networks (e.g., Li-Fi, Wi-Fi, Zigbee, satellite) - Cellular networks (e.g., 4G, 5G) - Content Distribution Networks (CDN)
Secure network components	- Operation of hardware (e.g., redundant power, warranty, support) - Transmission media - Network Access Control (NAC) devices - Endpoint security
Implement secure communication channels according to design	- Voice - Multimedia collaboration - Remote access - Data communications - Virtualized networks - Third-party connectivity
Identity and Access Management (IAM) - 13%	
Control physical and logical access to assets	- Information - Systems - Devices - Facilities - Applications

Manage identification and authentication of people, devices, and services	- Identity Management (IdM) implementation - Single/multi-factor authentication (MFA) - Accountability - Session management - Registration, proofing, and establishment of identity - Federated Identity Management (FIM) - Credential management systems - Single Sign On (SSO) - Just-In-Time (JIT)
Federated identity with a third-party service	- On-premise - Cloud - Hybrid
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) - Risk based access control
Manage the identity and access provisioning lifecycle	- Account access review (e.g., user, system, service) - Provisioning and deprovisioning (e.g., on /off boarding and transfers) - Role definition (e.g., people assigned to new roles) - Privilege escalation (e.g., managed service accounts, use of sudo, minimizing its use)
Implement authentication systems	- OpenID Connect (OIDC)/Open Authorization (Oauth) - Security Assertion Markup Language (SAML) - Kerberos - Remote Authentication Dial-In User Service (RADIUS)/Terminal Access Controller Access Control System Plus (TACACS+)
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 - Breach attack simulations - Compliance checks
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	- Remediation - Exception handling - Ethical disclosure
Conduct or facilitate security audits	- Internal - External - Third-party
Security Operations - 13%	
Understand and comply with investigations	- Evidence collection and handling - Reporting and documentation - Investigative techniques - Digital forensics tools, tactics, and procedures - Artifacts (e.g., computer, network, mobile device)
Conduct logging and monitoring activities	- Intrusion detection and prevention - Security Information and Event Management (SIEM) - Continuous monitoring - Egress monitoring - Log management - Threat intelligence (e.g., threat feeds, threat hunting) - User and Entity Behavior Analytics (UEBA)

Perform Configuration Management (CM) (e.g., provisioning, baselining, automation)	
Apply foundational security operations concepts	- Need-to-know/least privilege - Separation of Duties (SoD) and responsibilities - Privileged account management - Job rotation - Service Level Agreements (SLAs)
Apply resource protection	- Media management - Media protection techniques
Conduct incident management	- Detection - Response - Mitigation - Reporting - Recovery - Remediation - Lessons learned
Operate and maintain detective and preventative measures	- Firewalls (e.g., next generation, web application, network) - Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) - Whitelisting/blacklisting - Third-party provided security services - Sandboxing - Honeypots/honeynets - Anti-malware - Machine learning and Artificial Intelligence (AI) based tools
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 (HA), Quality of Service (QoS), and fault tolerance
Implement Disaster Recovery (DR) processes	- Response - Personnel - Communications - Assessment - Restoration - Training and awareness - Lessons learned
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 - 11%	
Understand and integrate security in the Software	- Development methodologies (e.g., Agile, Waterfall, DevOps, DevSecOps) - Maturity models (e.g., Capability Maturity Model (CMM), Software Assurance Maturity Model (SAMM))

Development Life Cycle (SDLC)	- Operation and maintenance - Change management - Integrated product team (IPT)
Identify and apply security controls in software development ecosystems	- Programming languages - Libraries - Tool sets - Integrated Development Environment (IDE) - Runtime - Continuous Integration and Continuous Delivery (CI/CD) - Security Orchestration, Automation, and Response (SOAR) - Software Configuration Management (SCM) - Code repositories - Application security testing (e.g., Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST))
Assess the effectiveness of software security	- Auditing and logging of changes - Risk analysis and mitigation
Assess security impact of acquired software	- Commercial-off-the-shelf (COTS) - Open source - Third-party - Managed services (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))
Define and apply secure coding guidelines and standards	- Security weaknesses and vulnerabilities at the source-code level - Security of Application Programming Interfaces (APIs) - Secure coding practices - Software-defined security

Broaden Your Knowledge with ISC2 CISSP Sample Questions:

Question: 1

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: 2

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: 3

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: 4

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: 5

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: 6

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: 7

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

Question: 8

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: 9

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: 10

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

Avail the Study Guide to Pass ISC2 CISSP Exam:

- Find out about the CISSP syllabus topics. Visiting the official site offers an idea about the exam structure and other important study resources. Going through the syllabus topics help to plan the exam in an organized manner.
- Once you are done exploring the **CISSP syllabus**, it is time to plan for studying and covering the syllabus topics from the core. Chalk out the best plan for yourself to cover each part of the syllabus in a hassle-free manner.
- A study schedule helps you to stay calm throughout your exam preparation. It should contain your materials and thoughts like study hours, number of topics for daily studying mentioned on it. The best bet to clear the exam is to follow your schedule rigorously.
- The candidate should not miss out on the scope to learn from the CISSP training. Joining the ISC2 provided training for CISSP exam helps a candidate to strengthen his practical knowledge base from the certification.
- Learning about the probable questions and gaining knowledge regarding the exam structure helps a lot. Go through the **CISSP sample questions** and boost your knowledge
- Make yourself a pro through online practicing the syllabus topics. CISSP practice tests would guide you on your strengths and weaknesses regarding the syllabus topics. Through rigorous practicing, you can improve the weaker sections too. Learn well about time management during exam and become confident gradually with practice tests.

Career Benefits:

- Passing the CISSP exam, helps a candidate to prosper highly in his career. Having the certification on the resume adds to the candidate's benefit and helps to get the best opportunities.

Here Is the Trusted Practice Test for the CISSP Certification

EduSum.Com is here with all the necessary details regarding the CISSP exam. We provide authentic practice tests for the CISSP exam. What do you gain from these practice tests? You get to experience the real exam-like questions made by industry experts and get a scope to improve your performance in the actual exam. Rely on EduSum.Com for rigorous, unlimited two-month attempts on the **CISSP practice tests**, and gradually build your confidence. Rigorous practice made many aspirants successful and made their journey easy towards grabbing the ISC2 Certified Information Systems Security Professional (CISSP).

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