EDUSUM

#1 Online Certification Guide

ISC2 CISSP

ISC2 Information Systems Security Professional Certification Questions & Answers

Exam Summary – Syllabus –Questions

CISSP

ISC2 Certified Information Systems Security Professional (CISSP)

125-175 Questions Exam – 700/1000 Cut Score – Duration of 240 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 ISC2 Information Systems Security Professional materials like CISSP 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 ISC2 Information Systems Security Professional certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

CISSP ISC2 Information Systems Security Professional Certification Details:

Exam Name	ISC2 Certified Information Systems Security Professional (CISSP)
Exam Code	CISSP
Exam Price	$749 (USD)
Duration	240 mins
Number of Questions	125-175
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,	- Methods and techniques to present awareness and training (e.g., social engineering, phishing, security champions, gamification)

education, and training program	- 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	- Threat modeling - Least privilege

engineering processes using secure design principles	- 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 Life Cycle (SDLC)	- Development methodologies (e.g., Agile, Waterfall, DevOps, DevSecOps) - Maturity models (e.g., Capability Maturity Model (CMM), Software Assurance Maturity Model (SAMM)) - 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

ISC2 CISSP Sample Questions:

Question: 1

This process establishes periodic meetings to manage and schedule major software, hardware, and security updates to the organization. This process is known as _____.

a) Change and configuration management
b) Upgrade and update management
c) Patch management
d) Systems and operational management

Answer: a

Question: 2

What communication connectors provide the BEST defense and security for leaked authentication vulnerabilities?

a) RJ-45
b) BNC
c) RJ-11
d) SC

Answer: d

Question: 3

After powering on a computer, it eventually boots the Linux operating system. Which of the following loads the kernel?

a) BIOS
b) MBR
c) UEFI
d) USER

Answer: b

Question: 4

Which of the following represents an acceptable amount of data loss measured in time?

a) RTO
b) Maximum tolerable downtime (MTD)
c) RPO
d) Work recovery time (WRT)

Answer: c

Question: 5

Which of the following is the Least important when securing backup tapes?

a) Test backup data to confirm the integrity of records saved to tape.
b) Easy access to tapes outside the SOC for quick availability.
c) Encrypt backup data on tapes to maintain the confidentiality of data.
d) Keep versions of backup tapes miles from the originating environment in case of serious incident or disaster.

Answer: b

Question: 6

Retinal and fingerprint scanners do which of the following when enrolling a new user, if designed securely?

a) Save an image of the user's retina or fingerprint, and then encrypt the image.
b) Convert the user's retina or fingerprint image into a hash, and then encrypt the hash.
c) Save an image of the user's retina or fingerprint.
d) Convert the user's retina or fingerprint image into a hash.

Answer: b

Question: 7

Egor is an administrator at VBC Corp. and sends encrypted messages to his boss. Which keys are distributed?

a) Public
b) Private
c) Passwords
d) Encrypted

Answer: a

Question: 8

When prioritizing use cases, at a minimum, the use cases must be designed for which of the following?

a) Security-related requirements
b) Input validation
c) All requirements
d) Poorly defined business requirements

Answer: d

Question: 9

When a system fails to display leaky banners, information that's useful to a hacker is visible in error messages. This is an example of which type of attack?

a) Leaky attack
b) Social engineering
c) Banner attack
d) Reading attack

Answer: c

Question: 10

What is an organization's largest security risk when it comes to using open source applications?

a) The source code is visible by anyone in the world.
b) The operations department does not install version updates and patches in a timely manner.
c) The creator(s) of the application may not have used secure software development procedures.
d) The creator(s) decide to discontinue further development of the application.

Answer: c

Study Guide to Crack ISC2 Information Systems Security Professional 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.