EDUSUM

#1 Online Certification Guide

ISC2 CCSP

ISC2 Cloud Security Professional Certification Questions & Answers

Exam Summary – Syllabus –Questions

CCSP

ISC2 Certified Cloud Security Professional (CCSP)

125 Questions Exam – 700/1000 Cut Score – Duration of 180 minutes

Table of Contents:

Know Your CCSP Certification Well:

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

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

Passing the CCSP exam makes you ISC2 Certified Cloud Security Professional (CCSP). Having the Cloud 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.

ISC2 CCSP Cloud Security Professional Certification Details:

Exam Name	ISC2 Certified Cloud Security Professional (CCSP)
Exam Code	CCSP
Exam Price	$599 (USD)
Duration	180 mins
Number of Questions	125
Passing Score	700/1000
Schedule Exam	**Pearson VUE**
Sample Questions	**ISC2 CCSP Sample Questions**
Practice Exam	**ISC2 CCSP Certification Practice Exam**

CCSP Syllabus:

Topic	Details
Cloud Concepts, Architecture and Design (17%)	
Understand Cloud Computing Concepts	- Cloud Computing Definitions - Cloud Computing Roles (e.g., cloud service customer, cloud service provider, cloud service partner, cloud service broker) - Key Cloud Computing Characteristics (e.g., on-demand self-service, broad network access, multi-tenancy, rapid elasticity and scalability, resource pooling, measured service) - Building Block Technologies (e.g., virtualization, storage, networking, databases, orchestration)
Describe Cloud Reference Architecture	- Cloud Computing Activities - Cloud Service Capabilities (e.g., application capability types, platform capability types, infrastructure capability types - Cloud Service Categories (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS)) - Cloud Deployment Models (e.g., public, private, hybrid, community) - Cloud Shared Considerations (e.g., interoperability, portability, reversibility, availability, security, privacy, resiliency, performance, governance, maintenance and versioning, service levels and Service Level Agreements (SLA), auditability, regulatory) - Impact of Related Technologies (e.g., machine learning, artificial intelligence, blockchain, Internet of Things (IoT), containers, quantum computing)
Understand Security Concepts Relevant to Cloud Computing	- Cryptography and Key Management - Access Control - Data and Media Sanitization (e.g., overwriting, cryptographic erase) - Network Security (e.g., network security groups) - Virtualization Security (e.g., hypervisor security, container security - Common Threats
Understand Design Principles of Secure Cloud Computing	- Cloud Secure Data Lifecycle - Cloud based Disaster Recovery (DR) and Business

Topic	Details
	Continuity (BC) planning - Cost Benefit Analysis - Functional Security Requirements (e.g., portability, interoperability, vendor lock-in) - Security Considerations for Different Cloud Categories (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))
Evaluate Cloud Service Providers	- Verification Against Criteria (e.g., International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27017, Payment Card Industry Data Security Standard (PCI DSS)) - System/subsystem Product Certifications (e.g., Common Criteria (CC), Federal Information Processing Standard (FIPS) 140-2)
Cloud Data Security (19%)	
Describe Cloud Data Concepts	- Cloud Data Life Cycle Phases - Data Dispersion
Design and Implement Cloud Data Storage Architectures	- Storage Types (e.g. long term, ephemeral, raw-disk) - Threats to Storage Types
Design and Apply Data Security Technologies and Strategies	- Encryption and Key Management - Hashing - Masking - Tokenization - Data Loss Prevention (DLP) - Data Obfuscation - Data De-identification (e.g., anonymization)
Implement Data Discovery	- Structured Data - Unstructured Data
Implement Data Classification	- Mapping - Labeling - Sensitive data (e.g., Protected Health Information (PHI), Personally Identifiable Information (PII), card holder data)
Design and Implement Information Rights Management (IRM)	- Objectives (e.g., data rights, provisioning, access models) - Appropriate Tools (e.g., issuing and revocation of certificates)
Plan and Implement Data Retention, Deletion and Archiving Policies	- Data Retention Policies - Data Deletion Procedures and Mechanisms

Topic	Details
	- Data Archiving Procedures and Mechanisms - Legal Hold
Design and Implement Auditability, Traceability and Accountability of Data Events	- Definition of Event Sources and Requirement of Identity Attribution - Logging, Storage and Analysis of Data Events - Chain of Custody and Non-repudiation
Cloud Platform and Infrastructure Security (17%)	
Comprehend Cloud Infrastructure Components	- Physical Environment - Network and Communications - Compute - Virtualization - Storage - Management Plane
Design a Secure Data Center	- Logical Design (e.g., tenant partitioning, access control) - Physical Design (e.g. location, buy or build) - Environmental Design (e.g., Heating, Ventilation and Air Conditioning (HVAC), multi-vendor pathway connectivity)
Analyze Risks Associated with Cloud Infrastructure	- Risk Assessment and Analysis - Cloud Vulnerabilities, Threats and Attacks - Virtualization Risks - Counter-measure Strategies
Design and Plan Security Controls	- Physical and Environmental Protection (e.g., on-premise) - System and Communication Protection - Virtualization Systems Protection - Identification, Authentication and Authorization in Cloud Infrastructure - Audit Mechanisms (e.g., log collection, packet capture)
Plan Disaster Recovery (DR) and Business Continuity (BC)	- Risks Related to the Cloud Environment - Business Requirements (e.g., Recovery Time Objective (RTO), Recovery Point Objective (RPO), Recovery Service Level (RSL)) - Business Continuity/Disaster Recovery Strategy - Creation, Implementation and Testing of Plan
Cloud Application Security (17%)	
Advocate Training and Awareness for Application Security	- Cloud Development Basics - Common Pitfalls - Common Cloud Vulnerabilities

Topic	Details
Describe the Secure Software Development Life Cycle (SDLC) Process	- Business Requirements - Phases and Methodologies
Apply the Secure Software Development Life Cycle (SDLC)	- Avoid Common Vulnerabilities During Development - Cloud-specific Risks - Quality Assurance - Threat Modeling - Software Configuration Management and Versioning
Apply Cloud Software Assurance and Validation	- Functional Testing - Security Testing Methodologies
Use Verified Secure Software	- Approved Application Programming Interfaces (API) - Supply-chain Management - Third Party Software Management - Validated Open Source Software
Comprehend the Specifics of Cloud Application Architecture	- Supplemental Security components (e.g., Web Application Firewall (WAF), Database Activity Monitoring (DAM), Extensible Markup Language (XML) firewalls, Application Programming Interface (API) gateway) - Cryptography - Sandboxing - Application Virtualization and Orchestration
Design Appropriate Identity and Access Management (IAM) Solutions	- Federated Identity - Identity Providers - Single Sign-On (SSO) - Multi-factor Authentication - Cloud Access Security Broker (CASB)
Cloud Security Operations (17%)	
Implement and Build Physical and Logical Infrastructure for Cloud Environment	- Hardware Specific Security Configuration Requirements (e.g., Basic Input Output System (BIOS), settings for virtualization and Trusted Platform Module (TPM), storage controllers, network controllers) - Installation and Configuration of Virtualization Management Tools - Virtual Hardware Specific Security Configuration Requirements (e.g., network, storage, memory, Central Processing Unit (CPU)) - Installation of Guest Operating System (OS) Virtualization Toolsets

Topic	Details
Operate Physical and Logical Infrastructure for Cloud Environment	- Configure Access Control for Local and Remote Access (e.g., Secure Keyboard Video Mouse (KVM), console-based access mechanisms, Remote Desktop Protocol (RDP)) - Secure Network Configuration (e.g., Virtual Local Area Networks (VLAN), Transport Layer Security (TLS), Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), Virtual Private Network (VPN)) - Operating System (OS) Hardening Through the Application of Baselines (e.g., Windows, Linux, VMware) - Availability of Stand-Alone Hosts - Availability of Clustered Hosts (e.g., Distributed Resource Scheduling (DRS), Dynamic Optimization (DO), storage clusters, maintenance mode, High Availability) - Availability of Guest Operating System (OS)
Manage Physical and Logical Infrastructure for Cloud Environment	- Access Controls for Remote Access (e.g., Remote Desktop Protocol (RDP), Secure Terminal Access, Secure Shell (SSH)) - Operating System (OS) Baseline Compliance Monitoring and Remediation - Patch Management - Performance and Capacity Monitoring (e.g., network, compute, storage, response time) - Hardware Monitoring (e.g., Disk, Central Processing Unit (CPU), fan speed, temperature) - Configuration of Host and Guest Operating System (OS) Backup and Restore Functions - Network Security Controls (e.g., firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), honeypots, vulnerability assessments, network security groups) - Management Plane (e.g., scheduling, orchestration, maintenance)
Implement Operational Controls and Standards (e.g., Information Technology Infrastructure Library (ITIL), International Organization for Standardization/International	- Change Management - Continuity Management - Information Security Management - Continual Service Improvement Management - Incident Management - Problem Management - Release Management - Deployment Management

Topic	Details
Electrotechnical Commission (ISO/IEC) 20000-1)	- Configuration Management - Service level Management - Availability Management - Capacity Management
Support Digital Forensics	- Forensic Data Collection Methodologies - Evidence Management - Collect, Acquire and Preserve Digital Evidence
Manage Communication with Relevant Parties	- Vendors - Customers - Partners - Regulators - Other Stakeholders
Manage Security Operations	- Security Operations Center (SOC) - Monitoring of Security Controls (e.g., firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), honeypots, vulnerability assessments, network security groups) - Log Capture and Analysis (e.g., Security Information and Event Management (SIEM), log management) - Incident Management
Legal, Risk and Compliance (13%)	
Articulate Legal Requirements and Unique Risks within the Cloud Environment	- Conflicting International Legislation - Evaluation of Legal Risks Specific to Cloud Computing - Legal Framework and Guidelines - eDiscovery (e.g., International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27050, Cloud Security Alliance (CSA) Guidance) - Forensics Requirements
Understand Privacy Issues	- Difference Between Contractual and Regulated Private Data (e.g., Protected Health Information (PHI), Personally Identifiable Information (PII)) - Country-Specific Legislation Related to Private Data (e.g., Protected Health Information (PHI), Personally Identifiable Information (PII)) - Jurisdictional Differences in Data Privacy - Standard Privacy Requirements (e.g., International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27018, Generally

Topic	Details
	Accepted Privacy Principles (GAPP), General Data Protection Regulation (GDPR))
Understand Audit Process, Methodologies, and Required Adaptations for a Cloud Environment	- Internal and External Audit Controls - Impact of Audit Requirements - Identify Assurance Challenges of Virtualization and Cloud - Types of Audit Reports (e.g., Statement on Standards for Attestation Engagements (SSAE), Service Organization Control (SOC), International Standard on Assurance Engagements (ISAE)) - Restrictions of Audit Scope Statements (e.g., Statement on Standards for Attestation Engagements (SSAE), International Standard on Assurance Engagements (ISAE)) - Gap Analysis - Audit Planning - Internal Information Security Management System (ISMS) - Internal Information Security Controls System - Policies (e.g., organizational, functional, cloud computing) - Identification and Involvement of Relevant Stakeholders - Specialized Compliance Requirements for Highly-Regulated Industries (e.g., North American Electric Reliability Corporation/ Critical Infrastructure Protection (NERC/CIP), Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI)) - Impact of Distributed Information Technology (IT) Model (e.g., diverse geographical locations and crossing over legal jurisdictions
Understand Implications of Cloud to Enterprise Risk Management	- Assess Providers Risk Management Programs (e.g., controls, methodologies, policies) - Difference Between Data Owner/Controller vs. Data Custodian/Processor (e.g., risk profile, risk appetite, responsibility) - Regulatory Transparency Requirements (e.g., breach notification, Sarbanes-Oxley (SOX), General Data Protection Regulation (GDPR)) - Risk Treatment (i.e., avoid, modify, share, retain) - Different Risk Frameworks - Metrics for Risk Management

Topic	Details
	- Assessment of Risk Environment (e.g., service, vendor, infrastructure)
Understand Outsourcing and Cloud Contract Design	- Business Requirements (e.g., Service Level Agreement (SLA), Master Service Agreement (MSA), Statement of Work (SOW)) - Vendor Management - Contract Management (e.g., right to audit, metrics, definitions, termination, litigation, assurance, compliance, access to cloud/data, cyber risk insurance) - Supply-Chain Management (e.g., International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27036)

ISC2 CCSP Sample Questions:

Question: 1

Software developers designing applications for the cloud should expect to include options to ensure all of the following capabilities except _____.

a) Encryption of data at rest
b) Encryption of data in transit
c) Data masking
d) Hashing database fields

Answer: d

Question: 2

How often should cable management efforts take place?

a) Annually
b) Continually
c) Quarterly
d) Weekly

Answer: b

Question: 3

Heating, ventilation, and air conditioning (HVAC) systems cool the data center by pushing warm air into _____.

a) The server inlets
b) Underfloor plenums
c) HVAC intakes
d) The outside world

Answer: d

Question: 4

When building a new data center within an urban environment, which of the following is probably the most restrictive aspect?

a) The size of the plot
b) Utility availability
c) Staffing
d) Municipal codes

Answer: d

Question: 5

In a platform as a service (PaaS) model, who should most likely be responsible for the security of the applications in the production environment?

a) Cloud customer
b) Cloud provider
c) Regulator
d) Programmers

Answer: a

Question: 6

In which court must the defendant be determined to have acted in a certain fashion according to the preponderance of the evidence?

a) Civil court
b) Criminal court
c) Religious court
d) Tribal court

Answer: a

Question: 7

What is the most secure form of code testing and review?

a) Open source
b) Proprietary/internal
c) Neither open source nor proprietary
d) Combination of open source and proprietary

Answer: d

Question: 8

From a security perspective, automation of configuration aids in _____.

a) Enhancing performance
b) Reducing potential attack vectors
c) Increasing ease of use of the systems
d) Reducing need for administrative personnel

Answer: b

Question: 9

Which phase of the software development lifecycle (SDLC) is most likely to involve crypto-shredding?

a) Define
b) Design
c) Test
d) Disposal

Answer: d

Question: 10

An event is something that can be measured within the environment. An incident is a(n) _____ event.

a) Deleterious
b) Negative
c) Unscheduled
d) Major

Answer: c

Study Guide to Crack ISC2 Cloud Security Professional CCSP Exam:

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

Reliable Online Practice Test for CCSP Certification

Make EduSum.com your best friend during your ISC2 Certified Cloud Security Professional (CCSP) exam preparation. We provide authentic practice tests for the CCSP exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual CCSP 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 CCSP exam.

Start Online practice of CCSP Exam by visiting URL
https://www.edusum.com/isc2/ccsp-isc2-cloud-security-professional