

CCSP

Certified Cloud Security Professional

Training & Certification



Course Highlights



48-Hour LIVE Instructor-Led Training



Telegram Group for Exam Practice



Learn Better with **Flash Cards & Mind Maps**



Regular assessments and knowledge checks



98% Exam Pass Rate



Experienced Industry Experts



Real-world **Case Studies**



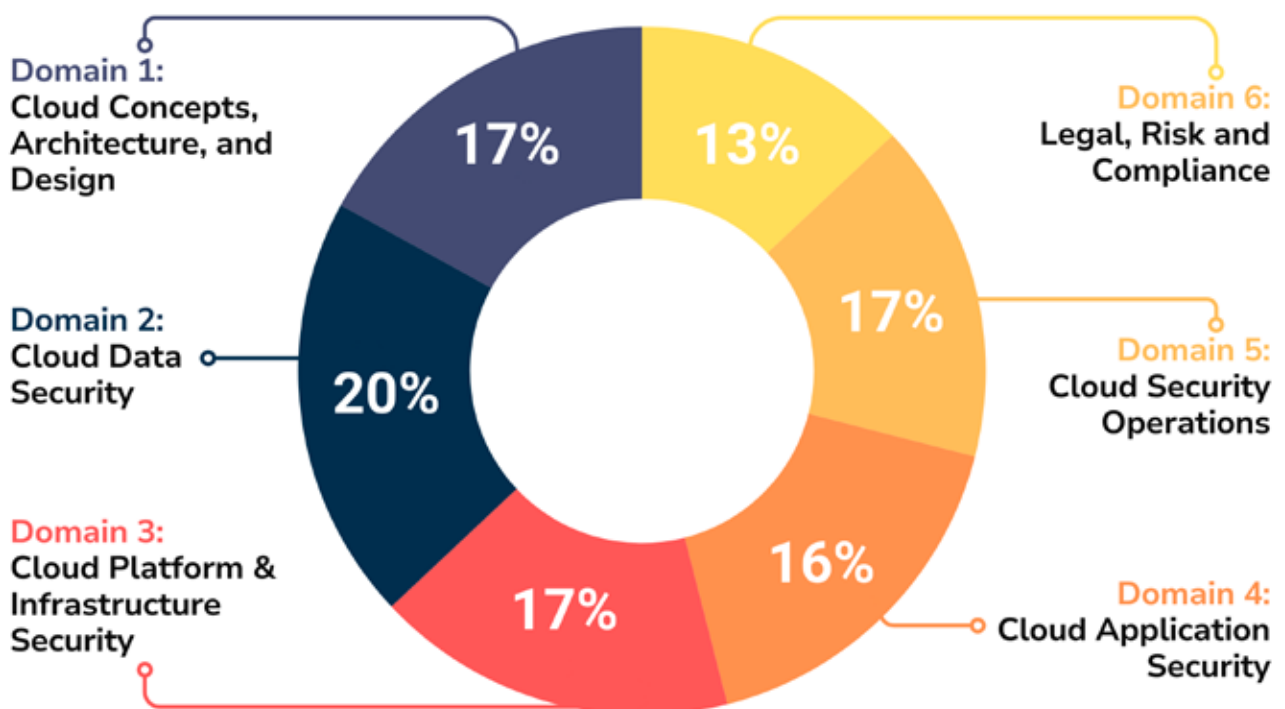
Post Training **Support** Till Exam



Access to Recorded Sessions

About Course

This certification-focused CCSP course is based on the new syllabus that is designed to empower learners with all the necessary skills and expertise to ace the CCSP certification. The key objective of the new version update of this certification training program is to arm learners with the right techniques and skills required to safeguard the critical data assets in a cloud environment. Built on the updated ISC2 CCSP syllabus, Version 4.0, this program equips professionals with the practical knowledge needed to design, secure, and manage cloud environments across today's enterprise landscape.



Course Objectives

- ✓ Design and implement security controls for cloud infrastructure, applications, and data across all major service models.
- ✓ Secure cloud-based applications across SaaS and PaaS environments using proven architectural and coding practices.
- ✓ Navigate the legal, privacy, and audit compliance requirements specific to cloud environments, including eDiscovery and forensic readiness.
- ✓ Build and manage cloud security operations covering monitoring, incident response, vulnerability assessment, and disaster recovery.
- ✓ Identify, assess, and treat risks associated with cloud vulnerabilities, threats, and multi-tenant infrastructure.
- ✓ Apply AI and ML security concepts, including threat detection, SOAR, data source validation, and regulatory requirements for cloud environments.
- ✓ Implement identity and access management solutions, including federated identity, SSO, MFA, CASB, and secrets and certificate management.
- ✓ Apply best practices for securing cloud services, data pipelines, and infrastructure at scale, including DevSecOps and supply chain risk management.



Target Audience

This CCSP training is suitable for experienced IT personnel who are involved with:

- ✓ Cloud Security Architect
- ✓ Cloud Engineer
- ✓ Cloud Consultant
- ✓ Cloud Administrator
- ✓ Cloud Security Analyst
- ✓ IT Auditor
- ✓ Professional Cloud Developer
- ✓ Information Security Professionals
- ✓ Risk and Compliance Professionals
- ✓ Security Engineers
- ✓ Governance and IT Audit Professionals

Pre-requisites

Candidates enrolling for this course must have five years of cumulative paid work experience in IT, with at least three years in information security and one year in one or more of the six CCSP CBK domains. This course is particularly suited for professionals working in cloud architecture, security engineering, IT auditing, governance, risk and compliance, and cloud operations. Professionals who do not yet meet the experience requirement can still take the exam and earn the Associate of ISC2 designation, then work toward full certification as they complete the required experience.

Note:

CCSP is a registered mark of The International Information Systems Security Certification Consortium, ISC2
InfosecTrain is not an authorized training partner of ISC2.

Exam Information

Certification Name	CCSP
Exam Duration	180 minutes
Number of Questions	100-150
Exam Format	Multiple Choice and Advanced Question Types
Passing Score	700 out of 1000 points
Exam Language	English, Chinese, Japanese and German
Accreditation	ANAB accredited to ISO/IEC 17024. Approved under DoD DoDM 8140.03



Course Content

Domain 1 **Cloud Concepts, Architecture, and Design (17%)**

1.1 Understand Cloud Computing Concepts

- ✓ Cloud Computing Definitions
- ✓ Cloud Computing Roles and Responsibilities
- ✓ Essential Cloud Computing Characteristics
- ✓ Building Block Technologies

1.2 Describe Cloud Reference Architecture

- ✓ Cloud Computing Activities
- ✓ Cloud Service Capabilities
- ✓ Cloud Service Categories
- ✓ Cloud Deployment Models
- ✓ Cloud Shared Considerations
- ✓ Impact of Related Technologies

1.3 Understand Security Concepts Relevant to Cloud Computing

- ✓ Cryptography and Key Management
- ✓ Identity and Access Control
- ✓ Data and Media Sanitization
- ✓ Network Security
- ✓ Virtualization Security
- ✓ Common Cloud Threats
- ✓ Security Hygiene

1.4 Understand Design Principles of Secure Cloud Computing

- ✓ Cloud Secure Data Lifecycle
- ✓ Cloud-based Business Continuity (BC) and Disaster Recovery (DR) Planning
- ✓ Business Impact Analysis (BIA)

- ✓ Functional Security Requirements
- ✓ Security Considerations and Responsibilities for Different Cloud Categories
- ✓ Cloud Design Patterns
- ✓ DevOps Security

1.5 Evaluate Cloud Service Providers (CSP)

- ✓ Verification Against Criteria
- ✓ System/Subsystem Product Certifications

1.6 Comprehend Artificial Intelligence (AI)/Machine Learning (ML)

- ✓ Cloud Threat Detection and Analysis
- ✓ Data Source Validation and Verification
- ✓ Security Orchestration, Automation and Response (SOAR)
- ✓ Ethical Concerns
- ✓ Regulatory Requirements



Domain 2 **Cloud Data Security (20%)**

2.1 Describe Cloud Data Concepts

- ✓ Cloud Data Lifecycle Phases
- ✓ Data Dispersion
- ✓ Data Flows

2.2 Design and Implement Cloud Data Storage Architectures

- ✓ Storage Types
- ✓ Threats to Storage Types

2.3 Design and Apply Data Security Technologies and Strategies

- ✓ Encryption and Key Management
- ✓ Hashing (e.g., data integrity, non-repudiation)
- ✓ Data Obfuscation (e.g., masking, anonymization)
- ✓ Tokenization
- ✓ Data Loss Prevention (DLP)
- ✓ Keys, Secrets and Certificates Management

2.4 Implement Data Discovery

- ✓ Structured Data
- ✓ Unstructured Data
- ✓ Semi-Structured Data
- ✓ Data Location

2.5 Plan and Implement Data Classification

- ✓ Data Classification Policies
- ✓ Data Mapping
- ✓ Data Labelling and Tagging

2.6 Design and Implement Information Rights Management (IRM)

- ✓ Objectives
- ✓ Appropriate Tools

2.7 Plan and Implement Data Retention, Deletion and Archiving Policies

- ✓ Data Retention Policies
- ✓ Data Deletion Procedures and Mechanisms
- ✓ Data Archiving Procedures and Mechanisms
- ✓ Legal Hold

2.8 Design and Implement Auditability, Traceability and Accountability of Data Events

- ✓ Definition of Event Sources and Requirement of Event Attributes
- ✓ Logging, Storage and Analysis of Data Events
- ✓ Chain of Custody and Non-repudiation

2.9 Comprehend Data Protection of AI and ML Data

- ✓ Data Set and Model Privacy
- ✓ Data Set and Model Security



Domain 3 **Cloud Platform and Infrastructure Security (17%)**

3.1 Comprehend Cloud Infrastructure Components

- ✓ Physical Environment
- ✓ Network and Communications
- ✓ Compute
- ✓ Virtualization
- ✓ Storage
- ✓ Management Plane

3.2 Design a Secure Data Center

- ✓ Logical Design
- ✓ Physical Design
- ✓ Environmental Design
- ✓ Design Resilience

3.3 Analyze Risks Associated with Cloud Infrastructure and Platforms

- ✓ Risk Assessment
- ✓ Cloud Vulnerabilities, Threats and Attacks
- ✓ Risk Treatment Strategies

3.4 Plan and Implementation of Security Controls

- ✓ Physical and Environmental Protection
- ✓ System, Storage and Communication Protection
- ✓ Identification, Authentication and Authorization in Cloud Environments
- ✓ Audit Mechanisms

3.5 Plan Business Continuity (BC) and Disaster Recovery (DR)

- ✓ Business Continuity (BC)/Disaster Recovery (DR) Strategy
- ✓ Business Requirements
- ✓ Creation, Implementation and Testing of Plan

Domain 4 **Cloud Application Security (16%)**

4.1 Advocate Training and Awareness for Application Security

- ✓ Cloud Development Basics
- ✓ Common Pitfalls
- ✓ Common Cloud Vulnerabilities

4.2 Describe the Secure Software Development Life Cycle (SDLC) Process

- ✓ Business Requirements
- ✓ Phases and Methodologies (e.g., design, code, test, maintain, waterfall vs. agile)

4.3 Apply the Secure Software Development Life Cycle (SDLC)

- ✓ Cloud-Specific Risks
- ✓ Threat Modelling
- ✓ Avoid Common Vulnerabilities During Development
- ✓ Secure Coding
- ✓ Software Configuration Management (CM) and Versioning

4.4 Apply Cloud Software Assurance and Validation

- ✓ Functional and Non-functional Testing
- ✓ Security Testing Methodologies
- ✓ Quality Assurance (QA)
- ✓ Abuse Case Testing

4.5 Use Verified Secure Software

- ✓ Securing Application Programming Interfaces (API)
- ✓ Supply-Chain Management
- ✓ Third-Party Software Management
- ✓ Validated Open-Source Software

4.6 Comprehend and Apply the Specifics of Cloud Application Architecture

- ✓ Supplemental Security Components
- ✓ Cryptography
- ✓ Sandboxing
- ✓ Application Virtualization and Orchestration

4.7 Design Appropriate Identity and Access Management (IAM) Solutions

- ✓ Federated Identity
- ✓ Identity Providers (IdP)
- ✓ Single Sign-On (SSO)
- ✓ Multi-Factor Authentication (MFA)
- ✓ Cloud Access Security Broker (CASB)
- ✓ Secrets, Key, and Certificate Management



Domain 5 **Cloud Security Operations (17%)**

5.1 Build and Implement Physical and Logical Infrastructure for Cloud Environment

- ✓ Hardware Specific Security Configuration Requirements
- ✓ Secure by Default
- ✓ Installation and Configuration of Management Plane Tools
- ✓ Virtual Hardware Specific Security Configuration Requirements
- ✓ Installation of Guest Operating System (OS) Virtualization Toolsets

5.2 Operate and Maintain Physical and Logical Infrastructure for Cloud Environment

- ✓ Access Controls for Local and Remote Access
- ✓ Secure Network Configuration
- ✓ Network Security Controls
- ✓ Operating Systems Hardening through Application of Baselines, Monitoring and Remediation
- ✓ Patch Management
- ✓ Availability of Clustered Hosts
- ✓ Availability of Guest Operating System (OS)
- ✓ Performance and Capacity Monitoring
- ✓ Hardware Monitoring
- ✓ Configuration of Host and Guest OS Backup and Restore Functions
- ✓ Management Plane

5.3 Implement Operational Controls and Standards

- ✓ Change Management
- ✓ Continuity Management
- ✓ Information Security Management
- ✓ Continual Service Improvement Management
- ✓ Incident Management

- ✓ Problem Management
- ✓ Release Management
- ✓ Deployment Management
- ✓ Configuration Management (CM)
- ✓ Service-Level Management
- ✓ Availability Management
- ✓ Capacity Management

5.4 Support Digital Forensics

- ✓ Forensic Data Collection Methodologies
- ✓ Evidence Management
- ✓ Collecting, Acquiring, and Preserving Digital Evidence

5.5 Manage Communication with Relevant Parties

- ✓ Vendors
- ✓ Customers
- ✓ Partners
- ✓ Regulators
- ✓ Other Stakeholders

5.6 Manage Security Operations

- ✓ Security Operations Center (SOC)
- ✓ Intelligent Monitoring of Security Controls
- ✓ Log Capture and Analysis
- ✓ Incident Response (IR)
- ✓ Vulnerability Assessments
- ✓ Penetration Testing

Domain 5 **Legal, Risk and Compliance (13%)**

6.1 Articulate Legal Requirements and Unique Risks within the Cloud Environment

- ✓ Conflicting International Legislation
- ✓ Evaluation of Legal Risks Specific to Cloud Computing
- ✓ Legal and Regulatory Frameworks and Guidelines
- ✓ eDiscovery
- ✓ Forensics Requirements

6.2 Understand Privacy Requirements

- ✓ Difference Between Contractual and Regulated Private Data
- ✓ Country-Specific Legislation Related to Private Data
- ✓ Jurisdictional Differences in Data Privacy
- ✓ Standard Privacy Requirements
- ✓ Privacy Impact Assessments (PIA)

6.3 Understand Audit Processes, 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
- ✓ Restrictions of Audit Scope Statements
- ✓ Gap Analysis
- ✓ Audit Planning
- ✓ Internal Information Security Management System (ISMS)
- ✓ Internal Information Security Controls System
- ✓ Policies

- ✓ Identification and Involvement of Relevant Stakeholders
- ✓ Specialized Compliance Requirements for Highly Regulated Industries
- ✓ Impact of Distributed Information Technology (IT) Model

6.4 Understand Implications of Cloud to Enterprise Risk Management

- ✓ Assess Providers Risk Management Programs
- ✓ Difference Between Data Roles
- ✓ Regulatory Transparency Requirements
- ✓ Risk Treatment
- ✓ Different Risk Frameworks
- ✓ Metrics for Risk Management
- ✓ Assessment of Risk Environment

6.5 Understand Outsourcing and Cloud Contract Design

- ✓ Business Requirements
- ✓ Vendor Management
- ✓ Contract Management
- ✓ Supply-Chain Management



Testimonials


Selvan Seluvappan, CCSP, CISM, PMP • 2nd
 Network Security Architect | Cybersecurity | Cloud Security | Project ...
 1mo • Edited •

+ Follow

I am excited to share that I have successfully earned the Certified Cloud Security Professional (CCSP) certification!

A special thanks to Mr. [Krish](#) for his exceptional training and guidance, and to Mr. [Prabh Nair](#) for his insightful YouTube content, both of which were invaluable in this journey.

This achievement inspires me to keep learning and growing in the field of cloud security. Here's to the next chapter! 🚀

#CCSP #CloudSecurity #ProfessionalGrowth


International Information System Security Certification Consortium
 The ISC2 Board of Directors hereby awards
SELVAN SELUVAPPAN
 the credential of
Certified Cloud Security Professional


Nikhil Patil • 2nd
 Senior technical specialist, CISSP, CCSP
 1w • Edited •

+ Follow

Excited to share that I have earned Certified Cloud Security Professional (CCSP) from ISC2 certification.

I wanted to express my deepest gratitude for my mentor [Krish](#) . for your training guidance and support to prepare for the exam.

I would also thankful for [Prabh Nair](#) (Coffee shots) and [Infosec Train](#) team support.

Thank you for believing in me and helping me grow in my career.


International Information System Security Certification Consortium
 The ISC2 Board of Directors hereby awards
Nikhil Patil
 the credential of
Certified Cloud Security Professional
 Having met all of the certification requirements, adoption of the ISC2 Code of Ethics, and successful performance on the required competency examination, subject to recertification every three years, this individual is entitled to all of the rights and privileges associated with this designation, as defined in the ISC2 Bylaws.


Vijayakumar T T • 2nd
 DGM IT | 17+ Years in IT Infrastructure & Cyber Security | CISSP | CG...
 3w •

+ Follow

Excited to announce that I've cleared the CCSP (Certified Cloud Security Professional) certification! 🎉

This journey has been both challenging and rewarding, and I couldn't have done it without the invaluable guidance and support from some amazing people.

A huge thank you to [Krish](#), [Prabh Nair](#) for his Coffee Shots, and [Infosec Train](#) for their incredible insights, resources, and mentorship throughout this process. Your support made all the difference in my preparation.

Looking forward to leveraging this knowledge to further enhance cloud security practices and contribute to the ever-evolving field of cybersecurity. 🚀🔒


International Information System Security Certification Consortium
 The ISC2 Board of Directors hereby awards
Vijayakumar T T
 the credential of
Certified Cloud Security Professional


Sarjerao Tupsamudre • 2nd
 Senior Cyber Security Architect @ UPL | CISSP CCSP
 3w • Edited •

+ Follow

Starting New Year with an important achievement of my Cyber Security Career by clearing the CCSP (Certified Cloud Security Professional) exam today.

Thanks to all those who have supported and guided me throughout the exam preparation...

Special thanks to [Avinash Selvamani](#) and [Krish](#) . for your valuable guidance and support

I will share tips/feedback on exam preparation based on my experience shortly..


 Candidate Name: Sarjerao M Tupsamudre
 ID/Examination number: 
 January 08, 2025


Hariharasudhan Gopalakrishnan, CISSP, CCSP • 2nd
 Lead Cloud Architect @ HCLTech | Enterprise Solution Design | Tech...
 3w • Edited •

+ Follow

View my verified achievement from [ISC2](#).

I'm thrilled to share that I have passed the CCSP (Certified Cloud Security Professional) certification! This would not have been possible without the incredible support of [Infosec Train](#) and my trainer [Krish](#) . for their engaging sessions that equipped me with the necessary tools for success.

I also want to acknowledge the community leaders [Prabh Nair](#) [Prashant Mahan](#), [CCSP-ISSAP](#) [CCSP Luke Ahmed](#) [Praveen Singh](#) who foster learning and growth. Your dedication inspires me to further my journey in cloud security.

#CCSP #CloudSecurity #ProfessionalDevelopment #ISC2


Certified Cloud Security Professional (CCSP) was issued by ISC2 to Hariharasudhan Gopalakrishnan.
 credly.com


Prakash Reddy • 3rd+
 Senior security Engineer | CISSP | CCSP
 4w •

+ Follow

I'm excited to share that I've passed the [CCSP](#) (Certified Cloud Security Professional) exam! This certification enhances my understanding of cloud security architecture and best practices.

Huge thanks to [#KKSingh](#) & [Infosec Train](#) for their training and guidance, which helped me pass this challenging exam.

Shoutout to [Prabh Nair](#) for his CCSP Coffee Shot videos on specific topics and valuable practice questions.

Dear Prakash Ranga Reddy:
 Congratulations! We are pleased to inform you that you have provisionally passed the Certified Cloud Security Professional (CCSP®) examination. Your examination result is provisional in that it may be subject to further psychometric and forensic evaluation before a certification decision is reached.



Contact us

www.infosectrain.com
sales@infosectrain.com

Follow us on

