

CCSP® – Certified Cloud Security Professional

Secure cloud environments from architecture to compliance — and prepare for the ISC2 CCSP exam with vendor-neutral, practical depth.

DURATION

5 days · 40 hours

LEVEL

Expert

CURRICULUM

15 modules · 5 labs

DELIVERYLive online, Onsite,
Corporate

Course overview

As more workloads move to the cloud, organisations need security professionals who understand how cloud changes architecture, data protection, operations and legal responsibilities. CCSP is ISC2's certification for that expertise. It is vendor-neutral, so it focuses on principles that apply to any provider, and this five-day course teaches those principles with examples from the major platforms.

Day one covers cloud concepts, architecture and design: reference architectures, service and deployment models, shared responsibility and secure design principles, plus how to evaluate cloud service providers. Day two focuses on cloud data security, including the data life cycle, storage architectures, encryption and key management, data discovery and classification, rights management and data events.

Day three addresses cloud platform and infrastructure security — physical and virtual components, risk analysis, security controls, and business continuity and disaster recovery in the cloud. Day four covers cloud application security, including the secure software development life cycle, testing, supply chain and identity solutions, followed by cloud security operations such as hardening, monitoring, incident management and digital forensics.

Day five covers legal, risk and compliance: jurisdiction, privacy, audit processes, risk management and outsourcing contracts, with particular attention to data protection obligations in India and the Gulf. The course closes with exam readiness. This course is aligned to the CCSP exam and prepares you for it; certification also requires experience and endorsement, so check the current requirements on the ISC2 website.

Highlights

- 40 hours of live, domain-by-domain preparation
- All six CCSP domains with cloud case studies
- Vendor-neutral, with AWS, Azure and Google Cloud examples
- Legal, risk and compliance in a cloud context
- Practice questions with detailed discussion

What's included

- Complete coverage of all six domains
- Vendor-neutral principles with multi-cloud examples
- Cloud data protection and key management deep dive
- Legal and compliance discussion for India and the Gulf
- Domain-end practice questions with discussion
- Study plan for the weeks after the course
- Course completion certificate from Ace Skills Consulting

Who this course is for

Who should attend

- Cloud security architects and engineers
- Security managers overseeing cloud adoption
- Enterprise architects and consultants
- CISSP holders specialising in cloud

Prerequisites

- Several years of IT experience including information security and cloud (ISC2 sets the exact requirement)
- Familiarity with at least one major cloud platform

Detailed curriculum — 5 days, 40 hours, 15 modules, 5 hands-on labs

Day 1 Cloud Concepts, Architecture & Design

8 hours

1.1 Cloud concepts

- Cloud computing roles and characteristics
- Shared responsibility
- Service and deployment models
- Related technologies such as containers and AI

1.2 Secure cloud architecture

- Reference architectures
- Cryptography and key management concepts
- Design principles for secure cloud
- Evaluating cloud service providers

LAB Evaluate a cloud provider against a security requirements checklist · 40 min

1.3 Cloud in practice

- Comparing AWS, Azure and Google Cloud security models
- Multi-cloud and hybrid considerations

Day 2 Cloud Data Security

8 hours

2.1 Data life cycle and storage

- Cloud data life cycle phases
- Data dispersion
- Storage architectures and threats

2.2 Protecting data

- Encryption and key management services
- Data loss prevention
- Hashing, masking and tokenisation
- Information rights management

LAB Design an encryption and key management approach for a SaaS application · 45 min

2.3 Classification and events

- Data discovery and classification
- Auditability and data events
- Retention, deletion and archiving

Day 3 Cloud Platform & Infrastructure Security

8 hours

3.1 Infrastructure components

- Physical environment and network
- Management plane security
- Compute, virtualisation and storage

3.2 Risks and controls

- Risk analysis for cloud infrastructure
- Identity and access for infrastructure
- Designing security controls

LAB Threat model a multi-tier cloud deployment · 40 min

3.3 Continuity and recovery

- Business continuity and disaster recovery strategies
- Testing recovery plans

Day 4 Cloud Application Security & Security Operations

8 hours

4.1 Cloud application security

- Secure software development life cycle
- Verified secure software and supply chain
- Application security testing
- Identity and access management solutions

4.2 Security operations

- Building and hardening infrastructure
- Security operations centre and monitoring
- Operational controls and standards
- Incident management

LAB Plan incident response for a cloud breach scenario · 45 min

4.3 Forensics and communication

- Digital forensics in the cloud
- Communication with stakeholders

Day 5 Legal, Risk & Compliance; Exam Readiness

8 hours

5.1 Legal and privacy

- Legal requirements and jurisdiction
- eDiscovery
- Privacy laws and cross-border data transfer

5.2 Audit, risk and outsourcing

- Audit processes in the cloud
- Contracts and service level agreements
- Enterprise risk management
- Vendor management

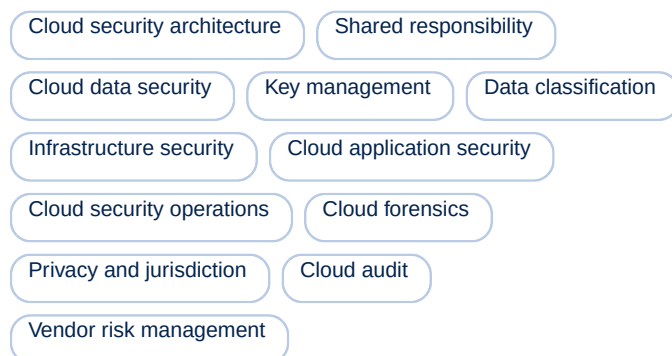
LAB Review a cloud contract for security and compliance gaps · 35 min

5.3 Exam readiness

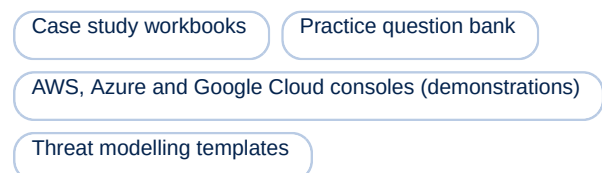
- Question technique
- Study plan
- Cross-domain practice set with review

Skills and tools

Skills you will build



Tools used in class



Certification exam

This course is aligned to the exam below and prepares you for it. The exam itself is booked and taken with the vendor.

Exam	CCSP – Certified Cloud Security Professional
Exam code	CCSP
Delivery	Test centre
Official page	https://www.isc2.org/certifications/ccsp

Exam skill areas covered

Cloud Architecture and Design

Cloud Platform and Infrastructure Security

Exam details are pending verification. Confirm the current exam code, format and fee on the official vendor page before booking.

Frequently asked questions

Is CCSP tied to a specific cloud provider?

No. CCSP is vendor-neutral. We use examples from AWS, Azure and Google Cloud to make the principles concrete.

Do I need CISSP first?

No, but ISC2 has historically allowed CISSP holders to use it towards the experience requirement. Check the current rules on the ISC2 website.

What is the exam format?

ISC2 publishes the current number of items, duration and passing standard on its website. Please confirm these before booking, as ISC2 updates exam formats from time to time.

How long should I study after the course?

Most learners revise for six to eight weeks, focusing on weaker domains and practice questions.

Can you run this for our cloud security team?

Yes. Private batches can use your cloud platforms and compliance obligations as case material.

Book a batch or talk to an advisor

Course page: aceskillsconsulting.com/course/ccsp-certified-cloud-security-professional · Email: info@aceskillsconsulting.com

Chennai office

Guindy, Chennai, Tamil Nadu

Delhi office

B-95, Old Post Office Street, Shakarpur

New Delhi 110092

Office: 98180 12523

CISSP and CCSP are registered marks of ISC2, Inc. All product names, logos, brands, trademarks and registered trademarks are the property of their respective owners. Ace Skills Consulting is an independent training provider; unless explicitly stated, it is not affiliated with, endorsed by or sponsored by any vendor mentioned on this site. Exam details are provided for guidance and may change — always confirm on the vendor's official website. Curriculum generated on 23 Oct 2026; topics and order may be adjusted by the trainer to suit each batch.