



ISC2

CCSP — Certified Cloud Security Professional Preparation Training

Delivered from Hacky Security's own curriculum, by instructors who also work our security operations centre. Classroom, online live, or at your office.

PROFESSIONAL

40 HOURS

5 DAYS

At a glance

COURSE	CCSP — Certified Cloud Security Professional
TRACK	ISC2
DOMAIN	Cyber Security
LEVEL	Professional
DURATION	40 hours (about 5 days)
DELIVERY	Classroom · Online live · On-site at your office
LANGUAGE	English
CLASS SIZE	Small cohorts — everyone gets lab time

WHAT IS INCLUDED

- ✓ Instructor-led delivery by practitioners who also work our SOC
- ✓ Hands-on lab access for the duration of the course
- ✓ Course materials and lab guides
- ✓ Hacky Security certificate of completion
- ✓ Post-course support by email

Who this is for

This is a professional course. It suits people already working in or moving into Cyber Security who want structured, hands-on preparation rather than a video library. If you are unsure whether the level fits your team, send us the job titles and we will tell you honestly — including if a different course would serve you better.

Course outline

About this course map

Six domains, mapped one-for-one to the ISC2 CCSP exam outline and taught in the same order, so nothing on the exam is left uncovered.

The outline that defines the current CCSP took effect on 1 August 2026. The six domain names are unchanged, but the content inside them is not: artificial intelligence and machine learning now appear as named topics in their own right, in the architecture domain and again in the data security domain. If you studied CCSP material written before that date, those sections are missing from it.

ISC2 does not publish a percentage weighting per domain for this outline, so the framing line for each domain below says what it is for rather than what share of the paper it takes. Classroom time follows the depth of the content, and the data security and operations domains take the most of it.

Domain 01 – Cloud Concepts, Architecture and Design

The vocabulary and the reference architecture that the other five domains assume you already have.

- Cloud computing definitions, roles, characteristics and the building-block technologies underneath
- The cloud reference architecture: service categories, deployment models and the activities in each
- Shared responsibility, and reading a provider's version of it against your own obligations
- Security concepts that carry over into cloud — cryptography, access control, virtualisation, hardening, monitoring
- Secure cloud design principles, threat modelling, and weighing a control against what it costs
- Business continuity and disaster recovery designed in rather than retrofitted
- Evaluating cloud service providers against certifications, standards and published criteria
- Artificial intelligence and machine learning services: how they are built, hosted and exposed

Domain 02 – Cloud Data Security

The domain that carries the most exam-relevant detail, because data is the thing the cloud actually holds.

- The cloud data lifecycle, and establishing where data genuinely lives at each phase
- Storage architectures for each service model, and the threats particular to each type
- Encryption and key management, hashing, masking, tokenisation and data de-identification
- Data discovery across structured, unstructured and semi-structured stores
- Data classification, data mapping and labelling
- Information rights management: objectives, tooling and its practical limits
- Retention, deletion and archiving policy, including legal hold and verifiable disposal
- Auditability, traceability and accountability: event sources, log capture, chain of custody, SIEM
- Protecting the data used to train, tune and run artificial intelligence and machine learning systems

Domain 03 – Cloud Platform and Infrastructure Security

Everything beneath the application, including the parts you cannot see and do not control.

- Physical, network, compute, virtualisation, storage and management plane components
- Secure data centre design across logical, physical and environmental considerations
- Risk assessment for cloud infrastructure and platforms, and the cloud-specific vulnerability landscape

- Counter-measure strategies: cloud-specific, virtualisation-specific, and the ones that transfer unchanged
- Planning security controls — physical and environmental protection, system and communication protection, identity and access management, audit mechanisms
- Business continuity and disaster recovery: strategy, planning, and testing it against a real provider outage
- Risk mitigation through shared responsibility, contractual terms and provider selection

Domain 04 — Cloud Application Security

Application security where the platform, the pipeline and the identity layer are all someone else's product.

- Training and awareness for developers building on cloud platforms
- Common cloud application pitfalls and the vulnerabilities that recur across providers
- The secure software development lifecycle, its phases and its business requirements
- Applying it in practice: threat modelling, secure coding, secure configuration, avoiding known weaknesses
- Cloud software assurance and validation — functional testing, static and dynamic analysis, interactive testing, vulnerability scanning, penetration testing
- Using verified secure software: supply chain management, third-party assurance and open source risk
- Cloud application architecture: cryptography, sandboxing, application virtualisation, API gateways, web application firewalls, database activity monitoring
- Identity and access management for applications: federated identity, identity providers, single sign-on, multifactor authentication, secrets management

Domain 05 — Cloud Security Operations

Running the thing once it is live, against a service management discipline rather than ad hoc practice.

- Building physical and logical infrastructure: hardware specification, installation, configuration, secure network design
- Operating and maintaining it: access control, patching, performance and capacity monitoring, hardening, backup and restore
- Implementing operational controls and standards against ITIL and ISO/IEC 20000-1
- Change, configuration, release and deployment management in an environment that changes continuously
- Incident, problem, availability, capacity, continuity and service level management
- Supporting digital forensics: evidence collection, acquisition and preservation when the host is not yours
- Managing communication with providers, customers, partners, regulators and internal stakeholders
- Running security operations: monitoring, log management, incident response and vulnerability assessment

Domain 06 — Legal, Risk and Compliance

The domain that decides whether a technically sound cloud design is a usable one.

- Conflicting international legislation, cyber laws and the legal risks unique to cloud
- eDiscovery and forensic requirements, and evidence handling across jurisdictions
- Privacy: personally identifiable information, contractual against regulated data, and country-specific regimes
- Standard privacy requirements and the frameworks used to demonstrate them
- Audit in a cloud context: internal and external controls, scope restrictions, gap analysis, assurance reports, audit planning
- Enterprise risk management: assessing provider risk, risk appetite, treatment options and risk frameworks
- Outsourcing and cloud contract design: service level agreements, vendor management, supply chain risk

Who should take this

Cloud and security architects, security engineers working in AWS, Azure or Google Cloud, GRC and audit staff who have to assess cloud estates, and CISSP holders who need the cloud depth their existing certification only gestures at.

ISC2 requires five years of cumulative full-time IT experience, of which three years must be in cybersecurity and one year in one or more of the six CCSP domains. A relevant post-secondary degree or the Cloud Security Alliance CCSK certificate can waive one year, but only one year can be waived in total. An active CISSP satisfies the whole experience requirement. Candidates without it can sit the exam and become an Associate of ISC2 while they accrue the experience.

You will need working knowledge of at least one major cloud platform and of general security practice. You do not need to be a cloud engineer.

The exam

The CCSP is set and awarded by ISC2. It moved from a fixed linear paper to Computerized Adaptive Testing on 1 October 2025, so the questions you see depend on how you answered the ones before.

- 100 to 150 items, three hours
- Adaptive format, with multiple choice and advanced item types
- A scaled score of 700 out of 1000 is required to pass
- Available in English, Japanese, Chinese, Korean, German and Spanish

The exam voucher is purchased separately from ISC2. We arrange it on your behalf and send you the code, and you book your own exam date. Certification also requires endorsement by an existing ISC2 member once you pass.

How we deliver it

Five days, classroom or online live, or at your office for a private group. Roughly a third of the time is spent in live cloud tenancies we own, working through the control decisions each domain describes — key management, logging pipelines, identity federation, provider assurance review — so the domains connect to something you can see.

Mapped to the ISC2 CCSP exam outline effective 1 August 2026, including the artificial intelligence and machine learning content new to that outline. Taught from Hacky Security's own curriculum and cloud estate by instructors who build and run cloud environments for clients.

Sitting the official exam

Exam voucher sold separately. We buy it from the certification body on your behalf and send you the code — you book your own exam date. This course is Hacky Security's own preparation training. The certification itself is awarded by the certification body, not by us.

Investment

Priced per cohort. Tell us how many people and which delivery mode and we will send a quote the same working day.

Book this course

Tell us how many people, where, and when — we will come back with dates and a quote within one working day.

+91-8091900310 • info@hackysecurity.com

<https://hackysecurity.com/courses/ccsp/>

CHANDIGARH • SHIMLA • DELHI • DUBAI • LONDON

Independent preparation training delivered from Hacky Security's own curriculum. Hacky Security Private Limited is not affiliated with or endorsed by the certification body named in this document. Certification names and codes are the trademarks of their respective owners and are used only to describe what this course prepares you for. Prices, durations and outlines are indicative and may change; the quotation we send you is the binding one. Issued 11 September 2026.