Complete Cloud Security Professional Training Course

15 – 19 November 2026
Phuket

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

Complete Cloud Security Professional Training Course

Ref: 36346_110440 **Date:** 15 – 19 November 2026 **Location:** Phuket **Fees:** 6000 Euro

Overview

The CCSP Certified Cloud Security Professional credential from ISC2 is vendor-neutral: it tests how a seasoned practitioner reasons about any provider's offering rather than how to click through one console. This five-day course prepares candidates for that mindset. It walks through the six domains of the CCSP Common Body of Knowledge in order, and teaches each through choices a cloud security manager actually signs: whether a workload is portable enough to leave a provider, which obfuscation method suits a dataset, what a provider's SOC 2 Type II exceptions really mean, which clauses to insist on before signing, and how to answer a litigation hold. Every domain closes with exam-style questions and a debrief on why the distractors are wrong. This programme is delivered by Agile Leaders Training Center.

Who Should Attend

- Practitioners with several years in IT and information security planning to sit the CCSP exam
- CISSP holders adding a cloud-specific credential
- Enterprise architects who approve designs spanning more than one provider
- Third-party and supplier assurance managers vetting cloud vendors
- Auditors, privacy officers and legal counsel reviewing cloud agreements

Departments and Industries

Suited to teams that must judge providers they do not run themselves.

- Supplier assurance teams in banking and insurance
- Architecture review boards in SaaS businesses
- Records management and privacy offices in hospitals
- Legal and purchasing teams drafting hosting agreements
- Government shared-services and digital units

Learning Objectives

By the end of the course, participants will be able to:

- Use the NIST SP 800-145 and ISO/IEC 17788 definitions to describe any offering and the roles of customer, provider, partner and broker.
- Judge interoperability, portability and reversibility before a workload is moved.
- Choose between tokenisation, masking, anonymisation and crypto-shredding for a given dataset.
- Recognise risks specific to Type 1 and Type 2 hypervisors, sandboxing and application virtualisation.
- Place STRIDE, SAST, DAST and OWASP ASVS checks into a cloud software lifecycle.
- Read SOC 1, SOC 2 and CSA STAR evidence and negotiate right-to-audit, breach-notice and exit terms.

AGILE LEADERS
Training Center

Course Agenda

Day 1: Domain 1 - Concepts, Reference Architecture and Design

- CCSP exam structure, ISC2 experience rules and a study plan
- NIST SP 800-145 and ISO/IEC 17788 vocabulary
- Roles: customer, provider, partner, broker, auditor and regulator
- Cross-cutting aspects: interoperability, portability, reversibility and availability
- Business impact analysis and the cost case for migration
- Evaluating a provider through Common Criteria and FIPS 140 validations

Day 2: Domain 2 - Protecting Data Held by a Provider

- Create, store, use, share, archive, destroy: the CCSP secure data lifecycle
- Raw, volume, object, structured and unstructured storage per service model
- Tokenisation, masking, anonymisation and key escrow compared
- Information rights management and data discovery
- Retention schedules, litigation hold and crypto-shredding
- Exam-style question set with debrief

Day 3: Domains 3 and 4 - Provider Platforms and Cloud Applications

- Type 1 versus Type 2 hypervisors, guest escape and tenant separation
- Provider data centre siting, power, cooling and redundancy tiers
- Recovery time and recovery point objectives across regions
- The cloud software lifecycle and the OWASP Top 10 in a cloud context
- STRIDE threat modelling, SAST, DAST and OWASP ASVS
- Sandboxing, application virtualisation and API gateways

Day 4: Domain 5 - Running Security Day to Day

- Building and securing the logical environment inside a tenant
- ITIL change, configuration, capacity and problem management
- Security operations visibility when telemetry belongs to the provider
- Evidence collection and chain of custody under ISO/IEC 27037
- Communicating with vendors, customers and regulators during an event
- Exam-style question set with debrief

Day 5: Domain 6 - Legal, Risk and Compliance, and Mock Exam

- Conflicting jurisdictions, data sovereignty and eDiscovery under ISO/IEC 27050
- Privacy principles and ISO/IEC 27018 for processors of personal data
- SOC 1, SOC 2 Type I and Type II, and the CSA STAR registry
- Hosting agreement clauses: right to audit, breach notice, exit and data return
- Enterprise risk appetite and residual risk when outsourcing to a provider
- Full-length timed mock exam and domain-by-domain score review

Practical Exercises

- Case: decide whether an HR system can leave its current provider, scoring portability and reversibility.
- Case: pick an obfuscation method for each column of a patient table.
- Case: read a SOC 2 Type II extract and list the exceptions that matter to your organisation.
- Case: redline a hosting agreement for audit rights, breach notice and exit.

FAQs

What background is recommended?

Several years in IT including time in information security. ISC2 sets its own experience rules for the credential; candidates should confirm them before booking the exam.

Is the course tied to one provider?

No. Like the CCSP exam it is vendor-neutral; provider names appear only as examples.

How does this differ from a hands-on engineering course?

It trains judgement across providers: contracts, assurance evidence, data decisions and risk, rather than configuring a single platform.

Conclusion

Participants finish having covered all six CCSP domains, a timed mock exam and several contract and assurance cases, with a personal list of weak areas to revise before the ISC2 exam.