

Course : Certified Cloud Security Professional (CCSP), ISC2 certification

Official training aligned with ISC2

Practical course - 5d - 35h00 - Ref. CCN

Price : 4040 € E.T.

Nouvelle édition

La certification CCSP (Certified Cloud Security Professional), délivrée par ISC2, est une certification de référence, vendor-neutral, dédiée à la sécurité du cloud computing. Cette formation vous permettra d'acquérir une vision stratégique et opérationnelle de la sécurité cloud afin de réussir l'examen officiel CCSP, en couvrant l'ensemble des 6 domaines du CCSP Common Body of Knowledge (CBK).

Teaching objectives

At the end of the training, the participant will be able to:

- ✓ Master cloud concepts, service models and reference architectures
- ✓ Design a secure, coherent and governed cloud architecture
- ✓ Define and manage a lifecycle data protection strategy for the cloud
- ✓ Securing cloud platforms, infrastructures and services
- ✓ Integrating security requirements into cloud applications and CI/CD chains
- ✓ Organize and manage cloud security operations, including supervision, incident management and continuity.
- ✓ Apply legal, risk management and compliance requirements specific to cloud environments
- ✓ Adopt the "cloud security leader" thinking expected by ISC2 to pass the CCSP exam
- ✓ Prepare effectively for the official CCSP exam (ISC2 format and expectations)

Intended audience

IT architects and engineers, information systems and security managers, DevOps/SecOps profiles, security consultants and IT risk, compliance and contract professionals.

PARTICIPANTS

IT architects and engineers, information systems and security managers, DevOps/SecOps profiles, security consultants and IT risk, compliance and contract professionals.

PREREQUISITES

CCSP certification requires 5 years' IT experience, including 3 years in cybersecurity and 1 year in cloud security. Exemptions are possible (diploma, CCSK). CISSP validates the whole.

TRAINER QUALIFICATIONS

The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

ASSESSMENT TERMS

The trainer evaluates each participant's academic progress throughout the training using multiple choice, scenarios, hands-on work and more.

Participants also complete a placement test before and after the course to measure the skills they've developed.

Prerequisites

CCSP certification requires 5 years' IT experience, including 3 years in cybersecurity and 1 year in cloud security. Exemptions are possible (diploma, CCSK). CISSP validates the whole.

Certification

The official exam takes place in English, in the form of a 3-hour MCQ comprising 100 to 150 questions, with a minimum score of 700/1000.

Course schedule

1 Area 1 - Cloud concepts, architecture and design

- Fundamental concepts of cloud computing.
- Cloud service models (IaaS, PaaS, SaaS) and deployment models.
- Principles of cloud architecture and secure design.
- Shared responsibility model.
- Governance and consistency of controls in a multicloud environment.
- Cloud services orchestration and component integration.

2 Area 2 - Cloud data security

- Data governance and responsibilities in the cloud.
- Classification and data protection requirements.
- Cloud data lifecycle management.
- Data protection controls (policies, procedures, mechanisms).
- Manage data localization, retention and deletion.

3 Area 3 - Cloud platform and infrastructure security

- Architecture and security of cloud infrastructures.
- Security for cloud platforms and services.
- Segmentation, isolation and cloud interconnections.
- Configuration and vulnerability management.
- Security controls for infrastructure services.

4 Area 4 - Cloud application security

- Application security requirements in cloud environments.
- Integrating security into the development and deployment cycle.
- API and application services security.
- Application risk management specific to the cloud.
- Secure-by-design approach and alignment with security policies.

5 Area 5 - Cloud security operations

- Organization and governance of cloud security operations.
- Supervision, logging and cloud-native monitoring.
- Management of cloud security events and incidents.
- Operational access and identity management.
- Business continuity, resilience and recovery in cloud environments.

TEACHING AIDS AND TECHNICAL RESOURCES

- The main teaching aids and instructional methods used in the training are audiovisual aids, documentation and course material, hands-on application exercises and corrected exercises for practical training courses, case studies and coverage of real cases for training seminars.
- At the end of each course or seminar, ORSYS provides participants with a course evaluation questionnaire that is analysed by our instructional teams.
- A check-in sheet for each half-day of attendance is provided at the end of the training, along with a course completion certificate if the trainee attended the entire session.

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you need special accessibility accommodations? Contact Mrs. Fosse, Disability Manager, at psh-accueil@orsys.fr to review your request and its feasibility.

6 Area 6 - Legal, Risk and Compliance

- Legal and regulatory frameworks applicable to cloud services.
- Contractual requirements and customer/supplier responsibilities.
- Cloud risk management.
- Compliance, audit and proof production.
- Application of policies and procedures to meet regulatory obligations.

7 Preparing for the CCSP exam

- Presentation of the CCSP exam.
- Methodology for answering ISC2 questions.
- Time management and common pitfalls.
- Assessment quizzes and exam-style questions.
- Advice from CCSP-certified experts.

Times

Courses take place from 09:00 to 12:30 and from 14:00 to 17:30.

Participants may arrive beginning at 08:45. Breaks and lunches are complimentary.

For four- and five-day hands-on courses, sessions end at 16:00 on the last day of the course, regardless of the teaching mode..

Dates and locations

REMOTE CLASS

2026 : 8 June, 21 Sep., 30 Nov.

PARIS LA DÉFENSE

2026 : 20 Apr., 1 June, 14 Sep., 23 Nov.