CSSP - Certified Cloud Security Professional

Certified Cloud Security Professional (CCSP®) training provides a comprehensive review of the knowledge required for understanding cloud computing and its information security risks and mitigation strategies. This training course will help students review and refresh their knowledge and identify areas they need to study for the CCSP exam. Content aligns with and comprehensively covers the six domains of the (ISC)² CCSP Common Body of Knowledge (CBK®), ensuring relevancy across all disciplines in the field of cloud security.

As an (ISC)2 Official Training Provider, we use courseware developed by (ISC)² – creator of the CCSP CBK – to ensure your training is relevant and up-to-date. Our instructors are verified security experts who hold the CCSP and have completed intensive training to teach (ISC)² content.

Training features:

- Instruction from an (ISC)2 Authorized Instructor
- Official (ISC)2 Student Training Guide
- Chapter quizzes
- Interactive flash cards to reinforce learning
- Real-world learning activities and scenarios
- Post-course assessment questions to gauge exam readiness

Who Should Attend

This training is intended for professionals who have at least five years of full-time IT experience, including three years in information security and at least one year in cloud security, and are pursuing CCSP certification to enhance credibility and career mobility. The seminar is ideal for those working in positions such as, but not limited to:

- Security Manager
- Systems Architect
- Systems Engineer
- Security Architect
- Security Consultant
- Security Engineer
- Enterprise Architect
- Security Administrator

Course Agenda

- Domain 1. Cloud Concepts, Architecture and Design
- Domain 2. Cloud Data Security
- Domain 3. Cloud Platform & Infrastructure Security
- Domain 4. Cloud Application Security
- Domain 5. Cloud Security Operations
- Domain 6. Legal, Risk and Compliance

Course Objectives

After completing this course, the student will be able to:

- Understand legal frameworks and guidelines that affect cloud services.
- Recognize the fundamentals of data privacy regulatory/legislative mandates.
- Assess risks, vulnerability, threats, and attacks in the cloud environment.
- Evaluate the design and plan for cloud infrastructure security controls.
- Evaluate what is necessary to manage security operations.
- Understand what operational controlsand standards to implement.
- Describe the types of cloud deployment models in the types of “as a service” cloud models currently available today.
- Identify key terminology, and associated definitions related to cloud technology.
- Establish a common terminology for use with in your team or workgroup.
- Build a business case for cloud adoption and determine business units that benefit rom cloud migration strategies.