Certified Cloud Security Professional (CCSP) Training and Certification

Course: **00046**
Filter: **Beginner**
Duration: **5 days**
Category:: **Cloud Security**
Price: **2500,00 €**

About Course

The (ISC)² Certified Cloud Security Professional CCSP Training Course is designed for security professionals seeking to enhance their knowledge of cloud security. The program covers various aspects of data security, cloud infrastructure security, and information security. Through this training, participants will learn how to secure data centers, cloud environments, and cloud-based data access. The focus will be on cloud security solutions and techniques for detecting and responding to security incidents. The training covers cloud computing technologies, including Microsoft Azure, as well as security practices related to physical infrastructure, cloud resource access control, and protection of sensitive data. Load balancers, security operations centers (SOCs), and cloud environment security will also be covered. Upon completion of the training, participants can attempt the CCSP exam, and earn the CCSP certification after passing the exam, which is a recognized industry standard for cloud security expertise. Passing the CCSP Certification Exam meets U.S. DoD Directive 8140/8570.01 Technical (IAT) Level-III, and Information Assurance Security Architect/Engineer (IASAE) Level-III.

What you'll learn

- Define Cloud Concepts, Architecture, and Design
- Implement Cloud Data Security
- Understand Cloud Platform and Infrastructure Security
- Secure Cloud Applications
- Operationalize Cloud Security
- Continue learning and face new challenges with after-course one-on-one instructor coaching

Targeted audience

- It is essential to train developers, project managers, heads of Information Systems departments (RSI/DSI), managers of Information Systems Security (RSSI) and more generally business decision-makers on this subject.

Pre-requisites

- Five years of cumulative, full-time working experience in IT (Information Technology) (three must be in information security, and one must be in one of the six CCSP CBK domains).
- Those without the required experience can take the exam to become an Associate of (ISC)²; while working toward the experience needed for full certification.

Curriculum

Module 1: Cloud Concepts, Architecture and Design

- Understand cloud computing concepts
- Describe cloud reference architecture
- Understand security concepts relevant to cloud computing
- Understand design principles of secure cloud computing
- Evaluate cloud service providers

Module 2: Cloud Data Security

- Describe cloud data concepts
- Design and implement cloud data storage architectures
- Design and apply data security technologies and strategies
- Plan and implement data classification
- Design and implement Information Rights Management (IRM)
- Plan and implement data retention, deletion, and archiving policies

- Design and implement auditability, traceability, and accountability of data events

Module 3: Cloud Platform and Infrastructure Security

- Comprehend cloud infrastructure and platform components
- Design a secure data center
- Analyze risks associated with cloud infrastructure and platforms
- Plan and implementation of security controls
- Plan business continuity (BC) and disaster recovery (DR)

Module 4: Cloud Application Security

- Advocate training and awareness for application security
- Describe the Secure Software Development Life Cycle (SDLC) process
- Apply the Secure Software Development Life Cycle (SDLC)
- Apply cloud software assurance and validation
- Use verified secure software
- Comprehend the specifics of cloud application architecture
- Design an appropriate identity and access management (IAM) solution

Module 5: Cloud Security Operations

- Build and implement physical and logical infrastructure for the cloud environment
- Operate and maintain physical and logical infrastructure for cloud environment
- Implement operational controls and standards
- Support digital forensics
- Manage communication with relevant parties
- Manage security operations

Module 6: Legal, Risk, and Compliance

- Articulate legal requirements and unique risks within the cloud environment
- Understand privacy issues
- Understand audit process, methodologies, and required adaptations for a cloud environment
- Understand implications of cloud to enterprise risk management
- Understand outsourcing and cloud contract design