Certified Cloud Security Professional (CCSP)

Course Duration: 10 Days

Course overview

(ISC)² and the Cloud Security Alliance (CSA) developed the Certified Cloud Security Professional (CCSP) credential to ensure that cloud security professionals have the required knowledge, skills, and abilities in cloud security design, implementation, architecture, operations, controls, and compliance with regulatory frameworks. A CCSP applies information security expertise to a cloud computing environment and demonstrates competence in cloud security architecture, design, operations, and service orchestration. This professional competence is measured against a globally recognized body of knowledge. The CCSP is a stand-alone credential that complements and builds upon existing credentials and educational programs, including (ISC)²'s Certified Information Systems Security Professional (CISSP) and CSA's Certificate of Cloud Security Knowledge (CCSK).

The topics included in the CCSP Common Body of Knowledge (CBK) ensure its relevancy across all disciplines in the field of cloud security. Successful candidates are competent in the following 6 domains:

- Cloud Concepts, Architecture and Design
- Cloud Data Security
- Cloud Platform & Infrastructure Security
- Cloud Application Security
- Cloud Security Operations
- Legal, Risk and Compliance

Who Should Attend?

The training seminar is ideal for those working in positions such as but not limited to:

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

Course Outline:

1) Cloud Concepts, Architecture and Design

- 1.1 Understand Cloud Computing Concepts
- 1.2 Describe Cloud Reference Architecture
- 1.3 Understand Security Concepts Relevant to Cloud Computing
- 1.4 Understand Design Principles of Secure Cloud Computing
- 1.5 Evaluate Cloud Service Providers

2) Cloud Computing Activities

- 2.1 Describe Cloud Data Concepts
- 2.2 Design and Implement Cloud Data Storage Architectures
- 2.3 Design and Apply Data Security Technologies and Strategies
- 2.4 Implement Data Discovery
- 2.5 Implement Data Classification
- 2.6 Design and Implement Information Rights Management (IRM)
- 2.7 Plan and Implement Data Retention, Deletion and Archiving Policies
- 2.8 Design and Implement Auditability, Traceability and Accountability of Data Events

3) Cloud Platform and Infrastructure Security

- 3.1 Comprehend Cloud Infrastructure Components
- 3.2 Design a Secure Data Center
- 3.3 Analyze Risks Associated with Cloud Infrastructure
- 3.4 Design and Plan Security Controls
- 3.5 Plan Disaster Recovery (DR) and Business Continuity (BC)Domain

4) Cloud Application Security

- 4.1 Advocate Training and Awareness for Application Security
- 4.2 Describe the Secure Software Development Life Cycle (SDLC) Process
- 4.3 Apply the Secure Software Development Life Cycle (SDLC)
- 4.4 Apply Cloud Software Assurance and Validation
- 4.5 Use Verified Secure Software
- 4.6 Comprehend the Specifics of Cloud Application Architecture
- 4.7 Design Appropriate Identity and Access Management (IAM) Solutions

5) Cloud Security Operations

5.1 Implement and Build Physical and Logical Infrastructure for Cloud Environment
5.2 Operate Physical and Logical Infrastructure for Cloud Environment
5.3 Manage Physical and Logical Infrastructure for Cloud Environment
5.4 Implement Operational Controls and Standards (e.g., Information Technology Infrastructure Library (ITIL), International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 20000-1)
5.6 Manage Communication with Relevant Parties
5.7 Manage Security Operations

6) Legal, Risk and Compliance

6.1 Articulate Legal Requirements and Unique Risks within the Cloud Environment
6.2 Understand Privacy Issues
6.3 Understand Audit Process, Methodologies, and Required Adaptations for a Cloud Environment
6.4 Understand Implications of Cloud to Enterprise Risk Management
6.5 Understand Outsourcing and Cloud Contract Design