Certified Cloud Security Professional (CCSP)

Course ID #: 7000-798-ZZ-Z
Hours: 35

Course Content

Course Description:

This (ISC)²® Certified Cloud Security Professional (CCSP)certification training course provides a thorough understanding of the information security risks and mitigation strategies critical to data security in the cloud. This CCSP training course covers the six domains of the Official (ISC)²; CCSP Common Body of Knowledge (CBK®), and prepares you to pass the CCSP exam and become a Certified Cloud Security Professional.

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.

Course Objectives:

Upon successful completion of this course, students will be able to:

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

Prerequisites:

Five years of cumulative, full-time working experience in IT (three must be in information security, and one must be in one of the six CCSP CBK domains).

Certified Cloud Security Professional (CCSP)

Course ID #: 7000-798-ZZ-Z
Hours: 35

Topics:

Lesson 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

Lesson 2: Cloud Data Security

- Describe cloud data concepts
- Design and implement cloud data storage architectures
- Design and apply data security technologies and strategies
- Implement data discovery
- 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

Lesson 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)

Lesson 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

Lesson 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

Lesson 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