(ISC)2 CERTIFIED CLOUD SECURITY PROFESSIONAL (CCSP)

Who Should Attend

This course is intended for IT professionals that have a minimum of five years' paid work experience in the industry with three of those years being in information security and at least one year in one of the six CCSP domains.

The CCSP certification is awarded to students who can show that they have attained the advanced knowledge and technical skills required to design, manage and secure data, applications and infrastructure in the cloud and employing the accepted best practices, policies and procedures.

Course Objectives

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

- Prepare for and pass the CCSP Exam.
- Identify and explain the five characteristics required to satisfy the NIST definition of cloud computing.
- Differentiate between various as-a-service delivery models and frameworks that are incorporated into the cloud computing reference architecture.
- Explain strategies for protecting data at rest and in motion.
- Discuss strategies for safeguarding data, classifying data, ensuring privacy, assuring compliance with regulatory agencies, and working with authorities during legal investigations.
- Contrast between forensic analyst in corporation data center and cloud computing environments.

Course Outline

1 – ARCHITECTURAL CONCEPTS AND DESIGN REQUIREMENTS

- Reviewing Cloud Computing Concepts
- Describing Cloud Reference Architecture
- Security Concepts Relevant to Cloud Computing
- Design Principles of Secure Cloud Computing
- Identifying Trusted Cloud Services

2 – CLOUD DATA SECURITY

- Understanding Cloud Data Lifecycle

- Designing and Implementing Cloud Data Storage Architectures
- Designing and Applying Data Security Strategies
- Understanding and Implementing Data Discovery and Classification Technologies
- Designing and Implementing Relevant Jurisdictional Data Protections for Personally Identifiable Information

3 – CLOUD PLATFORM AND INFRASTRUCTURE SECURITY

- Comprehending Cloud Infrastructure Components
- Analyzing Risks Associated to Cloud Infrastructure
- Designing and Planning Security Controls
- Planning Disaster Recovery and Business Continuity Management

4 – CLOUD APPLICATION SECURITY

- Recognizing the Need for Training and Awareness in Application Security
- Understanding Cloud Software Assurance and Validation
- Using Verified Secure Software
- Comprehending the Software Development Life-Cycle (SDLC) Process
- Applying the Secure Software Development Life-Cycle

5 -OPERATIONS

- Supporting the Planning Process for the Data Center Design
- Implementing and Building Physical Infrastructure for Cloud Environment
- Running Physical Infrastructure for Cloud Environment
- Managing Physical Infrastructure for Cloud Environment
- Building Logical infrastructure for Cloud Environment

6 – LEGAL AND COMPLIANCE

- Legal Requirements and Unique Risks Within Cloud Environment
- Privacy Issues, Including Jurisdictional Variation
- The Audit Process, Methodologies, and Required Adaptations for a Cloud Environment
- Implications of Cloud to Enterprise Risk Management
- Outsourcing and Cloud Contract Design