Certified Cloud Security Professional Preparation

Course Overview

This course is a comprehensive review of the knowledge and practices required for understanding cloud computing and its information security risks and mitigation strategies.

Even though you have already proved yourself that you are able to secure critical assets in the cloud, but cloud threat landscape is always changing, and even the most experienced person can benefit from having a guide on the journey to success. CCSP preparation course is here to help you discover the right path, create your plan and thrive toward the examination, to prepare yourself to be awarded with the globally respected security leader's certifications in the area of cloud security.

The course will cover everything you need to know about all 6 domains of CCSP Common Body of Knowledge (CBK), how to prepare for the exam and how to fulfill the experience requirement, the processes required to gain the CCSP certification, and how to maintain it for life.

Certification Magazine lists the top 75 certifications in its 2021 Annual Salary Survey. According to their survey, CCSP is the #1 ranked certification that IT professionals plan to achieve next in their careers.

Course Objectives

Upon completion of this course, you will be embedded with appropriate skill and knowledge in the following areas:

- Describe the physical and virtual components of and identify the principle technologies of cloud-based systems
- Define the roles and responsibilities of customers, providers, partners, brokers, and the various technical professionals that support cloud computing environments
- 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
- Discuss strategies for safeguarding data, classifying data, ensuring privacy, assuring compliance with regulatory agencies, and working with authorities during legal investigations
- Contrast between forensic analysis in corporate data center and cloud computing environments
- Evaluate and implement the security controls necessary to ensure confidentiality, integrity, and availability in cloud computing
- Identify and explain the six phases of the data lifecycle
- Explain strategies for protecting data at rest and data in motion
- Describe the role of encryption in protecting data and specific strategies for key management
- Compare a variety of cloud-based business continuity/disaster recovery strategies and select an appropriate solution to specific business requirements

- Contrast security aspects of Software Development Lifecycle (SDLC) in standard data center and cloud computing environments
- Describe how federated identity and access management solutions mitigate risks in cloud computing systems
- Conduct gap analysis between baseline and industry-standard best practices
- Develop Service Level Agreements (SLAs) for cloud computing environments
- Conduct risk assessments of existing and proposed cloud-based environments
- State the professional and ethical standards of (ISC)² and the Certified Cloud Security Professional

Course Outline

Day 1:

Domain 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

Day 2:

Domain 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
- 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

Day 3:

Domain 3 - Cloud Platform and Infrastructure Security

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

Domain 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

Day 4:

Domain 4 - Cloud Application Security (continue)

- Use Verified Secure Software
- Comprehend the Specifics of Cloud Application Architecture
- Design Appropriate Identity and Access Management (IAM) Solutions

Domain 5: Cloud Security Operations

- Implement and Build Physical and Logical Infrastructure for Cloud Environment
- Operate Physical and Logical Infrastructure for Cloud Environment
- Manage Physical and Logical Infrastructure for Cloud Environment
- Implement Operational Controls and Standards (e.g., Information Technology Infrastructure Library (ITIL), International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 20000-1)

Day 5:

Domain 5 - Cloud Security operation (continue)

- Support Digital Forensics
- Manage Communication with Relevant Parties
- Manage Security Operations

Domain 6 - Legal, Risk, and Compliance

- Articulate Legal Requirements and Unique Risks within the Cloud Environment
- Understand Privacy Issues
- Understand Audit Processes, Methodologies, and Required Adaptations for a
- Cloud Environment
- Understand Implications of Cloud to Enterprise Risk Management
- Understand Outsourcing and Cloud Contract Design

Target Student

The primary audiences for this course are as follow:

- Experienced practitioners, managers, and executives those required the skillset of cloud security,information security, and cyber security
- Security Manager, Enterprise Architect, Security Administrator, Security Architect, Security Consultant, Security Engineer, Systems Architect, Systems Engineer, and Information security professionals
- Professional in Digital/IS/IT and related fields
- Individual who is interested in global leader certification in cloud security as an opportunity for career enhancement and development

Course Duration

5 days