Rhythex Consulting
Information Security, Audit & Assurance

(ISC)²

Official (ISC)² CBK Training for the CCSP

The ***Certified Cloud Security Professional*** (CCSP®) provides a comprehensive review of the knowledge required for understanding cloud computing and its information security risks and mitigation strategies. This training course will help students review and refresh their knowledge and identify areas they need to study for the CCSP exam.

Official courseware is developed by (ISC)² – creator of the CCSP CBK – to ensure your training is relevant and up-to-date. Our instructors are verified security experts who hold the CCSP and have completed intensive training to teach (ISC)² content.

Training features:

- Instruction from an (ISC)² Authorized Instructor
- Official (ISC)² Student Training Guide
- Chapter quizzes
- Interactive flash cards to reinforce learning
- Real-world learning activities and scenarios
- Case studies and discussions
- Post-course assessment questions to gauge exam readiness

Who Should Attend

This training is intended for professionals who have at least five years of full-time IT experience, including three years in information security and at least one year in cloud security, and are pursuing CCSP certification to enhance credibility and career mobility. The seminar is ideal for those working in positions such as, but not limited to:

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

Course Domains

- Domain 1. Cloud Concepts, Architecture and Design
- Domain 2. Cloud Governance: Legal, Risk and Compliance
- Domain 3. Cloud Data Security

- Domain 4. Cloud Platform and Infrastructure Security
- Domain 5. Cloud Application Security
- Domain 6. Cloud Security Operations

Course Objectives

After completing this course, the student will be able to:

- Understand legal frameworks and guidelines that affect cloud services.
- Recognize the fundamentals of data privacy regulatory/legislative mandates.
- Assess risks, vulnerability, threats and attacks in the cloud environment.
- Evaluate the design and plan for cloud infrastructure security controls.
- Evaluate what is necessary to manage security operations.
- Understand what operational controls and standards to implement.
- Describe the types of cloud deployment models in the types of "as a service" cloud models currently available today.
- Identify key terminology and associated definitions related to cloud technology. Be able to establish a common terminology for use within a team or workgroup.
- Build a business case for cloud adoption and be able to determine with business units the benefits of the cloud and cloud migration strategies.

Domains/Modules/Chapters
This course covers the following chapters and learning objectives:

Chapter 1: Cloud Concepts, Architecture and Design
- State the essential characteristics of cloud computing
- Describe the fundamental cloud computing services
- Describe the cloud computing reference architectures
- Explain cloud computing activities
- Compare cloud service capabilities and models
- Describe cloud deployment models
- Summarize economic characteristics of cloud computing
- Evaluate cloud computing ROI and KPI metrics
- Summarize cloud computing security concepts
- Describe key security considerations for each service model
- Analyze key cloud service provider contractual relationship documents

Chapter 2: Cloud Governance: Legal, Risk and Compliance
- Explain the issues with international conflict of law
- Interpret guidelines for digital forensics
- Identify the fundamentals of data privacy regulatory/legislative mandates
- Summarize audit process, methodologies and cloud-ready adaptations
- Describe risk management related to cloud services
- Identify due care/diligence activities related to service contracts

Chapter 3: Cloud Data Security
- Discuss cloud data security concepts

- Describe cryptography
- Explain data discovery and classification technologies
- Interpret cloud data storage architectures
- Analyze information rights management
- Assess cloud data security strategies
- Compare solutions for cloud data retention, deletion and archival policies
- Explain basic security concepts in the cloud

Chapter 4: Cloud Platform and Infrastructure Security

- Compare cloud infrastructure components
- Select standard practices for implementing a secure data center design
- Assess risks, vulnerability, threats and attacks in the cloud environment
- Discover components for planning and implementing security controls
- Evaluate the design and plan for cloud infrastructure security controls
- Appraise appropriate identity and access management (IAM) solutions
- Recommend business continuity and disaster recovery (BCDR) standards

Chapter 5: Cloud Application Security

- Explain training and awareness solutions for application security
- Assess challenges in the secure software development life cycle (SDLC) process
- Select a threat model for securing software development
- Demonstrate cloud software assurance and validation
- Choose verified secure software
- Explain the specifics of a cloud application architecture

Chapter 6: Cloud Security Operations

- Analyze what is used to manage and operate physical and logical infrastructure of a cloud environment
- Discuss operational controls and standards
- Identify methodologies for supporting digital forensics
- Identify critical communication needs with relevant parties
- Define auditability, traceability and accountability of security-relevant data events
- Select requirements to implement secure operations

TRAINING DETAILS 1 – WEEK DAYS	
Duration:	**5 days (Week days)**
Date:	**12th – 16th June, 2023**
Fees:	**$1,400 (Training Kits & Examination fee inclusive) per participant**
Venue:	**Online Instructor-Led**

TRAINING DETAILS 2 - WEEKENDS	
Duration:	**5 days (Weekends) – 5 Saturdays only**
Date:	**29th April – 27th May, 2023**
Fees:	**$1,400 (Training Kits & Examination fee inclusive) per participant**
Venue:	**Online Instructor-Led - weekends**