CCSP Certification Prep Course

Course Summary

Description

This course is the most comprehensive review of cloud security concepts and industry best practices covering the six domains of the (ISC)2 Common Body of Knowledge (CBK). You will gain knowledge in identifying the types of controls necessary to administer various levels of confidentiality, integrity, and availability, with regard to securing data in the cloud. You will identify the virtual and physical components of the cloud infrastructure with regard to risk management analysis, including tools and techniques necessary for maintaining a secure cloud infrastructure. You will gain an understanding in cloud software assurance and validation, utilizing secure software, and the controls necessary for developing secure cloud environments. You will identify privacy issues and audit processes utilized within a cloud environment, including auditing controls, assurance issues, and the specific reporting attributes.

This five-day program is comprised of a total of six domains and includes:
- Official (ISC)2 CCSP Training Handbook
- Official (ISC)2 CCSP Flash Cards
- CCSP Certification Exam Voucher

Objectives

After taking this course, students will be able to understand the six domains required to pass the (ISC)2 Certified Cloud Security Professional (CCSP) exam:
- Architectural concepts and design requirements
- Cloud data security
- Cloud platform and infrastructure security
- Cloud application security
- Operations
- Legal and compliance

Topics

- Architecture Concepts and Design Requirements
- Cloud Data Security
- Cloud Platform and Infrastructure Security
- Cloud Application Security
- Operations
- Legal and Compliance

Audience

This course is designed for anyone whose position requires CCSP certification and for individuals whose responsibilities involve procuring, securing, and managing cloud environments or purchased cloud services.

Prerequisites

Before taking this course, students should be experienced information security professionals with at least five years of IT experience, including three years of information security and at least one year of cloud security experience. Students should also have taken the CISSP Certification Prep Course (PT20532).

Duration

Five days

![ProTech logo — protechtraining.com]

CCSP Certification Prep Course

Course Outline

I. Architecture Concepts and Design Requirements
   A. Cloud Computing Concepts
   B. Cloud Reference Architecture
   C. Security Concepts Relevant to Cloud Computing
   D. Design Principles of Secure Cloud Computing
   E. Trusted Cloud Services

II. Cloud Data Security
   A. Cloud Data Lifecycle
   B. Design and Implement Cloud Data Storage Architectures
   C. Design and Apply Data Security Strategies
   D. and Implement Data Discovery and Classification Technologies
   E. Design and Implement Data Rights Management
   F. Design and Implement Relevant Jurisdictional Data Protections for Personally Identifiable Information (PIN)
   G. Plan and Implement Data Retention, Deletion, and Archiving Policies
   H. Design and Implement Auditability, Traceability, and Accountability of Data Events

III. Cloud Platform and Infrastructure Security
   A. Cloud Infrastructure Components
   B. Risks Associated to Cloud Infrastructure
   C. Design and Plan Security Controls
   D. Plan Disaster Recovery and Business Continuity Management

IV. Cloud Application Security
   A. Need for Training and Awareness in Application Security
   B. Cloud Software Assurance and Validation
   C. Use Verified Secure Software
   D. Software Development Life-Cycle (SDLC) Process
   E. Apply the Software Development Life-Cycle
   F. Specifics of Cloud Application Architecture
   G. Design Appropriate Identity and Access Management (IAM) Solutions

V. Operations
   A. Support the Planning Process for the Data Center Design
   B. Implement and Build Physical Infrastructure for Cloud Environment
   C. Run Physical Infrastructure for Cloud Environment
   D. Manage Physical Infrastructure for Cloud Environment
   E. Build Logical Infrastructure for Cloud Environment
   F. Run Logical Infrastructure for Cloud Environment
   G. Manage Logical Infrastructure for Cloud Environment
   H. Ensure Compliance with Regulations and Controls (ITIL, ISO/IEC 20000-I)
   I. Conduct Risk Assessment to Logical and Physical Infrastructure
   J. Collection, Acquisition, and Preservation of Digital Evidence
   K. Manage Communication with Relevant Parties

VI. Legal and Compliance
   A. Legal Requirements and Unique Risks within the Cloud Environment
   B. Privacy Issues, Including Jurisdictional Variation
   C. Audit Process, Methodologies, and Required Adaptions for a Cloud Environment
   D. Implications of Cloud to Enterprise Risk Management
   E. Outsourcing and Cloud Contract Design
   F. Execute Vendor Management