Certified Cloud Security Professional (CCSP) Bootcamp

Length: 5 days
Format: Bootcamp
Time: Day

About This Course

This instructor-led training course provides a comprehensive review of information security concepts and industry best practices, covering the 6 domains of the CCSP CBK:

* Architectural Concepts & Design Requirements
* Cloud Data Security
* Cloud Platform & Infrastructure Security
* Cloud Application Security
* Operations
* Legal & Compliance

This training course will help candidates review and refresh their cloud security knowledge and help identify areas they need to study for the CCSP exam.

Required Exams

CCSP Exam

Audience Profile

CCSP is most appropriate for those whose day-to-day responsibilities involve procuring, securing and managing cloud environments or purchased cloud services. In other words, CCSPs are heavily involved with the cloud. Many CCSPs will be responsible for cloud security architecture, design, operations, and/or service orchestration.

The CCSP credential is suitable for mid-level to advanced professionals involved with IT architecture, web and cloud security engineering, information security, governance, risk and compliance, and even IT auditing.

Course Objectives

Outline

Module 1: * Cloud definitions
* Roles and Benefits
* IaaS PaaS SaaS
* Cloud Deployment Considerations and Multi Tenancy
* Public, Private, Community, Hybrid
* Key Principles of Enterprise Architecture

Module 2: * Data Storage
* Data Security Lifecycle
* Database Security
* Encryption
* Privacy
* Data Protection Policies
* Event Management

Module 3: * Securing the Hypervisor and Guest OS
* Virtualization Concerns
* Customer Concerns
* Data Center Concerns

Module 4: * Determining Data Sensitivity
* Who is Responsible for Security in Cloud Modules
* SDLC in the Cloud
* OWASP 1 through 5
* OWASP 6 through 10
* Defensive Coding
* Risks and Controls
* Crypto in the Cloud
* Common Architectures
* Identify and Access Management
* Data and Media Sanitization
* Intro to ID
* Defining Identity and Access Management
* Virtualization Overview
* Threat Modeling
* Threats to Cloud Computing
* Types of Testing
* BCP
* Non-Functional Testing
* Vulnerability Scans and Penetration Testing

Module 5: * Physical and Environmental Controls
* HR Controls
* Network Security
* Risk Intro
* Risk Assessment
* Risk Analysis
* Risk Mitigation

Module 6: * Incident Response

* Intro to Forensics
* Forensic Investigation Process
* Types of Evidence
* Types of Laws
* Specific Laws