

Certified Cloud Security Engineer

Course Duration: 40 Hrs.

Course code: 312-40

Course Overview

The Certified Cloud Security Engineer (C|CSE) course is a hands-on, multi-cloud security certification program designed to provide cybersecurity professionals with a holistic understanding of cloud security and practical skills, covering both vendor-neutral and vendor-specific concepts.

What you'll learn?

❖ **Cloud Security Fundamentals:**

Understanding the different cloud models (IaaS, PaaS, SaaS), shared responsibility model, and common cloud security threats and vulnerabilities.

❖ **Identity and Access Management (IAM):**

Learning about authentication, authorization, and access control mechanisms in cloud environments, including multi-factor authentication and role-based access control.

❖ **Data Security:**

Understanding data encryption, storage security, and data loss prevention techniques in the cloud.

Target Audience

The target audience for a Certified Cloud Security Engineer (C|CSE) course includes IT professionals, cybersecurity professionals, career starters, and individuals looking to enhance their cloud security knowledge and skills, including those with little to no work experience.

Pre-Requisites

To prepare for a Certified Cloud Security Engineer (CCSE) course, you should have a basic understanding of cloud computing concepts, IT security principles, and the shared responsibility model in cloud environments, along with some experience with cloud service providers, operating systems, networking, and virtualization technologies.

Course content

MODULE 01: Introduction to Cloud Security

It highlights various factors for evaluating service providers and understanding the shared security responsibility model of service providers. Understanding the shared responsibility model provided by the cloud service provider is essential to configuring the cloud environment securely and protecting organizational resources.

MODULE 02: Platform and Infrastructure Security in the Cloud

This module explains the key components and technology that make the architecture of the cloud and the various techniques involved in securing the multi-tenancy, virtualized, physical, and logical cloud components.

MODULE 03: Application Security in the Cloud

This module focuses on securing cloud applications, from designing to deployment of an application in the cloud.

MODULE 04: Data Security in the Cloud

Data security is the major concern while migrating to the cloud. This module covers the basics of cloud data storage, its life cycle, and various controls to protect data-in-rest and data-in-transit in the cloud.

MODULE 05: Operation Security in the Cloud

This module includes the security controls for building, implementing, operating, managing, and maintaining physical and logical infrastructure for cloud environments.

MODULE 06: Penetration Testing in the Cloud

This module demonstrates how to implement a comprehensive penetration testing methodology for assessing the security of an organization's cloud infrastructure.

MODULE 07: Incident Detection and Response in the Cloud

An incident response (IR) plan is crucial to prevent security breaches in the cloud. This module describes the incident response life cycle and highlights the considerations for responders in each phase of the IR plan in a cloud environment.

MODULE 08: Forensics Investigation in the Cloud

Access to forensic data and the forensic investigation process in a cloud computing environment differ from the network forensic investigation process.

MODULE 09: Business Continuity and Disaster Recovery in the Cloud

Business Continuity and Disaster Recovery (BC/DR) is important in the cloud because a third party manages the resources.

MODULE 10: Governance, Risk Management, and Compliance in the Cloud

This module highlights the standards, policies, and legal issues related to the cloud. It highlights various legal and compliance issues found in a cloud environment.

MODULE 11: Standards, Policies, and Legal Issues in the Cloud

It discusses various cloud security standards and audit planning in the cloud. It demonstrates the features, services, and tools for compliance and auditing in Azure, AWS, and Google Cloud.

Exam Preference

Exam Code	312-40
Number Of Questions	125
Passing Score	70%
Length Of Test	240 Minutes

