INFOSECTRAIN

CCSK

Certificate of Cloud Security Knowledge

Certificate of Cloud Security Knowledge, widely known as CCSK training course is an end to end knowledge-focused training and certification program that helps security professionals gain deep insights of the cloud security and related aspects while delivering far reaching understanding of how to address...

www.infosectrain.com
sales@infosectrain.com

Overview

Certificate of Cloud Security Knowledge, widely known as CCSK training course is an end to end knowledge-focused training and certification program that helps security professionals gain deep insights of the cloud security and related aspects while delivering far reaching understanding of how to address various cloud security concerns. The CCSK is an all-embracing training covering core essentials of cloud computing architectural framework, governance and operations in the cloud such as legal issues, information and data security management, and data centers operations among others. This highly valued cloud security programs allows security practitioners to advance their career with extensive know of the aforementioned cloud security areas.

Target Audience

The Certificate of Cloud Security Knowledge training course is highly recommended for:

- IT auditors
- IT professionals intending to excel their career opportunities with cloud security skills

Pre-Requisite

- Recommended a basic understanding of various security fundamentals including firewalls, encryption, identity management and secure developmentz

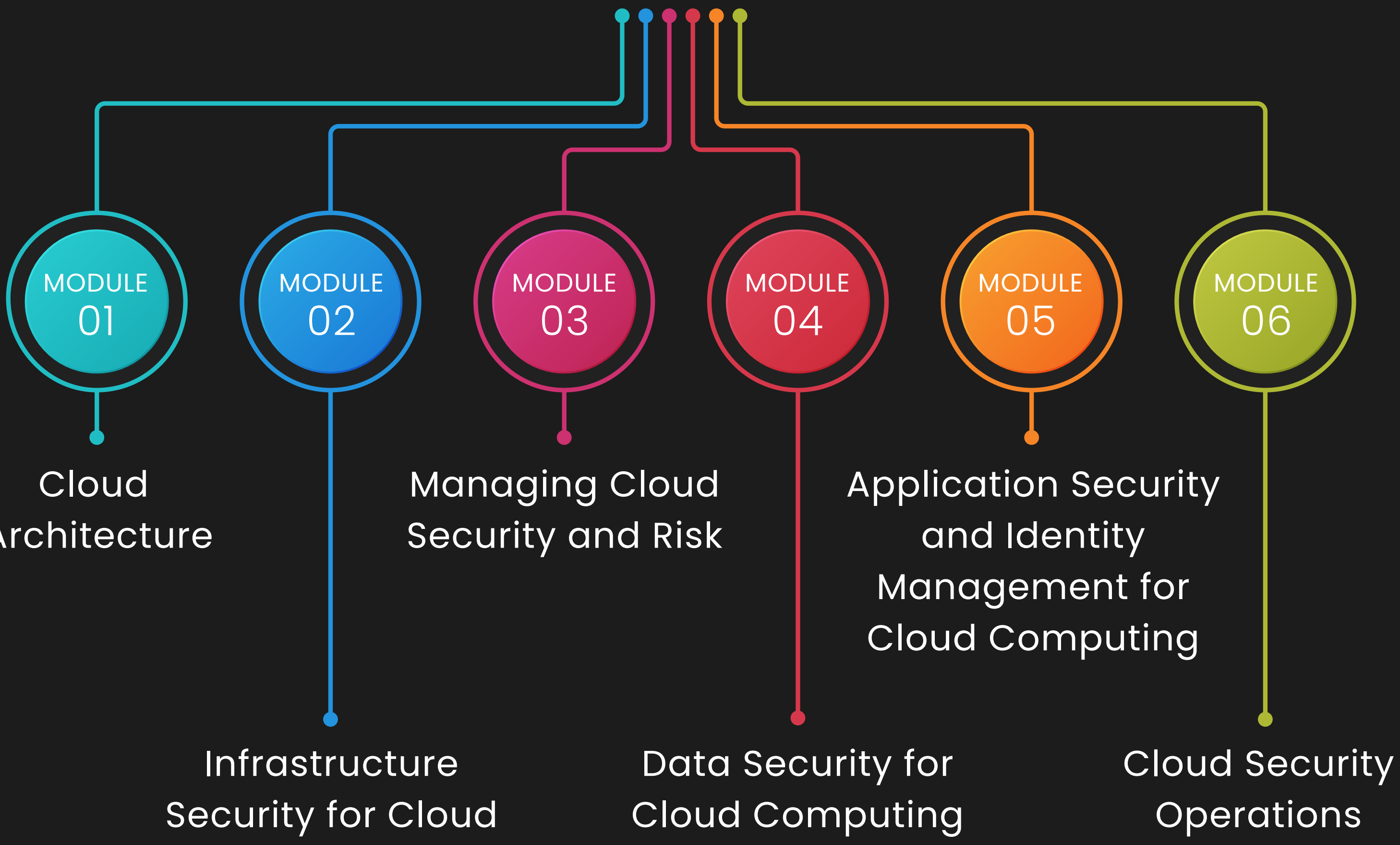
Exam Information

Certification Name	Certificate of Cloud Security Knowledge (CCSK)
Test Format	Multiplechoice questions
Number of Questions	60
Test Duration	90 minutes

Why Infosec Train?

- Certified & Experienced Instructor
- Flexible Schedule
- Access to the recorded sessions
- Post Training Support
- Tailor Made Training
- 4 hrs/day in Weekend/ Weekday

CCSK FOUNDATION COURSE



MODULE 01

Cloud Architecture

MODULE 02

Infrastructure Security for Cloud

MODULE 03

Managing Cloud Security and Risk

MODULE 04

Data Security for Cloud Computing

MODULE 05

Application Security and Identity Management for Cloud Computing

MODULE 06

Cloud Security Operations

Module 1. Cloud Architecture

Unit 1 - Introduction to Cloud Computing
Unit 2- Introduction & Cloud Architecture
Unit 3 - Cloud Essential Characteristics
Unit 4 - Cloud Service Models
Unit 5 - Cloud Deployment Models
Unit 6 - Shared Responsibilities

Module 2. Infrastructure Security for Cloud

Unit 1 - Module Intro
Unit 2 - Intro to Infrastructure Security for Cloud Computing
Unit 3 - Software Defined Networks
Unit 4 - Cloud Network Security
Unit 5 - Securing Compute Workloads
Unit 6 - Management Plane Security
Unit 7 - BCDR

Module 3. Managing Cloud Security and Risk

Unit 1 - Module Introduction
Unit 2 - Governance
Unit 3 - Managing Cloud Security Risk
Unit 4 - Legal
Unit 5 - Legal Issues In Cloud
Unit 6 - Compliance
Unit 7 - Audit
Unit 8 - CSA Tools

Module 4. Data Security for Cloud Computing

Unit 1 - Module Introduction
Unit 2 - Cloud Data Storage
Unit 3 - Securing Data In The Cloud
Unit 4 - Encryption For IaaS
Unit 5 - Encryption For PaaS & SaaS
Unit 6 - Encryption Key Management
Unit 7 - Other Data Security Options
Unit 8 - Data Security Lifecycle

Module 5. Application Security and Identity Management for Cloud Computing

Unit 1 - Module Introduction
Unit 2 - Secure Software Development Life Cycle (SSDLC)
Unit 3 - Testing & Assessment
Unit 4 - DevOps
Unit 5 - Secure Operations
Unit 6 - Identity & Access Management Definitions
Unit 7 - IAM Standards
Unit 8 - IAM In Practice

Module 6. Cloud Security Operations

Unit 1 - Module Introduction
Unit 2 - Selecting A Cloud Provider
Unit 3 - SECaaS Fundamentals
Unit 4 - SECaaS Categories
Unit 5 - Incident Response
Unit 6 - Domain 14 Considerations
Unit 7 - CCSK Exam Preparation

CCSK PLUS COURSE

*The CCSK Plus Course includes all the modules in the CCSK Foundation course with additional material.

The CCSK Plus builds on the foundation class with expanded material and offers extensive hands-on activities that reinforce classroom instruction. Students engage in a scenario of bringing a fictional organization securely into the cloud, which gives them the opportunity to apply their knowledge by performing a series of activities that would be required in a real-world environment. Below is an outline of the lab material covered in the CCSK Plus class.

Core Account Security

Students learn what to configure in the first 5 minutes of opening a new cloud account and enable security controls such as MFA, basic monitoring, and IAM.

IAM and Monitoring In-Depth

Attendees expand their work on the first lab and implement more-complex identity management and monitoring. This includes expanding IAM with Attribute Based Access Controls, implementing security alerting, and understanding how to structure enterprise-scale IAM and monitoring.

Network and Instance Security

Students create a virtual network (VPC) and implement a baseline security configuration. They also learn how to securely select and launch a virtual machine (instance), run a vulnerability assessment in the cloud, and connect to the instance.

Encryption and Storage Security

Students expand their deployment by adding a storage volume encrypted with a customer managed key. They also learn how to secure snapshots and other data.

Application Security and Federation

Students finish the technical labs by completely building out a 2-tier application and implementing federated identity using OpenID.

Risk and Provider Assessment

Students use the CSA Cloud Controls Matrix and STAR registry to evaluate risk and select a cloud provider.

INFOSECTRAIN

www.infosectrain.com | sales@infosectrain.com