Cloud Security: Scope & Sequence

Last updated: 31 August 2021

Table of Contents

Introduction

With more companies moving to the cloud, the need for cloud security is becoming increasingly apparent. Because of this, the IT and cybersecurity industries have seen an increase in demand for knowledgeable experts to help companies stay secure in the cloud.

The Certificate of Cloud Security Knowledge (CCSK) is an introductory course targeted towards professionals working in IT and cybersecurity. This course provides a broad overview of cloud security and allows students to gain critical insights into how security issues change in the cloud, including data security, key management, and identity and access management.

Target Audience

This introductory level course to cloud security is targeted towards learners enrolled in technology degree programs at higher education institutions and IT professionals who want to pursue a career in Cloud Security.

Prerequisites

There is no official work experience required, however, it is helpful for attendees to have at least a basic understanding of security fundamentals such as firewalls, secure development,

encryption, and identity and access management which can be learned by taking the Cisco Networking Academy Introduction to Cybersecurity and Cybersecurity Essentials courses.

Certificate

- This course prepares students to take the certificate exam to earn their CCSK.
- This course also provides possible Continuing Professional Education (CPE) credits.

Although there are currently no official CPE designations for this course, we do issue a certificate of completion with the stated number of hours it takes to complete the course. Students can then use this certificate of completion for CPE credit submission. Please note, however, that the actual qualification and distribution of CPE credits will be determined by whoever receives the request.

Course Description

Learn how to develop a holistic cloud security program relative to globally accepted standards using the Cloud Security Alliance (CSA) Security Guidance V.4 and recommendations from European Union Agency for Cybersecurity (ENISA). You will also be introduced to CSA's governance, risk, and compliance tool for the cloud - Cloud Controls Matrix (CCM).

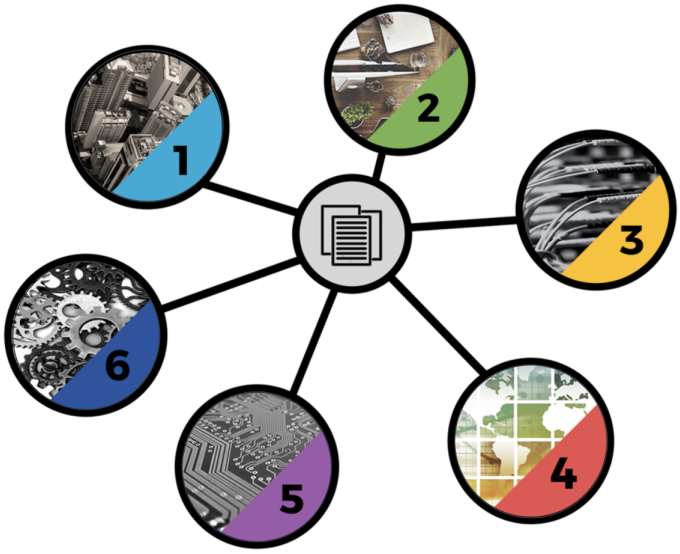
Curriculum Objectives

The aim of this course is to spark the student's interest in cloud security and familiarize the student with the universal concepts of cloud computing. In addition, the course provides students with a base of knowledge on cloud computing security theory and acquaints students with security threats and best practices for securing the cloud. This course also assists students as they prepare to take the CCSK exam.

Course Structure

Split into six modules, this foundation course covers all the domains from the CSA Security Guidance v4 along with information on the Cloud Controls Matrix and recommendations from ENISA.

At the end of each unit is a knowledge check that students must pass before moving forward. In addition, students will also be able to take a final exam at the end of the course to help as they prepare to take the exam.



Course Objectives

Module 1: Cloud Architecture

- *Understand the components of cloud infrastructure*
- *Assess the security implications of virtual networks and workloads*
- *Learn the security advantages and disadvantages of working with cloud infrastructure*
- *Evaluate how to secure the cloud management plane*
- *Learn how to manage business continuity for cloud computing*

Module 2: Infrastructure Security for Cloud

- *Understand the components of cloud infrastructure*
- *Assess the security implications of virtual networks and workloads*
- *Learn the security advantages and disadvantages of working with cloud infrastructure*
- *Evaluate how to secure the cloud management plane*
- *Learn how to manage business continuity for cloud computing*

Module 3: Managing Cloud Security and Risk

- *The implications of cloud on governance, with a focus on contracts and controls*
- *How cloud affects enterprise risk management*
- *Some top-level legal areas cloud tends to affect (but not legal advice)*
- *Managing compliance and audits for cloud deployments*
- *Tools from the Cloud Security Alliance to help assess and manage risk*

Module 4: Data Security for Cloud Computing

- *Understand the different cloud storage models*
- *Define security issues for data in the cloud*
- *Assess the role and effectiveness of access controls*
- *Learn different cloud encryption models*

- *Understand additional data security options*
- *Introduce data security lifecycle*

Module 5. Application Security and Identity Management for Cloud Computing
- *Discover how application security differs in cloud computing*
- *Review secure software development basics and how those change in the cloud*
- *Leverage cloud capabilities for more secure cloud applications*

Module 6. Cloud Security Operations
- *How to select cloud providers*
- *The advantages and disadvantages of security as a service*
- *The different major security as a service categories*
- *How to respond to security incidents in the cloud*
- *The security issues of technologies related to cloud computing: Big Data, mobile, serverless, IoT*
- *Security as a service recommendations*

Course Outline

The CCSK Foundation course starts with the fundamentals, then increases in complexity as it works through all 14 domains of the CSA Security Guidance, recommendations from the European Union Agency for Cybersecurity (ENISA), and an overview of the Cloud Controls Matrix (CCM).

Module 1. Cloud Architecture
The fundamentals of cloud computing, including definitions, architectures, and the role of virtualization. Key topics include cloud computing service models, delivery models, and fundamental characteristics. It also introduces the Shared Responsibilities Model and a framework for approaching cloud security.

Topics Covered:
- 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
Delves into the details of securing the core infrastructure for cloud computing- including cloud components, networks, management interfaces, and administrator credentials. It delves into virtual networking and workload security, including the basics of containers and serverless.

Topics Covered:
- 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 - Business Continuity and Disaster Recovery (BCDR)

Module 3. Managing Cloud Security and Risk
Covers important considerations for managing security for cloud computing. It begins with risk assessment and governance, then covers legal and compliance issues, such as discovery requirements in the cloud. It also covers important CSA risk tools including the Consensus Assessment Initiative Questionnaire (CAIQ), Cloud Controls Matrix (CCM), and Security, Trust, Assurance, and Risk (STAR) registry.

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

Module 4. Data Security for Cloud Computing
Covers information lifecycle management for the cloud and how to apply security controls, with an emphasis on public cloud. Topics include the Data Security Lifecycle, cloud storage models, data security issues with different delivery models, and managing encryption in and for the cloud, including customer managed keys (BYOK).

Topics Covered:
- 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
Covers identity management and application security for cloud deployments. Topics include federated identity and different Identity and Access Management (IAM) applications, secure development, and managing application security in and for the cloud.

Topics Covered:

- 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

Key considerations when evaluating, selecting, and managing cloud computing providers. We also discuss the role of security as a service providers and the impact of cloud on incident response.

Topics Covered:

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

Equipment/System Requirements

This course is accessed online with no additional equipment or system requirements.