CCSK Course Outlines

cloud security alliance

CCSK COURSE OUTLINES

Preview what you will be learning in the CCSK Foundation or CCSK Plus courses. View the outline of the modules and materials covered in the CCSK Foundation Course along with the additional lab content covered in the CCSK Plus course below.

CCSK FOUNDATION COURSE

The CCSK Foundation course starts with the fundamentals, then increases in complexity as it works through all 16 domains of the CSA Security Guidance, recommendations from the European Union Agency for Network & Information Security (ENISA), and an overview of the Cloud Controls Matrix.

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 - 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 CAIQ, CCM, and STAR registry.

Topics Covered:

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

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 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 - 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.

