

Cloud Security Alliance CCSK Training

Course Description

Cloud Computing Security Knowledge – Basic

There is a lot of hype and uncertainty around cloud security, but this class will slice through the hyperbole and provide students with the practical knowledge they need to understand the real cloud security issues and solutions. The Cloud Computing Security Knowledge- Basic class provides students a comprehensive one day review of cloud security fundamentals and prepares them to take the Cloud Security Alliance CCSK certification exam.

Starting with a detailed description of cloud computing, the course covers all major domains in the latest Guidance document from the Cloud Security Alliance, and the recommendations from the European Network and Information Security Agency (ENISA). This class is geared towards security professionals, but is also useful for anyone looking to expand their knowledge of cloud security. (We recommend attendees have at least a basic understanding of security fundamentals, such as firewalls, secure development, encryption, and identity management).

Course Outline:

This course is broken out into 56 modules that cover the 13 domains of the CSA Guidance and the ENISA Cloud Computing: Benefits, Risks and Recommendations for Information Security.

Module 1: Introduction to Cloud Computing. This module covers 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 a model for assessing the risk of moving to the cloud.

Module 2: Creating and Securing a Public Cloud Instance. This module digs into the details of the different cloud delivery models and their basic security issues. Students will learn the differences between security responsibilities for SaaS, PaaS, and IaaS, and key questions to ask a potential provider. The instructors will also demonstrate creating and applying security to a simple cloud instance on IaaS.

Module 3: Managing Cloud Security and Risk. This module 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 finishes with a discussion on portability and interoperability and managing incident response when working with cloud providers.

Module 4: Securing Public Cloud Data. One of the biggest issues in cloud security is protecting data. This module 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.

Module 5: Securing Cloud Users and Applications. This module 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.

Module 6: Creating and Securing a Private Cloud. In this module we move from the public cloud to the private cloud. Although we tend to have more control over private clouds, that doesn't mean they are immune to security issues. Topics include security risks of private clouds, and the management and security tools available to mitigate them.

Note- due to time constraints and the extensive amount of material covered in this class we are not able to include hands-on activities. But instructors will lead key demonstrations and provide guidance so you can attempt to apply your skills outside the classroom using a self-study guide.

Cloud Computing Security Knowledge - Plus

The CCSK- Plus class builds upon the CCSK Basic class with expanded material and extensive hands-on activities with a second day of training. Students will learn to apply their knowledge as they perform a series of exercises as they complete a scenario bringing a fictional organization securely into the cloud.

This second day of training includes additional lecture, although students will spend most of their time assessing, building, and securing a cloud infrastructure during the exercises.

Course Outline:

This is a two day class that begins with the CCSK- Basic training, followed by a second day of additional content and hands-on activities. The Plus content expands the course with:

Exercise 1: Introduction and Risk Analysis. Students will be introduced to the day's scenario and build a threat model for migrating to the cloud.

Exercise 2: Create and Secure a Public Cloud Instance. Students will create a basic cloud instance on a public cloud infrastructure and establish a security baseline.

Topics include creating an AWS instance, establishing network security, and understanding machine images.

Exercise 3: Encrypt Public Cloud Data. In this module students will dive into cloud storage options and learn the basics to encrypt data for their public cloud deployment.

Exercise 4: Create and Secure a Cloud Application: Now the students will secure their first public application for the cloud, following best practices such as architecting their cloud application stack and managing appropriate network security.

Exercise 5: Identity Management for the Cloud. Students will create a basic federated identity infrastructure to support their cloud application and learn additional details on standards like SAML and OAuth.

Exercise 6: Private Cloud Risk Analysis. Students will change gears and assess the risk of building a private, internal cloud computing environment.

Exercise 7: Create and Secure a Private Cloud. Students will establish a basic private cloud, then launch and secure their first cloud instances.

