HP Education Services Course Overview

Cloud Computing Security Knowledge - CCSK Plus (V3.1) (H8P76S)

This course slices through the hyperbole and provides students with the practical knowledge they need to understand the real cloud security issues and solutions. The training gives students a comprehensive review of cloud security fundamentals. Students will learn to apply their knowledge by performing a series of exercises and hands-on labs that brings a fictional organization securely into the cloud.
This course prepares students for the Cloud Security Alliance CCSK certification exam.

Course Description

Beginning 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). During the final day of training, students assess, build, and secure a cloud Infrastructure.

All students attending this training automatically receive an HP Helion Cloud account for a period of 30 days. This allows students to successfully complete all hands-on exercises during training. After training, continued access to the Helion Cloud may be used to reinforce class learning with additional practice.

Hands-on is performed using the HP Helion Cloud. Additionally, students receive formally designed lab exercises that they may optionally complete using the Amazon Cloud.

Included:
30-day HP Helion Cloud Account (no credit card required)
CSA CCSK exam voucher (valid for 2 attempts)

Audience

This class is geared towards security professionals, but is also useful for anyone looking to expand their knowledge of cloud security.

Course title:	Cloud Computing Security Knowledge - CCSK Plus (V3.1)
HP product number:	H8P76S
Category/Subcategory:	Security
Course length:	3 days
Level:	Intermediate
Delivery language:	English
To order:	You can order this course online at **http://www.hp.com/learn/security**. At the site, select a country, then choose "registration" or "Book a course" and fill out the online registration form.

Prerequisites

We recommend attendees have at least a basic understanding of security fundamentals, such as firewalls, secure development, encryption, and identity management. For security foundations training, refer to the HP Information Security Common Body of Knowledge curriculum found at hp.com/learn/security.

Why education services from HP?

- HP is a CSA Master Training Partner
- Unmatched technical expertise and support for HP products and technologies
- Recognized as an IDC MarketScape leader for IT education (IDC MarketScape: Worldwide IT Education and Training 2012 Vendor Analysis, doc #232870, February 2012)
- Global training with more than 90 training locations worldwide
- More than 30 years of Education Consulting
- Comprehensive curriculum of job-specific training leading to vendor certification
- Training you need, when and where you need it with our Virtual Instructor Led Training (VILT)
- Streamlined purchase and management of training with HP Care Pack Services for Education

Detailed course outline

Module 1 Introduction And Cloud Architectures

Objectives

- Define cloud computing and its business benefits.
- List the attributes that define cloud computing.
- Identify pros and cons of cloud computing choices.
- Discuss the different components of the cloud computing stack.
- Differentiate service models and deployment models.
- Describe individual service models and how they operate.
- Describe individual deployment models and how they operate.

Module 2 Adapting Governance And Information Risk Mgt

Objectives

- List the key elements of information security governance related to cloud operations
- Identify strategies to manage provider governance
- Describe the steps in risk management lifecycle specifically for moving to the cloud
- List alternatives for risk treatment used by CSA
- Discuss levels of maturity in risk management
- Differentiate risk treatment implementation responsibility across service models
- Identify types of assets and how to evaluate their value to the organization
- Describe how incidents change in cloud
- Identify challenges in incident response when working with a cloud provider at various service levels
- List the steps in responding to a security incident

Module 3 Compliance And Audit In The Cloud

Objectives

- Identify types legal responsibilities based on business compliance, regulations, and geography
- Discuss responsibility and accountability for assessing and mitigating information security risks
- Discuss contractual elements that support compliance and verification
- Describe types of audit and how to plan for them
- List required artifacts for auditing
- Describe how to handle the results of an audit

Module 4 Physical And Administrative Controls

Objectives

- Recognize sample security controls for data center perimeter
- Describe how cloud provider employment policies affect information security

Module 5 Infrastructure Technology

Objectives

- Identify architectural layers in a cloud environment.
- Provide a high level description of the operation of hypervisors in creating, updating, and destroying virtual machines
- Discuss operation of the cloud management plane.
- List elements of virtual networking.
- Give a general description of the operation of shared storage.
- List additional infrastructure elements required in the operation of a cloud architecture.
- Differentiate the infrastructure delivery for different service models.

Module 6 Securing Cloud Infrastructure

Objectives

- Discuss the security advantages and disadvantages of working with virtual infrastructure
- Identify security concerns in a cloud environment
- List elements to secure the host and hypervisor levels
- Discuss how to secure the cloud management plane
- Describe how to secure virtual networking
- Describe how to secure virtual machines during creation, use, movement, and destruction
- List ways to secure API interfaces
- Learn the security basics for the difference service models
- Assess the security implications of different deployment models

Module 7 Data Security For Cloud Computing

Objectives

- Describe different cloud storage models
- Define security issues for data in the cloud
- Describe data security lifecycle

- Use functions, actors, and locations to identify cloud security issues, and specific controls to address security and governance
- Discuss data encryption and key management
- Describe forms of data loss prevention

Module 8 Cloud Identity And Access Management

Objectives

- Define identity, entitlement, and access management terms
- Differentiate between identity and access management
- List best practices in provisioning identity and entitlement
- Describe how to build an entitlement matrix
- Differentiate between authentication, authorization, and access control
- Describe architectural models for provisioning and how to integrate them
- Describe the operation of federated identity management
- List key identity management standards and how they facilitate interoperation

Module 9 Developing And Securing Cloud Applications

Objectives

- Describe the importance of standard interfaces and the potential costs of vendor lock-in
- Differentiate between portability and interoperability
- Describe how to minimize disruption of service during vendor change
- Define Application Architecture, Design, and Operations lifecycle
- Discuss impact of cloud operations on SDLC and identify threat modeling requirements
- Differentiate static and dynamic testing methods and give examples of each
- Examine application security tools and vulnerability management processes
- Discuss the role of compliance in cloud applications
- Describe methods of ongoing application monitoring

Module 10 Security As A Service

Objectives

- Define SECaaS
- List advantages and concerns for SECaaS
- Describe various forms of security offered as services

Module 11 Vendor Relationships

Objectives

- List elements of risk management planning and implementation to look for in a cloud service provider
- Identify strategies to manage provider governance
- Advocate for contractual clarity in all phases of risk management and information security
- Describe elements of supplier assessment for cloud providers

Module 12 Cloud Risk Assessment Exercise – Public Cloud

Objectives

- Perform minimal risk assessment for moving data and/or processing to the cloud
  - Evaluate asset types
  - Estimate impact of breach
  - Map to service and deployment models
  - Sketch data flows

Module 13 Create And Secure A Public Cloud Instance Lab

Objectives

- Reinforce your understanding of public IaaS architectures
- Define core IaaS components/options
  - Images
  - Instances
  - Volumes
  - Regions, Security Groups, and Availability Zones
  - Object storage and snapshots
- Launch and connect to your first instance
  - Manage Images and host keys
- Secure your instance
- Verify instance availability

Module 14 Encrypting A Storage Volume Lab

Objectives

- Describe why encryption is important
- Select an encryption method
- Create and attach a storage volume
- Encrypt and format the volume
- Configure key management options
- Predict the effects of rebooting
- Attach the encrypted volume to another instance (Advanced Exercise)
- Install MySQL on the encrypted volume

Module 15 Create And Secure a Cloud Application Lab

Objectives

- Understand basic cloud application architectures
- Manage multiple Security Groups for enhanced network security
- Assess the security risks of snapshots

Module 16 Identity And Access Management Lab

Objectives

- Secure your HP Helion “management plane” with IAM
- Describe federated identity architectures
- Implement federated identity for your application using OpenID
- Describe how to apply the same principles in an enterprise production environment

For more information

To locate country contact information and to learn more about education services, please visit our worldwide web site at
http://www.hp.com/learn/security
http://www.csathailand.org
e-mail: academy@csathailand.org
Tel. +666 2532 4628

H8P76sa.00 Created on Jan 2015