Certificate of Cloud Security Knowledge (CCSK) - Plus H8P76S

HPE course number	H8P76S
Course length	3 Days
Delivery mode	ILT, VILT
View schedule, local pricing, and register	**View now**
View related courses	**View now**

Why HPE Education Services?

- Comprehensive worldwide HPE technical, IT industry and personal development training
- Training and certification preparation for ITIL®, Security, VMware®, Linux, Microsoft and more
- Innovative training options that match individual learning styles
- Anytime, anywhere remote learning via HPE Digital Learner subscriptions
- Verifiable digital badges for proof of training, skill recognition and career development
- Simplified purchase options with HPE Training Credits

This course slices through the hyperbole and provides students with the practical knowledge to understand the real cloud security issues and solutions. The course provides a comprehensive review of cloud security fundamentals, including a detailed description of cloud computing. It covers all major domains in the latest guidance document from the Cloud Security Alliance, as well as the recommendations from the European Network and Information Security Agency
(ENISA). Throughout the training, students assess, build, and secure a cloud infrastructure through hands-on labs using Amazon Cloud.
This course prepares students for the Cloud Security Alliance CCSK certification exam.

Audience

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

Prerequisites

- We recommend attendees have at least a basic understanding of security fundamentals, including firewalls, secure development, encryption, and identity management.
- For security foundations training, refer to HL945S: Information Security Essentials

Course objectives

The objective of this course is to provide students with a base of knowledge of cloud computing security theory and practice, and to assist students in taking the CCSK exam.

Certifications and related examinations

The course gives students a comprehensive review of cloud security fundamentals and prepares them for the Cloud Security Alliance CCSK certification exam. The course includes an exam voucher from the Cloud Security Alliance for the CCSK certification exam.

Detailed course outline

Module 1: Introduction and Cloud Architectures	• 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 • Discuss shared responsibility for security across models • Identify cloud impact on related technologies that rely on cloud, or are commonly seen in cloud deployments
Module 2: Infrastructure Security for Cloud	• Discuss the security advantages and disadvantages of working with virtual infrastructure • Discuss how to secure the cloud management plane • Understand the components of cloud infrastructure • Assess the security implications of virtual networks and workloads	• Discuss the security advantages and disadvantages of working with virtual infrastructure • Describe how to secure virtual networking • Describe how to secure virtual workloads during creation, use, movement, and destruction
Module 3: Managing Cloud Security and Risks	• List the key elements of information security governance related to cloud operations • Review the implications of cloud on governance, with a focus on contracts and controls • Identify strategies to manage provider governance • Describe the steps in the risk management lifecycle specifically for moving to the cloud • Differentiate risk treatment and implementation responsibility across service models • Identify the tools of governance • Manage compliance and audits for cloud deployments. • Discuss tools from the Cloud Security Alliance to help assess and manage risk • Identify legal responsibilities based on business compliance, regulations, and geography	• Discuss contractual elements that support compliance and verification • Identify jurisdiction and regulation requirements • Describe legal ramifications and procedures for legal accountability • Describe types of audit and how to plan for them • List required artifacts for auditing • Describe how to handle the results of an audit • Discuss SLAs and setting expectations around what the customer does versus what the provider does (the most important aspect of incident response for cloud-based resources) • Use functions, actors, and locations to identify cloud security issues, and specific controls to address security and governance • Review the data security lifecycle in the cloud
Module 4: Data Security for Cloud	• Understand business continuity and disaster recovery in the cloud • Define security issues for data in the cloud • Assess the role and effectiveness of access controls	• Describe data security lifecycle for cloud use • Discuss data encryption and key management • Describe forms of data loss prevention
Module 5: Securing Cloud Applications and Users	• Discover how application security differs in cloud computing • Review secure software development basics and how they change in the cloud • Leverage cloud capabilities for more secure cloud applications • Describe the importance of standard interfaces and the potential costs of vendor lock-in • Define the application architecture, design, and operations lifecycle • Discuss the 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	• 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 6: Cloud Security Operations	• Identify challenges in incident response when working with a cloud provider at various service levels • Understand why cloud incidents need to be handled differently • Explain the incident response lifecycle • Define SECaaS	• List advantages and concerns for SECaaS • Describe various forms of security offered as services • Identify cloud impact on related technologies that rely on cloud or are commonly seen in cloud deployments
Labs	• Core account security • IAM and monitoring in-depth • Network and instance security	• Encryption and storage security • Application security and federation • Risk and provider assessment lab

Learn more at

hpe.com/ww/learnsecurity

Follow us:

Hewlett Packard Enterprise