Hewlett Packard Enterprise

Cloud Computing Security Knowledge 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?

- IDC MarketScape leader 5 years running for IT education and training*
- Recognized by IDC for leading with global coverage, unmatched technical expertise, and targeted education consulting services*
- Key partnerships with industry leaders OpenStack®, VMware®, Linux®, Microsoft®, ITIL, PMI, CSA, and SUSE
- Complete continuum of training delivery options—self-paced eLearning, custom education consulting, traditional classroom, video on-demand instruction, live virtual instructor-led with hands-on lab, dedicated onsite training
- Simplified purchase option with HPE Training Credits

*Realize Technology Value with Training, IDC Infographic 2037, Sponsored by HPE, October 2017

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 including a detailed description of cloud computing. It 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 through hands-on labs using Amazon Cloud.

This course prepares students for the Cloud Security Alliance CCSK certification exam.

Audience

- This class is geared towards 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, such as firewalls, secure development, encryption, and identity management
- For security foundations training, refer to the Information Security Essentials course at hpe.com/ww/learnsecurity

Course objectives

- To provide students with a base of knowledge on cloud computing security theory and practice and assist students in taking the CCSK exam.

Certifications and related examinations

- Cloud Security Alliance—CCSK

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: Adapting governance and information risk management	• 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	• Differentiate risk treatment implementation responsibility across service models • List key aspects of business continuity and disaster recovery planning for cloud • 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	• 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
Module 4: Infrastructure technology	• 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 5: Securing cloud infrastructure	• Discuss the security advantages and disadvantages of working with virtual infrastructure • 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 • Identify the security basics for the difference service models • Assess the security implications of different deployment models
Module 6: Data security for cloud computing	• Describe different cloud storage models • Define security issues for data in the cloud • Assess the role and effectiveness of access controls • 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 7: Cloud identity and access management	• 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 8: Developing and securing cloud applications	• 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 9: Security as a Service	• Define SECaaS • List advantages and concerns for SECaaS	• Describe various forms of security offered as services
Module 10: Vendor relationships	• 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 provider
Module 11: Create and Secure Root Account	• Reinforce your understanding of public IaaS architectures • Define core IaaS components/options – Images – Instances – Volumes • Regions, VPCs, Security Groups, and Availability Zones	• Object storage and snapshots • Lock down your root account • Create an initial super-admin user • Start initial monitoring with CloudTrail
Module 12: Identity and Access Management	• Implement in-cloud identity management and entitlements • Recognize and use the AWS IAM “primitives” • Create a service account for AWS • Describe and implement IAM roles • Create a custom IAM policy • Distinguish between user and resource based policies • Assess differences between console and API access and credentials	• Implement more-comprehensive monitoring and alerting • Recognize cloud logging architectures • Select basic alerting options • Automate event-driven security • Distinguish event from configuration logging
Module 13: Network and Instance Security	• Build and secure a network in AWS • These principles will translate to most Software Defined Networks (SDNs) and cloud providers • Learn the AWS network primitives/components • Create a VPC with public and private subnets • Distinguish between security groups work and firewalls	• Implement basic security groups • Secure your first instance • Understand the different types of images • Review the different types of instances (e.g. immutable) • Launch, secure, and connect to your first instance

Module 14: Encryption and Storage Security	• Review encryption concepts • Select an encryption method • Create and attach an encrypted Amazon EBS volume • Select key management options	• Describe snapshot security • Review your vulnerability assessment results • Run an update and initiate a second scan
Module 15: Application Security and Federation	• Understand basic cloud application architectures • Manage multiple Security Groups for enhanced network security	• Evaluate the role of server-less and PaaS in enhancing security • Integrate federated identity management using OpenID
Module 16: Risk and Provider Assessment	• Apply the fundamentals of risk assessments of cloud providers • Learn to use risk assessment tools • The Common Assessment Initiative	• The Cloud Controls Matrix • The Cloud Security Alliance Star Registry • Perform a risk assessment to choose a provider

Learn more at
hpe.com/ww/learnsecurity

Follow us:

H8P76S C.00, January 2018

Hewlett Packard
Enterprise