Hewlett Packard Enterprise

Cloud Computing Security Knowledge Plus 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.

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

Why HPE Education Services?

- IDC MarketScape leader 4 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 (ISC)²
- 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

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

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.

Hands-on is performed using the Amazon Cloud.

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 HPE Information Security Common Body of Knowledge curriculum found at **hpe.com/ww/learnsecurity**.

Certification(s)

• Cloud Security Alliance—CCSK

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.

*Realize Technology Value with Training, IDC Infographic 2037, Sponsored by HPE, January 2016

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
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 • 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	• 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: Traditional risk treatment plans	• Recognize sample security controls for data center perimeter • Describe how cloud provider employment policies affect information security
Module 5: 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 6: Securing cloud infrastructure	• 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	• 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	• 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	• 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	• Define SECaaS • List advantages and concerns for SECaaS • Describe various forms of security offered as services
Module 11: 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 providers
Module 12: Cloud risk assessment exercise-public cloud	• 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

Course data sheet

Module 13: Create and secure a public cloud instance	• Reinforce your understanding of public IaaS architectures • Define core IaaS components/options • Lock down your root account • Launch and connect to your first instance • Manage images and host keys • Secure your instance • Verify instance availability
Module 14: Encrypting a storage volume	• 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 • Install MySQL on the encrypted volume
Module 15: Create and secure a cloud application	• 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	• Secure your HPE 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

Learn more at
hpe.com/ww/learnsecurity

Follow us:

c04570175, September 2016, Rev. 4

Hewlett Packard Enterprise