

HP Education Services Course Overview

Cloud Computing: Security Threats and Measures (H9P45s)



Cloud computing is today's approach to effective IT computing systems, databases, and networks. In addition to the benefits it brings to organizations, a lot of security threats and uncertainties come along. This 2-day intensive course aims to provide attendees with practical security knowledge on cloud computing environment.

Course Objective

Upon successful completion of this course, attendees will be able to identify security risks and concerns on cloud computing environment and understand the best practices on handling cloud security issues.

Audience

This course is useful for anyone looking to expand their knowledge of cloud security

Prerequisites

We recommend attendees have basic understanding on cloud computing concept.

Course Title:	Cloud Computing: Security Threats and Measures
HP Product Number:	H9P45s
Category/Subcategory:	Cloud Computing
Course Length:	2 Days
Level:	Basic
Delivery Language:	English
To Order:	In HK, please contact HP Education Services on (852) 3070-6692 or email at hp-education.hk@hp.com or visit www.hp.com.hk/education Other countries please visit www.education.hp.com

Detail Course Outline

DAY 1 –

Cloud Computing Basics

- Review the basic concepts in cloud computing
- Characteristics of cloud computing
- Service model of cloud computing (SaaS, PaaS, IaaS)
- Cloud computing frameworks

Introduction to Cloud Computing Security

- Common Security Threats
- Common Security Threats in Cloud environment
- Various Security Aspects in Cloud Computing

Security in Cloud Computing: IaaS Scenario

- Physical Security
 - What are the security considerations in protecting the equipments when they go into the cloud?
- Network Communication Security
 - How to keep data secure when they are transmitted on network?
- Data Center Operations
 - Issues & assessments on cloud infrastructure availability, performances and service levels

Security in Cloud Computing: PaaS Scenario

- Virtualization Security
 - Security controls in the hypervisor
 - Virtualization Guest / Host Interaction Controls

DAY 2 –

Security in Cloud Computing: SaaS Scenario

- Application Security
 - How to define a secure application?
 - What are the common application security flaws?
- Information Lifecycle Management
 - How information should be created, distributed, used, maintained and disposed in cloud computing environment from service / content providers' perspective
- Encryption and Key Management
 - How encryptions help in cloud computing
 - Issues in using and distributing keys in cloud computing

- Identity and Access Management (IAM)
 - What can be done to ensure appropriate access to resources stored on cloud
 - How to assess the IAM capability of the cloud service provider?

Security in Cloud Computing: Additional Controls & Other Aspects

- File System Security
 - How are files protected on file system?
 - What are the security controls provided by common file systems
- Patch Management
 - Best practices on patch management in cloud computing
- Business Continuity and Disaster Recovery
 - What to do in case of disaster when using cloud computing?
- Legal and E-Discovery
 - Jurisdictional and contractual considerations in cloud computing

Audit, Certification and Governance in Cloud Computing Environment

- Audit Logging requirements
- Incident Response and Forensics Investigation
- Audit, certification and governance in cloud computing environment from CSA
- How to interpret SAS70 results for secure cloud computing environment
- How to achieve ISO 27001 for cloud computing environment

