

CCSP—Certified Cloud Security Professional H0DU2S

HPE course number	H0DU2S
Course length	5 Days
Delivery modes	ILT, VILT
View schedule, local pricing, and register	View now
View related courses	View now

This Official (ISC)² course provides a comprehensive review of cloud security concepts and industry best practices, covering the 6 domains of the CCSP CBK: Architectural concepts and design requirements, cloud data security, cloud platform and infrastructure security, cloud application security, operations, legal and compliance. In this course, you will find that several types of activities are used to reinforce topics and increase knowledge retention. These activities include open-ended questions from the instructor to the students, matching and poll questions, group activities, open/closed questions, and group discussions. This interactive learning technique is based on sound adult learning theories.

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

Audience

The course is designed for experienced information security professionals with at least five years of full-time IT experience, including three years of information security and at least one year of cloud security experience. The CCSP credential can be appropriate for mid-level to advanced professionals involved with IT architecture Web and cloud security engineering, information security, governance, risk and compliance, and even IT auditing. This course builds on and brings together the holistic view of the topics covered in the everyday environment of an information assurance professional.

concepts with regard to customer, provider, partner, measured services, scalability, virtualization, storage, and networking. Students will also be able to understand the cloud reference architecture based on activities defined by industry standard documents.

- Identify the types of controls necessary to administer various levels of confidentiality, integrity, and availability, with regard to securing data in the cloud. You will gain knowledge on topics of data discovery and classification techniques, digital rights management, privacy of data, data retention. Deletion and archiving, data event logging, chain of custody and non-repudiation, and the strategic use of security information and event management.

Course objectives

After completing this workshop, participants will be able to:

- Describe the building blocks necessary to develop cloud-based systems, including

- Identify the virtual and physical components of the cloud infrastructure with regard to risk management analysis, including tools and techniques necessary for maintaining a secure cloud infrastructure. In addition to risk analysis, you will gain an understanding in how to prepare and maintain business continuity and disaster recovery plans, including techniques and concepts for identifying critical systems, and lost data recovery.
- Demonstrate an understanding of the Software Development Life Cycle, you will gain an understanding in cloud software assurance and validation, utilizing secure software, and the controls necessary for developing secure cloud environments with regard to program interfaces, cloud application architecture, and how to ensure data and application integrity, confidentiality, and availability through identity and access management solutions.
- Demonstrate an ability to develop, plan, implement, run, and manage the physical and logical cloud infrastructure through an understanding of the necessary controls and resources, best practices in monitoring and auditing, and the importance of risk assessment in both the physical and logical cloud infrastructures.
- Identify privacy issues and audit processes utilized within a cloud environment, including, auditing controls, assurance issues, and the specific reporting attributes. Topics covered include: ethical behavior and required compliance within regulatory frameworks, which includes investigative techniques for crime analysis and evidence gathering methods.

Benefits to you

- This training course will help candidates review and refresh their cloud security knowledge and help identify areas they need to study for the CCSP exam and features.
- Official (ISC)² courseware.
- Taught by an authorized (ISC)² instructor.
- Student handbook.
- Collaboration with classmates.
- Real-world learning activities and scenarios.

Detailed course outline

Domain 1: Architectural concepts and design Requirements—Cloud computing concepts and definitions based on the ISO/IEC 17788 standard: Security concepts and principles relevant to secure cloud computing.

- Understand cloud computing concepts
- Describe cloud reference architecture
- Understand security concepts relevant to cloud computing
- Understand design principles of secure cloud computing
- Identify trusted cloud services

Domain 2: Cloud data security—Concepts, principles, structures, and standards used to design, implement, monitor, and secure operating systems, equipment, networks, applications, and those controls used to enforce various levels of confidentiality, integrity, and availability in cloud environments.

- Understand cloud data lifecycle
- Design and implement cloud data storage architectures
- Design and apply data security strategies
- Understand and implement data discovery and classification technologies
- Design and implement data rights management
- Design and implement relevant jurisdictional data protections for Personally Identifiable Information (PII)
- Plan and implement data retention, deletion, and archiving policies
- Design and implement auditability, traceability, and accountability of data events

Domain 3: Cloud platform and infrastructure security—Knowledge of the cloud infrastructure components, both the physical and virtual, existing threats, and mitigating and developing plans to deal with those threats.

- Comprehend cloud infrastructure components
- Analyze risks associated to cloud infrastructure
- Design and plan security controls
- Plan disaster recovery and business continuity management

Domain 4: Cloud application security—Processes involved with cloud software assurance and validation; and the use of verified secure software.

- Recognize the need for training and awareness in application security
- Understand cloud software assurance and validation
- Use verified secure software
- Comprehend the Software Development Life Cycle (SDLC) process
- Apply the secure Software Development Life Cycle
- Comprehend the specifics of cloud application architecture
- Design appropriate Identity and Access Management (IAM) solutions

Domain 5: Operations—Identifying critical information and the execution of selected measures that eliminate or reduce adversary exploitation of it; requirements of cloud architecture to running and managing that infrastructure; definition of controls over hardware, media, and the operators with access privileges as well as the auditing and monitoring are the mechanisms, tools and facilities.

- Support the planning process for the data center design
- Implement and build physical infrastructure for cloud environment
- Run physical infrastructure for cloud environment
- Manage physical infrastructure for cloud environment
- Build logical infrastructure for cloud environment
- Run logical infrastructure for cloud environment
- Manage logical infrastructure for cloud environment
- Ensure compliance with regulations and controls (e.g., ITIL, ISO/IEC 20000-1)
- Conduct risk assessment to logical and physical infrastructure
- Understand the collection, acquisition, and preservation of digital evidence
- Manage communication with relevant parties

Domain 6: Legal and Compliance—Addresses ethical behavior and compliance with regulatory frameworks. Includes investigative measures and techniques; gathering evidence (e.g., legal controls, eDiscovery, and forensics); privacy issues and audit processes and methodologies; implications of cloud environments in relation to enterprise risk management.

- Understand legal requirements and unique risks within the cloud environment
- Understand privacy issues, including jurisdictional variation
- Understand audit process, methodologies, and required adaptations for a cloud environment
- Understand implications of cloud to enterprise risk management
- Understand outsourcing and cloud contract design
- Execute vendor management

Learn more at
hpe.com/ww/learnsecurity

Follow us:



© Copyright 2015–2016 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries. The OpenStack Word Mark is either a registered trademark/service mark or trademark/service mark of the OpenStack Foundation, in the United States and other countries and is used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation or the OpenStack community. Pivotal and Cloud Foundry are trademarks and/or registered trademarks of Pivotal Software, Inc. in the United States and/or other countries. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other third-party trademark(s) is/are the property of their respective owner(s).