

Brochure

# CCSK and CCSP Equal highest standard for Cloud Security Expertise

Education Services—Security in knowledge



**Hewlett Packard**  
Enterprise

The cloud is a powerful vehicle that enables you to consume or deliver highly scalable, technology-enabled services over the Internet. With security a top concern for organizations wanting to adopt cloud services, learning what you need to know about security in the cloud is critical for success. HPE is pleased to offer two industry leading cloud security certification programs including the Certificate of Cloud Security Knowledge (CCSK) by the Cloud Security Alliance (CSA) and the Certified Cloud Security Professional (CCSP) by (ISC)<sup>2</sup>

### **Cloud Security Alliance (CSA) Master Training Program**

#### **Program to accelerate worldwide access and adoption of Certificate of Cloud Security Knowledge (CCSK) Certification**

As the Master Training Partner (MTP) for the Cloud Security Alliance, HPE is committed to providing leading-edge cloud education and solutions to keep pace with the constantly changing landscape.

### **How to reduce the risk of your cloud-based services**

The promise of the cloud is appealing: reduced costs, greater agility, flexibility, scalability, and potentially greater security. At the same time, IT organizations recognize that the cloud introduces a number of issues related to security, data integrity, compliance, service level agreements, and data architecture that must be addressed. Therefore, the adoption of cloud services is being tempered by a significant level of uncertainty. Numerous surveys indicate that the top concerns for moving to the cloud are: 1) security, 2) data loss, and 3) loss of control. In other words, enterprises are looking for assurances that they are not adding risk to the business by leveraging the cloud. For many, moving to the cloud is still a leap of faith.

“Working with HPE, a company who shares a strong commitment to providing leading edge cloud education and solutions, this is another step forward in our mission to deliver the best practices for security assurance within cloud computing.”

-Jim Reavis, CEO of the CSA

### Who are CCSKs

CCSK is beneficial to many IT and security professionals and those that have earned a CCSK come from a variety of backgrounds as follows:

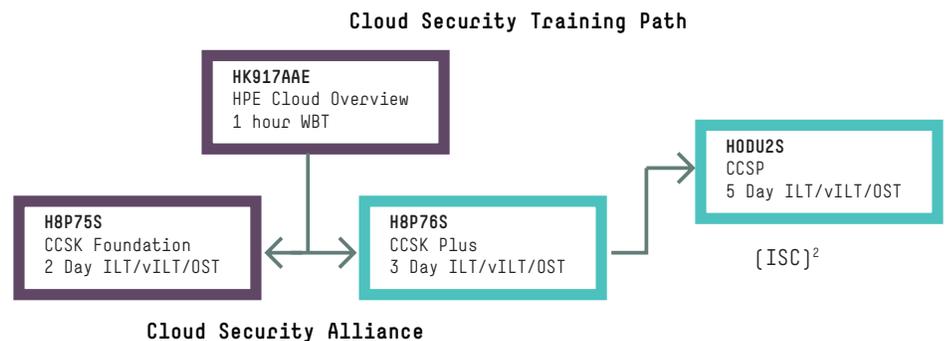
- **Cloud providers and information security services firms** wish to demonstrate expertise in cloud as a competitive advantage, and have therefore encouraged their employees to earn the CCSK.
- **All Third Party Assessment Organizations (3PAOs)** within US Government’s FedRamp program have CCSKs on staff because they need an objective, consistent level of cloud security knowledge and mastery of good practices.
- **Cloud customers** are faced with an increasing number of providers and services, and corresponding risks and benefits. Enterprise users who engage with many different cloud providers find CCSK especially helpful in establishing a baseline of security best practices as they deal with broad array of cloud computing, they can grow their business by demonstrating, through a globally recognized credential, special knowledge of the cloud and cloud-specific security assurance.
- **Individuals and firms that provide audit, attestation or certification services** know that, as more and more systems are migrated to cloud computing they can grow their business by demonstrating through a globally recognized credential, special knowledge of the cloud and cloud-specific security assurance.

### CCSK—your ticket to a better career and help to provide a more secure cloud

CCSK training can equip you and your team with the latest guidance from the CSA on security fundamentals, threats and best practices, designed to help secure the cloud.

The CCSK certification training has already helped thousands of IT and security professionals with responsibility related to cloud computing and delivers:

- The ability to demonstrate your technical knowledge, skills, and to effectively develop a holistic cloud security program relative to globally accepted standards.
- Differentiate yourself from other candidates in the fast growing cloud security market
- Includes 14 domains from the latest CSA Guidance document, the CSA Cloud Controls Matrix (CCM) and recommendations from the European Network and Information Security Agency (ENISA)
- Prepares security professionals for Certificate of Cloud Security Knowledge (CCSK) Certification
- Advanced training includes extensive hands-on activity created to apply knowledge and bring a fictional organization more securely to the cloud
- Retire one year of field experience required to achieve CCSP by (ISC)<sup>2</sup>



## CCSK guidance

Cloud architecture
Governance and enterprise
Legal and electronic discovery
Compliance and audit
Information lifecycle management
Portability and interoperability
Traditional security, Business Continuity Management, and Disaster Recovery
Data center operations
Incident response
Application security
Encryption and key management
Identity and access management
Virtualization
Security-as-a-Service
ENISA document

We recommend that 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 training at [hpe.com/ww/learnsecurity](https://hpe.com/ww/learnsecurity).

## Complement your knowledge investments

You may wonder how CCSK relates to certifications and education you have already received. CCSK early adopters have multiple certifications and we have been able to discuss the synergy with CCSK holders who also have achieved other certifications. CSA is committed to working with key user certification organizations to make sure that the CCSK aligns with other industry certifications.

One of the most widely sought user accreditations is the Certified Information Systems Auditor®, from ISACA®. The CISA is considered the gold standard for information technology audit, and is sought by professionals with related job duties. CISAs have shared that CCSK provides the necessary context and focus to successfully audit cloud environments. The more knowledge one has about how clouds work and how they can be secured, the easier it is to identify the appropriate measures to test control objectives and make recommendations for IT systems that one will rarely touch and see.

Among the most common certification we see held by CCSKs is the Certified Information Systems Security Professional® (CISSP) from (ISC)²®. CISSP holders indicate that the CISSP background has been very useful in helping them study for and pass the CCSK. The CISSP Body of Knowledge consists of 8 domains, while CCSK has 14. All of the CISSP domains have an analog in the CCSK. Where CCSK and CISSP have the same domain, the CCSK builds upon the CISSP domain and provides context that is important to cloud.

For more information complementing your knowledge investments, please visit [cloudsecurityalliance.org/education/ccsk/#\\_about](https://cloudsecurityalliance.org/education/ccsk/#_about)

“CISOs have been demanding a paradigm shift in how we train security practitioners for the challenges their businesses face now and in the near future. The choice between certification-focused boot camps and a four-year degree is not what they need. They need reality-based training that they can take back to work and start implementing immediately to make their business more secure now and that is just what HPE delivers.”

-Cathy Pitt, Distinguished Technologist

## NEXT Step: Certified Cloud Security Professional (CCSP)

Backed by the two leading non-profits focused on cloud and information security, CSA and (ISC)<sup>2</sup>, the CCSP credential denotes professionals with deep-seated knowledge and competency derived from hands-on experience with cyber, information, software and cloud computing infrastructure security. CCSPs help you achieve the highest standard for cloud security expertise and enable your organization to benefit from the power of cloud computing while keeping sensitive data secure.

CCSP provides the next step after achieving CCSK to continue expanding your knowledge in cloud security and cloud security best practices.

Where CCSK includes 14 knowledge domains, the CCSP provides expanded knowledge across the six domains below:

- Architectural Concepts and Design Requirements
- Cloud Data Security
- Cloud Platform and Infrastructure Security
- Cloud Application Security
- Operations
- Legal and Compliance

Like CCSK, the CCSP is beneficial to many IT and security professionals including

- Enterprise Architect
- Security Administrator
- Systems Engineer
- Security Architect
- Security Consultant
- Security Engineer
- Security Manager
- Systems Architect

## CCSP Requirements

To qualify for the CCSP, you must have a minimum of five years of cumulative paid full-time information technology work experience, of which three years must be in information security and one year in one of the six domains listed previously. Earning the CCSK can be substituted for the one year of experience in one of the six domains. Earning (ISC)<sup>2</sup> CISSP credential can be substituted for the entire CCSP experience requirement.

Candidates that don't meet the minimum requirements for CCSP may earn the Associate of CCSP.

Learn more at  
[hpe.com/ww/learnsecurity](http://hpe.com/ww/learnsecurity)



Sign up for updates

★ Rate this document



© 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.

Certified Information Systems Auditor™, from ISACA® are registered trademarks of ISACA in the US and other countries. (ISC)<sup>2</sup> and CISSP are registered trademarks of (ISC)<sup>2</sup>, Inc.

4AA5-8201ENW, May 2016, Rev. 1