

Certificate of Cloud Security Knowledge (CCSK™)

Seldom has a technology offered more opportunity and more risk than the cloud. Let the marketplace know you are ready for the challenge with the first credential dedicated to cloud security, offered by the world's thought leader in cloud security.

This is the mother of all cloud computing security certifications. The Certificate of Cloud Security Knowledge certification is vendor-neutral and certifies competency in key cloud security areas.

—CIO.com, Top Ten Cloud Computing Certifications



Certificate of Cloud Security Knowledge (CCSK™)

It took a special group of people to perceive from the start the likely impact cloud would have on computing. Those same early adopters recognize that the degree of potential risk and reward attached to the cloud calls for a deep understanding of cloud-related security and assurance issues.

They know there is an advantage to differentiating themselves from other professionals by master leading- edge thought in this growing field and having an objective, third-party credential reflecting their expertise. And they are taking action, by earning the CCSK from the CSA.

The professionals who have earned a CCSK come from a variety of backgrounds and have pursued their cloud certificate for several reasons:

- 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 from its inception. Being able to state that their employees hold the CCSK allows their potential clients to rest easy, knowing that the necessary skills will be brought to bear on their project.
- All Third-Party Assessment Organizations (3PAOs) within the 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 responsibilities, which may range from cloud governance to configuring technical security controls.
- 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.

What is CCSK?

The CCSK is a credential verifying successful completion of an exam that tests a broad foundation of knowledge about cloud security.

Here are a few "fast facts":

- **Content:** 14 domains, covering topics such as architecture, governance, compliance, operations, encryption and virtualization
- **Body of knowledge:** CSA's "Security Guidance for Critical Areas of Focus in Cloud Computing V4.0" (English language version), the CSA Cloud Controls Matrix (CCM) and the ENISA report, "Cloud Computing: Benefits, Risks and Recommendations for Information Security"
- **Exam:** Taken online, completed in 90 minutes. 60 multiple-choice questions selected randomly from the CCSK question pool; passing score—80%
- **CPEs:** The CCSK can be used to satisfy continuing professional education credits for several other IT credentials.

CCSK is a requirement for any auditor providing services for CSA STAR Attestation, CSA's cloud provider assessment specification co-developed with the American Institute of Certified Public Accountants (AICPA).

Preparing for the Exam:

CSA's Self-Paced Training Course prepares you to earn your certificate with lessons that can be completed on-the-go, at home, wherever you go.



Class Options

CCSK Foundation

Provides students a comprehensive, one-day review of cloud security fundamentals and the certificate's body of knowledge and prepares them to take the CCSK exam.



Introduction to Cloud Computing:

This module covers the fundamentals of cloud computing, including definitions, architectures, and the role of virtualization. Key topics include cloud computing service models, delivery models, and fundamental characteristics. It also introduces the Shared Responsibilities Model and a framework for approaching cloud security.



Infrastructure Security for Cloud Computing:

This module digs into the details of securing the core infrastructure for cloud computing- including cloud components, networks, management interfaces, and administrator credentials. It delves into virtual networking and workload security, including the basics of containers and serverless.



Managing Cloud Security and Risk:

This module covers important considerations for managing security for cloud computing. It begins with risk assessment and governance, then covers legal and compliance issues, such as discovery requirements in the cloud. It also covers important CSA risk tools including the CAIQ, CCM, and STAR registry.



Data Security for Cloud Computing:

One of the biggest issues in cloud security is protecting data. This module covers information lifecycle management for the cloud and how to apply security controls, with an emphasis on public cloud. Topics include the Data Security Lifecycle, cloud storage models, data security issues with different delivery models, and managing encryption in and for the cloud, including customer managed keys (BYOK).



Application Security and Identity Management for Cloud Computing:

This module covers identity management and application security for cloud deployments. Topics include federated identity and different IAM applications, secure development, and managing application security in and for the cloud.



Cloud Security Operations:

This module covers key considerations when evaluating, selecting, and managing cloud computing providers. We also discuss the role of Security as a Service providers and the impact of cloud on Incident Response.

CCSK Plus

Builds on the CCSK Foundation class with a second day of training that covers expanded material and offers extensive hands-on activities that reinforce classroom instruction. Students engage in a scenario of bringing a fictional organization securely into the cloud, which gives them the opportunity to apply their knowledge by performing a series of activities that would be required in a real-world environment. CCSK Foundation Modules included.



- **Core Account Security.** Students learn what to configure in the first 5 minutes of opening a new cloud account and enable security controls such as MFA, basic monitoring, and IAM.
- **IAM and Monitoring In-Depth.** Attendees expand their work on the first lab and implement more-complex identity management and monitoring. This includes expanding IAM with Attribute Based Access Controls, implementing security alerting, and understanding how to structure enterprise-scale IAM and monitoring.
- **Network and Instance Security.** Students create a virtual network (VPC) and implement a baseline security configuration. They also learn how to securely select and launch a virtual machine (instance), run a vulnerability assessment in the cloud, and connect to the instance.

- **Encryption and Storage Security:** Students expand their deployment by adding a storage volume encrypted with a customer managed key. They also learn how to secure snapshots and other data.
- **Application Security and Federation.** Students finish the technical labs by completely building out a 2-tier application and implementing federated identity using OpenID.
- **Risk and Provider Assessment.** Students use the CSA CCM and STAR registry to evaluate risk and select a cloud provider.

These courses are available via CSA's training partner network. Some trainers can provide distance learning options or onsite training to make the learning experience as convenient as possible.

Choose the Right Class-Format for You

Self-Paced Training is a good fit if you...

- Can't travel due to budget restrictions
- Have a complicated schedule and can't fit in a regular class.
- Are paying for your training out-of-pocket.
- Want to invest in multiple complementary certifications.
- Need a course that can be completed on-the-go, at home, work, wherever you go..
- Want a learning experience customized to you.
- Want online training that's based on research from subject matter experts out in the field.

Instructor-Led Online is good fit if you...

- Require one-to-one interaction.
- Can't travel due to budget restrictions.
- Like a class to help motivate you to keep up.

In-Person Training is best if....

- You ask lots of questions.
- You learn best through face-to-face interactions.
- Your company has the training budget to pay for you to travel.

Navigating the Certification Ecosystem

For those holding ISACA's Certified Information Systems Auditor® (CISA®) designation, better understanding of how clouds work and how they can be secured makes it easier to identify the appropriate measures to test control objectives and make appropriate recommendations.

Holders of the Certified Information Systems Security Professional® (CISSP®) from (ISC)2® benefit from the alignment between the bodies of knowledge of the two credentials. All CISSP's 10 domains have an analog in CCSK's 14 domains; where the domains overlap, CCSK builds on the CISSP domain and provides cloud-specific context.

About CSA

The Cloud Security Alliance is the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. CSA harnesses the subject matter expertise of industry practitioners, associations, governments, and its corporate and individual members to offer cloud security-specific research, education, certification, events and products. CSA's activities, knowledge and extensive network benefit the entire community impacted by cloud—from providers and customers, to governments, entrepreneurs and the assurance industry—and provide a forum through which diverse parties can work together to create and maintain a trusted cloud ecosystem.

Cloud Security Alliance
www.cloudsecurityalliance.org
info@cloudsecurityalliance.org

