CERTIFICATE OF CLOUD SECURITY KNOWLEDGE +

(V4.0) By Cloud Security Alliance (CSA)

CCSK™
Certificate of
Cloud Security Knowledge

OVERVIEW

As enterprises and consumers move greater amounts of sensitive information to the cloud, employers struggle to find information security leaders who have the necessary breadth and depth of knowledge to establish cloud security programs protecting sensitive information.

The CCSK is intended to provide understanding of security issues and best practices over a broad range of cloud computing domains. As cloud computing is becoming the dominant information technology system, CCSK is applicable to a wide variety of Information technology and information security jobs in virtually every organization.

CCSK helps you to validate your competence gained through experience in cloud security and demonstrate your technical knowledge, skills, and abilities to effectively develop a holistic cloud security program relative to globally accepted standards.

CCSK helps the organization protect against threats with qualified professionals who have the expertise to competently design, build, and maintain a secure cloud business environment. Increase organization confidence that candidates are qualified and committed to cloud security. Ensure practitioners use a universal language, circumventing ambiguity with industry-accepted cloud security terms and practices lastly increase organizations' credibility when working with constituents.

COURSE : **CSA-CCSK+ | Instructor-Led**

DURATION : **3 days**

LEARNING OBJECTIVES

- Validate competency and experience in cloud security
- Demonstrate technical knowledge, skills, and abilities in developing a holistic cloud security program relative to globally accepted standards
- Gain access to tools, networking and idea exchange with peers
- Protect against threats with qualified professionals who have the expertise to competently design, build, and maintain a secure cloud business environment
- Ensure use of universal language, circumventing ambiguity with industry-accepted cloud security terms and practice.

PREREQUISITES

- N/A

AUDIENCE

- Auditor wanting to perform and lead CSA Security, Trust & Assurance Registry (STAR) program audits
- Project manager or consultant wanting to master the CSA START program requirements
- Person responsible for the Information security in an organization
- Member of the information security team
- Expert advisor in information technology

COURSE OUTLINE

Module 1: Intro to Cloud Computing

- NST Definitions
- Essential characteristics
- Service models
- Deployment models

Objectives

1. Define cloud computing and why you care about it.
2. Discuss the different components of the cloud computing stack.
3. Work through the cloud reference models and understand where security fits in.

Module 2: Infrastructure Security for Cloud

- Securing base infrastructure
- Management plane security
- Securing virtual hosts and networks
- IaaS, PaaS, SaaS security

Objectives

1. Understand the components of cloud infrastructure.
2. Assess the security implications of virtual networks and workloads.
3. Learn the security advantages and disadvantages of working with cloud infrastructure.
4. Evaluate how to secure the cloud management plane.
5. Learn how to manage business continuity for cloud computing.

Module 3: Managing Cloud Security Risk

- Risk & governance
- Legal & compliance
- Audit
- Data governance

Objectives

1. Governance & Risk
   - Tools of governance
   - Adjusting risk management for cloud computing
2. Legal
   - Jurisdictions, Contracts, eDiscovery
3. Compliance & Audit
   - Compliance and compliance inheritance
   - Audit management for cloud
4. Information Governance
   - Covered in the Data Security Domain
5. Introduction to the CC, and CAIQ

COURSE OUTLINE

Module 4: Data Security for Cloud Computing

- Cloud data architectures
- Data security & encryption
- CASB and data loss prevention
- BC/DR

Objectives

1. Understand different cloud storage models.
2. Define security issues for data in the cloud.
3. Access the role and effectiveness of access controls.
4. Learn different cloud encryption models.
5. Understand additional data security options.
6. Introduce data security lifecycle.

Module 5: Securing Cloud Applications, Users & Related Technologies

- Application security
- Identity and access management
- Related technologies

Objectives

1. Discover how application security differs in cloud computing.
2. Review secure software development basics and how those change in the cloud.
3. Leverage cloud capabilities for more secure cloud applications.

Module 6: Cloud Security Operations

- What to look for in a cloud provider
- Security as a service
- Incident response

Objectives

1. Learn how to select cloud providers.
2. Understand the advantages & disadvantages of Security as a Service.
3. Access the different major Security as a Service categories.
4. Learn how to respond to security incidents in the cloud.
5. Understand the security issues of technologies related to cloud computing: Big Data, Mobile, Serverless, IoT.

LAD Handbook

Exercise 1: Core Account Security

- Understand public IaaS architectures
- Review EC2 components/options
  - Images
  - Instances
  - Volumes
  - Regions, VPCs, Security Groups, and Availability Zones
- Lock down your root account
- Create an initial super-admin user
- Start initial monitoring with CloudTrail

Exercise 2: IAM & Monitoring

- Learn how in-cloud identity management and entitlements work
  - Understand the AWS IAM “primitives”
  - Create service accounts for AWS
  - Understand IAM roles
  - Create custom IAM policies
  - Learn the differences between console and API access and credentials
- Implement more-comprehensive monitoring and alerting.
  - Review cloud logging architectures lagging
  - Understand basic alerting options
  - Introduction to event-driven security automation
  - Learn the difference between event and configuration

Exercise 3: Network & Instance Security

- Learn how to build and secure a network in AWS
  - These principles will translate to most Software Defined Networks (SDNs) and cloud providers
  - Learn the AWS network primitives/components
  - Create a VPC with public and private subnets
  - Understand how security groups work and how they differ from firewalls
  - Implement basic security groups
- Secure your first instance
  - Understand the different types of images
  - Review the different types of instances
  - (e.g immutable)
  - Launch, secure, and connect your first instance

LAD Handbook

Exercise 4: Encryption and Storage Securityt

- Why encrypt?
- Select an encryption method
- Create and attach an encrypted Amazon EBS volume
- Understand key management options
- Understand snapshot security
- Review your vulnerability assessment results
- Run an update, initiate a second scan. Compare results obtained.

Exercise 5: Application Security & Federation

- Understand basic cloud application architectures
- Manage multiple Security Groups for enhanced network
- Evaluate the role of server-less and PasS in enhancing Security
- Integrate federated identity management using OpenID

Exercise 6: Risk & Provider Assessment Lab

- Understand the fundamentals of risk assessment of cloud providers

- Learn to use risk assessment tools:
  - The Common Assessment Initiative
  - The Cloud Controls Matrix
  - The Cloud Security Alliance Star Registry

- Perform a risk assessment to choose a provider

General Information

- The certification/exam fees are bundled with the training fees
- Participant Handbook: 124 pages
- Lab Handbook: 162 pages

CCSK Examination

The CCSK is an examination testing for a broad foundation of knowledge about cloud security, with topics ranging from architecture, governance, compliance, operations, encryption, virtualization and much more.

- 60 MCQs
- Duration: 90 minutes
- Passing score: 80%

CCSK exam tokens are valid for 2 years from the date of training. Exam token are valid for 2 attempts. If you fail the second time, then you will need to purchase another token at $395 USD.

Once you are a CCSK holder you are always a CCSK holder. There are no maintenance fees or obligations.

For details regarding the exam, including hardware and software requirements, download the complimentary Exam Guide:
https://cloudsecurityalliance.org/education/ccsk/#_prepare

Normal Price: RM8,699.00
Early Bird Price: RM8,299.00

CLICK TO REGISTER

*Limited Seats Available

For more information, kindly contact us at:

LGMS | LE Global Services Sdn Bhd
A-11-01, Empire Office Tower
Jalan SS 16/1,
47500 Subang Jaya
Selangor, Malaysia

+603-8605 0155
training@lgms.global
www.lgms.global