Cloud Security Alliance (CSA) Certificate of Cloud Security Knowledge (CCSK) v4 Preparation Guide

A Self-Study Guide to Preparing for the CCSK v4 Exam

Welcome to the Certificate of Cloud Security Knowledge (CCSK), the industry's first user certification for secure cloud computing. The CCSK is designed to ensure that a broad range of professionals with a responsibility related to cloud computing have a demonstrated awareness of the security threats and best practices for securing the cloud.

Basic Facts about the CCSK Examination

The CCSK examination is a timed, multiple choice examination located at https://ccsk.cloudsecurityalliance.org/. The examination consists of 60 multiple choice questions, and must be completed within 90 minutes. A participant must correctly answer 80% of the questions to receive a passing score.

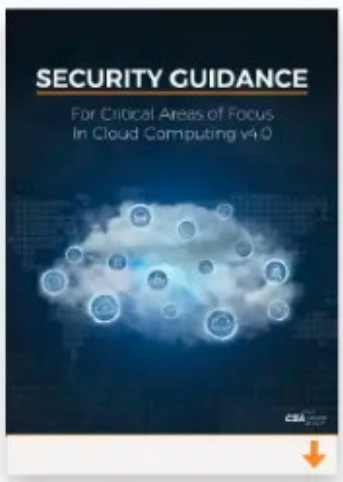
It is not possible to pause or stop the examination and finish it at a later date. Therefore, the participant should be properly prepared to take the test before starting, and while you can choose to take the test any time of the day or night, one should budget for 90 minutes of uninterrupted time once you make the commitment to start the test.

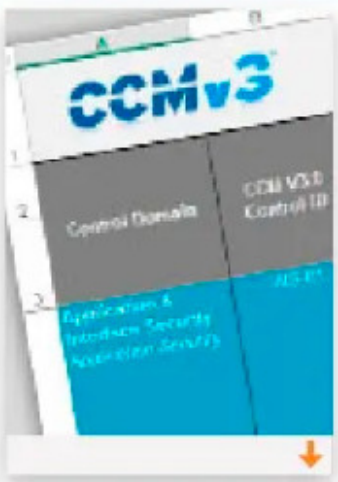
If you have any problems with the test itself, or other extenuating circumstances such as network outages that inhibit your ability to complete the test, please contact CCSK Test Support at ccsk-admin@cloudsecurityalliance.org

Studying for the CCSK Examination

The body of knowledge for the CCSK examination is the CSA Security Guidance for Critical Areas of Focus in Cloud Computing v4, English language version, the ENISA report "Cloud Computing: Benefits, Risks and Recommendations for Information Security"

These research documents can be downloaded here*





87% of the questions are based on the CSA Guidance v4, 7% on the CSA's CCM 3.0.1 and 6% of the questions are based on the ENISA report. The very best way to prepare for the CCSK examination is to thoroughly read and understand these three documents.

CCSK Key Examination Concepts

CSA Guidance For Critical Areas of Focus in Cloud Computing V 4.0 English

Domain 1 Cloud Computing Concepts and Architectures

- Definitions of Cloud Computing
  - Service Models
  - Deployment Models
  - Reference and Architecture Models
  - Logical Model
- Cloud Security Scope, Responsibilities, and Models
- Areas of Critical Focus in Cloud Security

Domain 2: Governance and Enterprise Risk Management

- Tools of Cloud Governance
- Enterprise Risk Management in the Cloud
- Effects of various Service and Deployment Models
- Cloud Risk Trade-offs and Tools

Domain 3: Legal Issues, Contracts and Electronic Discovery

- Legal Frameworks Governing Data Protection and Privacy
  - Cross-Border Data Transfer
  - Regional Considerations
- Contracts and Provider Selection
  - Contracts
  - Due Diligence
  - Third-Party Audits and Attestations
- Electronic Discovery
  - Data Custody
  - Data Preservation
  - Data Collection
  - Response to a Subpoena or Search Warrant

Domain 4: Compliance and Audit Management

- Compliance in the Cloud
  - Compliance impact on cloud contracts
  - Compliance scope
  - Compliance analysis requirements

- Audit Management in the Cloud
  - Right to audit
  - Audit scope
  - Auditor requirements

Domain 5: Information Governance

- Governance Domains
- Six phases of the Data Security Lifecycle and their key elements
- Data Security Functions, Actors and Controls

Domain 6: Management Plane and Business Continuity

- Business Continuity and Disaster Recovery in the Cloud
- Architect for Failure
- Management Plane Security

Domain 7: Infrastructure Security

- Cloud Network Virtualization
- Security Changes With Cloud Networking
- Challenges of Virtual Appliances
- SDN Security Benefits
- Micro-segmentation and the Software Defined Perimeter
- Hybrid Cloud Considerations
- Cloud Compute and Workload Security

Domain 8: Virtualization and Containers

- Mayor Virtualizations Categories
- Network
- Storage
- Containers

Domain 9: Incident Response

- Incident Response Lifecycle
- How the Cloud Impacts IR

Domain 10: Application Security

- Opportunities and Challenges
- Secure Software Development Lifecycle
- How Cloud Impacts Application Design and Architectures

- The Rise and Role of DevOps

Domain 11: Data Security and Encryption

- Data Security Controls
- Cloud Data Storage Types
- Managing Data Migrations to the Cloud
- Securing Data in the Cloud

Domain 12: Identity, Entitlement, and Access Management

- IAM Standards for Cloud Computing
- Managing Users and Identities
- Authentication and Credentials
- Entitlement and Access Management

Domain 13: Security as a Service

- Potential Benefits and Concerns of SecaaS
- Major Categories of Security as a Service Offerings

Domain 14: Related Technologies

- Big Data
- Internet of Things
- Mobile
- Serverless Computing

ENISA Cloud Computing: Benefits, Risks and Recommendations for Information Security

- Isolation failure
- Economic Denial of Service
- Licensing Risks
- VM hopping
- Five key legal issues common across all scenarios
- Top security risks in ENISA research
- OVF
- Underlying vulnerability in Loss of Governance
- User provisioning vulnerability
- Risk concerns of a cloud provider being acquired
- Security benefits of cloud

- Risks R.1 – R.35 and underlying vulnerabilities
- Data controller versus data processor definitions
- In Infrastructure as a Service (IaaS), who is responsible for guest systems monitoring

Cloud Security Alliance - Cloud Controls Matrix

- CCM Domains
- CCM Controls
- Architectural Relevance
- Delivery Model Applicability
- Scope Applicability
- Mapped Standards and Frameworks

If you do not pass the test... Test participants will receive two opportunities to pass the test. While you may take your second attempt as soon as you wish, we highly recommend studying the source material again prior to taking the test. Because of question randomization, you may see a very different exam with mostly different questions.

If you are interested in a more structured learning experience, we highly recommend the CCSK & CCM Training courses.. As with any IT certification, formal training is an excellent way to improve your chance of successfully passing the exam, sharing real-world experiences with your peers and getting cloud systems hands-on to apply the best practices.

*Resources Links

CSA Guidance: https://cloudsecurityalliance.org/download/security-guidance-v4/
Cloud Controls Matrix: https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/
ENISA: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment
CCSK Training Schedule: https://cloudsecurityalliance.org/education/#_ccsk