Preparing to take the Certificate of Cloud Security Knowledge (CCSK)

A Cloud Security Alliance Guide

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 50 multiple choice questions, and must be completed within 60 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 60 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

More general information about the CCSK is available at http://cloudsecurityalliance.org/ccsk_faq.html

The CCSK homepage is http://cloudsecurityalliance.org/certifyme.html

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 V2.1, English language version, and the ENISA report “Cloud Computing: Benefits, Risks and Recommendations for Information Security”. These research documents can be downloaded here:


70% of the questions are based on the CSA Guidance, 20% of the questions are based on the ENISA report and 10% of the questions are applied knowledge questions related to the best practices in both documents. The very best way to prepare for the CCSK examination is to thoroughly read and understand these two documents.
CCSK Key Examination Concepts

CSA Guidance For Critical Areas of Focus in Cloud Computing V2.1 English

Domain 1
NIST Definition of Cloud Computing (Essential Characteristics, Cloud Service Models, Cloud Deployment Models)
Multi-Tenancy
Cloud Reference Model
Jericho Cloud Cube Model
Cloud Security Reference Model
Cloud Service Brokers

Domain 2
Contractual Security Requirements
Enterprise and Information Risk Management
Third Party Management Recommendations

Domain 3
Cloud versus outsourcing
Three dimensions of legal issues
Contract enforceability
eDiscovery considerations
Jurisdictions and data locations

Domain 4
Compliance impact on cloud contracts
SAS 70 Type II
ISO 27001/27002
Compliance analysis requirements
Auditor requirements

Domain 5
Six phases of the Data Security Lifecycle and their key elements
Data Remanence
Data Commingling
Data Backup
Data Discovery
Data Aggregation

Domain 6
Key Portability Objectives of S-P-I
Lock-In risk mitigation techniques by cloud delivery model

Domain 7
Insider Abuse
Business Continuity Management/Disaster Recovery due diligence
Provider employee considerations

Domain 8
Provider selection
Resource sharing
Patch management
Technical support

Domain 9
Recommended provider tools and capabilities
Response tradeoffs
Questionable provider offerings

Domain 10
SDLC impact and implications
Differences in S-P-I models

Domain 11
Key management best practices
Key management standards
Encryption practices in S-P-I models

Domain 12
Identity Federation
Authorization
Access Control
Provisioning

Domain 13
Virtual Machine security features
VM attack surfaces
Compartmentalization of VMs

ENISA Cloud Computing: Benefits, Risks and Recommendations for Information Security
Security
Security benefits of cloud
Risks R.1 – R.35 and underlying vulnerabilities
Information assurance framework
Division of liabilities
Key legal issues

Applied Knowledge
Classify popular cloud providers into S-P-I model
Redundancy
Securing popular cloud services
Vulnerability assessment considerations
Practical encryption use cases

If you do not pass the test…

In 2010, participants will receive two opportunities to pass the test for each testing token they purchase. If this is the case, we recommend that you do not immediately retake the examination, but instead take several days to re-read the source material as many of the questions will likely stand out on a second reading.