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 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 V3, English language version, and the ENISA report "Cloud Computing: Benefits, Risks and Recommendations for Information Security". These research documents can be downloaded here:

CSA Guidance: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf
ENISA: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

92% of the questions are based on the CSA Guidance and 8% 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 two documents.

CCSK Key Examination Concepts

CSA Guidance For Critical Areas of Focus in Cloud Computing V3.0 English

Domain 1 Architecture

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

- Service Level Agreements

Domain 2: Governance and Enterprise Risk Management
- Contractual Security Requirements
- Enterprise and Information Risk Management
- Third Party Management Recommendations
- Supply chain examination
- Use of Cost Savings for Cloud

Domain 3: Legal Issues: Contracts and Electronic Discovery
- Consideration of cloud-related issues in three dimensions
- eDiscovery considerations
- Jurisdictions and data locations
- Liability for activities of subcontractors
- Due diligence responsibility
- Federal Rules of Civil Procedure and electronically stored information
- Metadata
- Litigation hold

Domain 4: Compliance and Audit Management
- Definition of Compliance
- Right to audit
- Compliance impact on cloud contracts
- Audit scope and compliance scope
- Compliance analysis requirements
- Auditor requirements

Domain 5: Information Management and Data Security
- Six phases of the Data Security Lifecycle and their key elements
- Volume storage
- Object storage
- Logical vs physical locations of data
- Three valid options for protecting data
- Data Loss Prevention
- Detection Data Migration to the Cloud
- Encryption in IaaS, PaaS & SaaS
- Database Activity Monitoring and File Activity Monitoring
- Data Backup
- Data Dispersion
- Data Fragmentation

Domain 6: Interoperability and Portability
- Definitions of Portability and Interoperability
- Virtualization impacts on Portability and Interoperability
- SAML and WS-Security
- Size of Data Sets
- Lock-In considerations by IaaS, PaaS & SaaS delivery models
- Mitigating hardware compatibility issues

Domain 7: Traditional Security, Business Continuity, and Disaster Recovery

- Four D's of perimeter security
- Cloud backup and disaster recovery services
- Customer due diligence related to BCM/DR
- Business Continuity Management/Disaster Recovery due diligence
- Restoration Plan
- Physical location of cloud provider

Domain 8: Data Center Operations

- Relation to Cloud Controls Matrix
- Queries run by data center operators
- Technical aspects of a Provider's data center operations customer should understand
- Logging and report generation in multi-site clouds

Domain 9: Incident Response

- Factor allowing for more efficient and effective containment and recovery in a cloud
- Main data source for detection and analysis of an incident
- Investigating and containing an incident in an Infrastructure as a Service environment
- Reducing the occurrence of application level incidents
- How often should incident response testing occur
- Offline analysis of potential incidents

Domain 10: Application Security

- identity, entitlement, and access management (IdEA)
- SDLC impact and implications
- Differences in S-P-I models
- Consideration when performing a remote vulnerability test of a cloud-based application
- Categories of security monitoring for applications
- Entitlement matrix

Domain 11: Encryption and Key Management

- Adequate encryption protection of data in the cloud
- Key management best practices, location of keys, keys per user
- Relationship to tokenization, masking, anonymization and cloud database controls

Domain 12: Identity, Entitlement, and Access Management

- Relationship between identities and attributes
- Identity Federation
- Relationship between Policy Decision Point (PDP) and Policy Enforcement Point (PEP)
- SAML and WS-Federation
- Provisioning and authoritative sources

Domain 13: Virtualization

- Security concerns for hypervisor architecture

- VM guest hardening, blind spots, VM Sprawl, data comingling, instant-on gaps
- In-Motion VM characteristics that can create a serious complexity for audits
- How can virtual machine communications bypass network security controls
- VM attack surfaces
- Compartmentalization of VMs

Domain 14: Security as a Service

- 10 categories
- Barriers to developing full confidence in security as a service (SECaaS)
- When deploying Security as a Service in a highly regulated industry or environment, what should both parties agree on in advance and include in the SLA
- Logging and reporting implications
- How can web security as a service be deployed
- What measures do Security as a Service providers take to earn the trust of their customers

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 vs data processor definitions
- in Infrastructure as a Service (IaaS), who is responsible for guest systems monitoring

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.

