

Certificate of Cloud Auditing Knowledge

instructor-led training syllabus

CCAK Overview

The CCAK instructor-led training course curriculum consists of 5 major areas of coverage:

1. Cloud Governance
2. Cloud Compliance
3. Cloud Auditing
4. Cloud Assurance
5. CSA Tools: CCM, CAIQ and STAR Program

The areas of coverage are covered in 9 modules, with specific coverage areas as listed below.

CCAK Objectives

The objectives of the CCAK training are to provide knowledge about:

- cloud security **assessment methods and techniques** and how to use them to evaluate a cloud service prior to and during the provision of the service and
- how to ensure that a cloud service is compliant with the company requirements and is aligned with the governance approach of the organization.
- In addition, the CCAK will give those individuals with an auditing role and background the necessary knowledge to be able to update their expertise from on-prem IT security auditing to cloud and hybrid security auditing.

Course Structure

The CCAK course is divided into nine modules that cover the essential principles of auditing cloud computing systems.

MODULE 1: Cloud Governance (4 hrs)

- Overview of governance
- Cloud assurance
- Cloud governance frameworks
- Cloud risk management
- Cloud governance tools

MODULE 2: Cloud Compliance Program (3 hrs)

- Designing a cloud compliance program
- Building a cloud compliance program
- Legal and regulatory requirements
- Standards and security frameworks
- Identifying controls and measuring effectiveness
- CSA certification, attestation and validation

MODULE 3: CCM and CAIQ Goals, Objectives and Structure (1.5 hrs)

- CCM
- CAIQ
- Relationship to standards: mappings and gap analysis
- Transition from CCM V3.0.1 to CCM V4

MODULE 4: A Threat Analysis Methodology for Cloud Using CCM (1 hr)

- Definitions and purpose
- Attack details and impacts
- Mitigating controls and metrics
- Use case

MODULE 5: Evaluating a Cloud Compliance Program (1.5 hrs)

- Evaluation approach
- A governance perspective
- Legal, regulatory and standards perspectives
- Risk perspectives
- Services changes implications
- The need for continuous assurance/continuous compliance

MODULE 6: Cloud Auditing (2 hrs)

- Audit characteristics, criteria & principles
- Auditing standards for cloud computing
- Auditing an on-premises environment vs. cloud
- Differences in assessing cloud services and cloud delivery models
- Cloud audit building, planning and execution

MODULE 7: CCM: Auditing Controls (1 hr)

- CCM audit scoping guidance
- CCM risk evaluation guide
- CCM audit workbook
- CCM an auditing example

MODULE 8: Continuous Assurance and Compliance (1 hr)

- DevOps and DevSecOps
- Auditing CI/CD pipelines
- DevSecOps automation and maturity

MODULE 9: STAR Program (1 hr)

- Standard for security and privacy
- Open Certification Framework
- STAR Registry
- STAR Level 1
- STAR Level 2
- STAR Level 3