

# Cloud Audit Certification Training (CCAK)

Course: **00062**

Filter: **Beginner**

Duration: **20 hours**

Category:: **Cyber Security**

Price: **3000,00 €**

## About Course

In this course, you will learn the essential principles of auditing cloud computing systems to successfully obtain the Cloud Audit Certification (CCAK). The CCAK Certification training program was developed by the Cloud Security Alliance, the global leader in cloud security best practices, in partnership with ISACA, an international professional association focused on IT audit, security, cybersecurity, risk, privacy, and governance.

## What you'll learn

- Ensure the right controls for confidentiality, integrity, and accessibility.
- Mitigate risks and costs of audit management and penalties for non-compliance.
- Enhance organizational reputation and customer trust.
- Follow the Official ISACA Curriculum.
- Continue learning and face new challenges with after-course one-on-one instructor coaching.

## Pre-requisites

- To succeed in this course, you should have some foundational education or experience in cybersecurity.

## Curriculum

## **Module 1: Cloud Governance**

- In this module, you will learn about the basics of cloud governance, including:
- Assurance
- Governance Frameworks
- Risk Management
- Governance Tools

## **Module 2: Cloud Compliance Program**

- In this module, you will learn:
- How to design and build a Cloud Compliance Program
- Legal and regulatory requirements
- Standards and security frameworks
- How to identify controls and measure effectiveness
- CSA certification, attestation, and validation

## **Module 3: CCM And CAIQ Goals, Objectives, and Structure**

- In this module, you will learn about:
- The CSA Cloud Controls Matrix (CCM)
- The Consensus Assessments Initiative Questionnaire (CAIQ)
- The relationship to standards: mappings and gap analysis
- The transition from CCM V3.0.1 to CCM V4

## **Module 4: Threat Analysis Methodology for Cloud Using CCM**

- In this module, you will learn about:
- Definitions and purpose
- Attack details and impacts
- Mitigating controls and metrics

## **Module 5: Evaluating A Cloud Compliance Program**

- Governance perspectives
- Legal, regulatory, and standards perspectives

- Risk perspectives
- Services changes implications
- The need for continuous assurance/continuous compliance

### **Module 6: Cloud Auditing**

- In this module, you will learn how to:
- Audit characteristics, criteria, and principles
- Audit standards for cloud computing
- Audit an on-premises environment vs. cloud
- Pinpoint the differences in assessing cloud services vs. cloud delivery models
- Build, plan, and execute a cloud audit

### **Module 7: CCM Auditing Controls**

- In this module, you will learn about:
- Audit scoping guidance
- Risk evaluation guide
- Using an audit workbook

### **Module 8: Continuous Assurance and Compliance**

- In this module, you will learn about:
- DevOps and DevSecOps
- Auditing CI/CD pipelines
- DevSecOps automation and maturity

### **Module 9: STAR Program**

- In this module, you will learn about:
- Security and privacy standards
- Open Certification Framework
- STAR Registry
- STAR Levels 1, 2 and 3