Certificate of Cloud Auditing Knowledge (CCAK)

Duration: 16 Hours (2 Days)

Overview

The Certificate of Cloud Auditing Knowledge (CCAK) course is a specialized training program designed to equip learners with comprehensive knowledge and skills for auditing cloud computing systems. The course covers a range of topics including Cloud governance, compliance, risk management, and the use of Cloud Security Alliance (CSA)'s Cloud Controls Matrix (CCM) and Consensus Assessments Initiative Questionnaire (CAIQ). Through CCAK training, participants will learn to design and evaluate Cloud compliance programs, understand Legal and regulatory requirements, and implement Continuous assurance mechanisms. CCAK certification validates the expertise of professionals in cloud security audit and enhances their ability to manage cloud risks effectively. By delving into various modules, learners will gain practical insights into Cloud audit characteristics, Threat analysis, and the STAR program, which are essential for maintaining cloud security and compliance in an ever-evolving technological landscape.

Audience Profile

The CCAK course equips professionals for governance, risk management, and compliance in cloud environments, ideal for IT auditors and security experts.

- IT Auditors
- Cloud Security Professionals
- Compliance Managers
- Risk Management Officers
- Cloud Governance Specialists
- Information Security Analysts
- Cybersecurity Consultants
- Cloud Architects
- Cloud Service Providers
- Data Privacy Officers
- IT Governance Professionals
- Cloud Compliance Lawyers
- Security Operations Managers
- CISOs (Chief Information Security Officers)
- Regulatory Affairs Managers
- DevOps and DevSecOps Engineers (interested in compliance and auditing)

Course Syllabus

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

Module 1: Cloud Governance

- Overview of governance
- Cloud assurance
- Cloud governance frameworks

- Cloud risk management
- Cloud governance tools

Module 2: Cloud Compliance Program

- 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

- 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

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

Module 5: Evaluating a Cloud Compliance Program

- 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

- 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

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

Module 8: Continuous Assurance and Compliance

- DevOps and DevSecOps
- Auditing CI/CD pipelines

- DevSecOps automation and maturity

Module 9: STAR Program

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