+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 30/06/2025

Sign up

CCSK certification training

ALL-IN-ONE : EXAM INCLUDED IN PRICE

2 days (14 hours)

Presentation

Immerse yourself in the world of cloud security with our training course dedicated to CCSK certification from the cloud security alliance. This structured course covers the entire cycle of securing a multi-cloud environment, from strategic governance to incident response and Zero Trust IAM. By the end of the course, you'll be fully prepared for the official CCSK exam, and able to manage the security of your AWS, Azure and GCP infrastructures with confidence.

You'll start by getting to grips with CSA's flagship repositories to map your cloud services and establish a clear responsibility matrix. You'll learn how to assess risks, align your policies with RGPD, ISO 27017/18 and SecNumCloud requirements, and then deploy meaningful governance dashboards for your executive committee.

You will then enter the operational heart of cloud security: developing a "least privilege" IAM strategy, configuring centralized logs and threat detection with SIEM, advanced network segmentation and Zero Trust bastions. These concepts will be immediately applied in practical workshops.

The training continues with securing workloads - VMs, Kubernetes containers and serverless functions - and integrating DevSecOps: SAST/SCA scans, automatic SBOM generation and continuous deployments to a protected cluster. You'll also learn how to orchestrate incident response, automate encrypted backups and test resilience via chaos engineering exercises.

As with all our training courses, this one will be presented with the latest CCSK certification updates.

Objectives

- Validate CCSK v5 certification
- Govern multicloud security
- Deploy Zero Trust and least-privilege IAM
- Implement workload protection
- Automate DevSecOps & monitoring
- Orchestrate cloud incident response

Target audience

- Cybersecurity managers
- Cloud architect
- GRC consultants
- Cloud project managers

PREREQUISITES

- Basic IT security: firewalls, encryption, access management
- Fundamental knowledge of cloud computing
- Network (TCP/IP, VPN, proxy) and system (Linux/Windows) skills useful for labs

CCSK training program

Fundamentals of cloud computing

- Key definitions and evolution of the cloud
- Service models: IaaS, PaaS, SaaS
- Deployment models: public, private, hybrid, multi-cloud
- Principle of shared supplier/customer responsibility
- Key terminology: region, zone, tenant, marketplace

Governance & CSA standards

- Role of the Cloud Security Steering Committee
- Security Guidance v5: structure and usage
- Cloud Controls Matrix (CCM): mapping controls
- Managing cloud policies and procedures
- Workshop: Mapping cloud services and assigning responsibilities (RACI)

Risk Management, Audit & Compliance

- Risk analysis methodologies adapted to the cloud
- Standards / frameworks: ISO 27017/18, SOC 2, SecNumCloud, RGPD
- Supplier due diligence: CSA CAIQ questionnaires, audit reports
- Security contracts & SLAs: essential clauses

- Workshop: Drawing up a cloud risk heat map and treatment plan

Identity & Access Management and Zero Trust

- Zero Trust principles and identity as a new perimeter
- Identity federations, OAuth 2.0, OpenID Connect, SAML
- Account lifecycle management, roles and RBAC/ABAC strategies
- Strong authentication concepts (MFA, FIDO2)
- Workshop: Creating a "least privilege" IAM strategy and verifying posture

Monitoring, Logging & Continuous Audit

- Log collection: CloudTrail, Azure Monitor, GCP Audit Logs
- SIEM, UEBA and multi-cloud correlation
- CSPM / CWPP tools for continuous auditing
- Cloud threat detection & response principles
- Dashboards and key performance indicators (KPIs)

Network security & Cloud architecture

- Logical segmentation (VPC/VNet), private/public subnets
- Native network controls: SG, NACL, NSG, WAF firewall
- Hybrid network designs and transit gateways
- Securing APIs & API gateways
- Network resilience: high availability, multi-region, CDN

Data protection & encryption

- Classification and lifecycle of data in the cloud
- At-rest / in-transit / in-use encryption, key management (KMS, HSM)
- BYOK / HYOK strategies and key rotation
- Data loss prevention (DLP) and masking
- RGPD compliance: localization, consent, right to be forgotten

Workload security & DevSecOps

- Hardening of VMs, containers and serverless functions
- CIS benchmarks, Kubernetes controls & eBPF policy
- Integrating security into CI/CD (shift-left)
- Secret management and SBOM: best practices
- Workshop: Implementing a DevSecOps CI/CD pipeline with SAST + SCA scans

Incident Response, Emerging Strategies & Exam Preparation

- Cloud incident response plan and table-top exercises
- Backups, disaster recovery and chaos engineering
- Trends 2025: Advanced Zero Trust, IA/GenAI security, FinOps
- CCSK exam simulation (60 MCQs, open-book) and targeted debriefing
- Individual post-certification skills roadmap

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced IT technology, or to acquire specific business knowledge or modern methods.

Positioning at training start

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical training: 60% hands-on, 40% theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Certification

A certificate will be awarded to each trainee who has completed the entire course.