

Mis à jour le 01/07/2025

S'inscrire

Formation certification CCAK

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

2 jours (14 heures)

Présentation

Le CCAK (Certificate of Cloud Auditing Knowledge) est la première certification mondiale entièrement dédiée à l'audit de la sécurité dans le cloud.

Cette formation CCAK vous permettra de concevoir et conduire un audit cloud de bout en bout, en intégrant les spécificités du cloud computing (responsabilité partagée, infrastructure dynamique, automatisation DevSecOps).

Vous apprendrez à évaluer les risques, analyser les contrôles, auditer des workloads cloud-natifs, et à restituer vos constats sous forme de tableaux de bord exploitables par le COMEX.

Votre équipe pourra maîtriser l'utilisation des outils de conformité cloud tels que la Cloud Controls Matrix (CCM v4), le CAIQ, et les guides d'audit CSA. Vous saurez également adapter les exigences réglementaires (RGPD, ISO 27001/17, SecNumCloud) à des services IaaS, PaaS et SaaS.

Le CCAK vous permet de piloter des audits cloud, de sécuriser les relations avec les fournisseurs cloud, et de garantir que votre organisation respecte ses obligations de conformité en environnement hybride ou multicloud.

Comme pour toutes nos formations, celle-ci vous sera présentée avec les toutes dernières actualisations pour le passage de la certification [CCAK](#).

Objectifs

- Comprendre les spécificités de l'audit dans un environnement cloud

- Maîtriser la Cloud Controls Matrix (CCM), le CAIQ et le programme CSA STAR
- Élaborer un plan d'audit cloud fondé sur les risques
- Intégrer les contraintes réglementaires et contractuelles dans le périmètre d'audit
- Préparer et réussir l'examen CCAK avec méthode

Public visé

- Responsable cybersécurité
- Architecte cloud
- Consultants GRC
- Auditeur IT

PRÉ-REQUIS

- Bases de sécurité informatique : pare-feu, chiffrement, IAM, réseaux

Programme de notre formation CCAK

Comprendre les fondamentaux de l'audit cloud

- Évolution du cloud computing et défis pour l'audit
- Spécificités du cloud : élasticité, self-service, mutualisation
- Modèle de responsabilité partagée client / fournisseur
- Rôle de l'audit dans les environnements cloud
- Présentation générale de la certification CCAK

Gouvernance et cadre de conformité cloud

- Référentiels : ISO 27001/17, RGPD, NIST, SecNumCloud
- Acteurs clés : client, fournisseur, tiers, régulateurs
- Politique de sécurité et pilotage des contrôles cloud
- Gouvernance des données et enjeux transfrontaliers
- Outils de traçabilité et contractualisation des engagements
- Atelier : Identifier les responsabilités contractuelles dans un projet SaaS en s'appuyant sur le modèle CCM

Construire un programme de conformité cloud

- Définir les objectifs de conformité dans un contexte multicloud
- Méthodologie d'élaboration d'un programme de conformité
- Choisir les contrôles pertinents à auditer
- Intégration des standards CSA : CCM v4, CAIQ
- Introduction au programme CSA STAR

Maîtriser la Cloud Controls Matrix (CCM v4)

- Architecture de la CCM : domaines, contrôles, mapping ISO/NIST
- Utiliser la CAIQ pour auditer un fournisseur cloud
- Focus sur les contrôles critiques (IAM, logs, chiffrement, réseau)
- Adapter la CCM à un environnement IaaS, PaaS ou SaaS
- Introduction aux guides d'audit CSA et à la notation
- Atelier : Évaluer un contrôle CCM "IAM" à l'aide d'un guide d'audit CSA et noter la conformité

Évaluer les risques et menaces liés au cloud

- Risques spécifiques au cloud : shadow IT, mauvaise configuration, log insuffisant
- Menaces : perte de données, compromission d'API, vulnérabilités partagées
- Modèles d'analyse : STRIDE, impact business, arbres d'attaque
- Priorisation par gravité et probabilité
- Techniques d'audit orientées risque
- Atelier : Construire une heatmap de risques cloud pour une entreprise fictive (multicloud + SaaS)

Préparer et réaliser un audit cloud

- Définir le périmètre de l'audit cloud
- Sélection des contrôles : approche basée sur le risque
- Méthodologie d'audit (planification, collecte, scoring, restitution)
- Différences avec un audit IT traditionnel
- Livrables attendus : plan d'audit, grilles, rapport final

Assurance continue, DevSecOps & automatisation

- Intégrer l'audit dans un pipeline CI/CD
- Notions de drift detection et contrôles en continu
- Outils DevSecOps : GitOps, Terraform, OPA/Rego
- Journalisation et supervision automatisée
- Audit des workloads cloud-natifs (VM, conteneurs, fonctions)
- Atelier : Implémenter un scan de conformité (secrets, vulnérabilités) dans un pipeline CI/CD GitHub Actions

Exploiter le programme CSA STAR

- Fonctionnement du programme STAR
- Auto-évaluation, certification ISO 27001 et attestations SOC 2
- Intégrer STAR dans une démarche de sélection fournisseur
- Utiliser STAR pour comparer les postures sécurité cloud
- Lien entre STAR, CCM et due diligence fournisseurs

Préparer et réussir la certification CCAK

- Structure de l'examen : 76 QCM, 2h, score requis 70 %

- Types de questions posées et thématiques clés
- Recommandations pour l'étude et lecture active du référentiel
- Simulations d'audit : synthèse, restitution, présentation COMEX
- Examen blanc + plan de révision personnalisé

Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.