FORMATION PRATIQUE · PRÉPARATION À LA CERTIFICATION

CISA (Certified Information Systems Auditor), préparation à la certification ISACA

Certification **ISACA** — CISA® · Préparation à l'examen

DURÉE	MODALITÉ	RÉFÉRENCE	PRIX
5 jours 35h00 de formation	**Pratique** Présentiel / à distance	**CKA** Certification ISACA	**2 625 000 FCFA** H.T. par participant

Ce cours prépare à l'examen CISA® (Certified Information Systems Auditor) de l'ISACA®, la certification de référence des auditeurs des systèmes d'information. Il couvre les cinq domaines de l'examen : processus d'audit des SI, gouvernance et gestion des SI, acquisition, conception et implantation des SI, exploitation, entretien et soutien des SI, protection des actifs informationnels. Cette formation est donnée en français.

01 Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- Préparer l'examen de certification CISA® (Certified Information Systems Auditor) de l'ISACA
- Connaître les cinq domaines sur lesquels porte la certification CISA®
- Comprendre les concepts relatifs à l'audit des systèmes d'information et à la gouvernance des TI

02 Le programme en bref

01 Domaine 1: processus d'audit des systèmes d'information

02 Domaine 2 : gouvernance et gestion des systèmes d'information

03 Domaine 3 : acquisition, conception, implantation des SI

04 Domaine 4 : exploitation, entretien et soutien des systèmes d'information

05 Domaine 5 : protection des actifs informationnels

PUBLIC CONCERNÉ

Auditeurs TI/SI, les professionnels du contrôle, de l'assurance et de la sécurité de l'information.

PRÉREQUIS

Avoir cinq ans ou plus d'expérience dans l'audit, le contrôle, l'assurance ou la sécurité des SI/TI.

VOS FORMATEURS

Des consultants spécialistes du domaine, validés par notre équipe pédagogique, avec cinq à dix ans d'expérience terrain au minimum.

02 Programme détaillé

5 modules · 5 jours · 35h00

1 Domaine 1: processus d'audit des systèmes d'information

- Normes, lignes directrices et codes de déontologie en matière d'audit des SI.
- Processus d'affaires.
- Types de contrôles.
- Planification de l'audit basée sur le risque.
- Types d'audits et d'évaluations.
- Gestion du projet d'audit.
- Méthodologie d'échantillonnage.
- Techniques de collecte des preuves d'audit.
- Analyse des données.
- Techniques d'établissement de rapports et de communication.
- Assurance qualité et amélioration du processus d'audit.

2 Domaine 2 : gouvernance et gestion des systèmes d'information

- Gouvernance informatique et stratégie informatique.
- Cadres liés à l'informatique.
- Normes, politiques et procédures informatiques.
- Structure organisationnelle.
- Architecture d'entreprise.
- Gestion des risques de l'entreprise.
- Modèles de maturité.
- Lois, règlements et normes industrielles affectant l'organisation.
- Gestion des ressources informatiques.
- Acquisition et gestion des fournisseurs de services informatiques.
- Contrôle des performances informatiques et établissement de rapports.
- Assurance et gestion de la qualité des technologies de l'information.

3 Domaine 3 : acquisition, conception, implantation des SI

- Gouvernance et gestion des projets.
- Analyse de rentabilité et de faisabilité.
- Méthodologies de développement des systèmes.
- Identification et conception des contrôles.
- Méthodologies de test.
- Gestion de la configuration et des versions.
- Migration des systèmes, déploiement de l'infrastructure et conversion des données.
- Revue post-implémentation.

4 Domaine 4 : exploitation, entretien et soutien des systèmes d'information

- Composants technologiques communs.
- Gestion des actifs informatiques.
- Planification des tâches et automatisation des processus de production.
- Interfaces de systèmes.
- Informatique pour l'utilisateur final.
- Gouvernance des données.
- Gestion des performances des systèmes.
- Gestion des problèmes et des incidents.
- Gestion des changements, des configurations, des versions et des correctifs.
- Gestion des niveaux de service informatique.
- Gestion des bases de données.
- Analyse d'impact sur les activités (BIA).
- Résilience des systèmes.
- Sauvegarde, stockage et restauration des données.
- Plan de continuité des activités (BCP).
- Plans de reprise après sinistre (DRP).

5 Domaine 5 : protection des actifs informationnels

- Cadres, normes et lignes directrices en matière de sécurité du patrimoine informationnel.
- Principes de protection de la vie privée.
- Contrôles de l'accès physique et de l'environnement.
- Gestion des identités et des accès.
- Sécurité des réseaux et des points finaux.
- Classification des données.
- Chiffrement des données et techniques liées au chiffrement.
- Infrastructure à clé publique (PKI).
- Techniques de communication basées sur le web.
- Environnements virtualisés.
- Dispositifs mobiles, sans fil et Internet des objets (IoT).
- Formation et programmes de sensibilisation à la sécurité.
- Méthodes et techniques d'attaque des systèmes d'information.
- Outils et techniques de test de sécurité.
- Outils et techniques de contrôle de la sécurité.
- Gestion des réponses aux incidents.
- Collecte de preuves et criminalistique.

03 Informations pratiques

Horaires

Les cours ont lieu de 9h à 12h30 et de 14h à 17h30. Les participants sont accueillis à partir de 8h45. Les pauses et déjeuners sont offerts.

Pour les formations de 4 ou 5 jours, quelle que soit la modalité, les sessions se terminent à 16h le dernier jour.

Solutions de financement

Plusieurs solutions existent pour financer votre formation et dépendent de votre situation professionnelle. Découvrez-les sur notre page « Comment financer sa formation » ou contactez votre conseiller formation.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les formations pratiques, études de cas ou présentation de cas réels pour les séminaires de formation. À l'issue de chaque formation ou séminaire, Crisalida fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques. Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ (PSH)

Notre référent handicap répond à toute question ou besoin d'aménagement : crisalid@crisalida.ci.

DATES ET LIEUX — 2026

CLASSE À DISTANCE

14 déc. 2026

ABIDJAN

14 déc. 2026

CERTIFICATION	L'examen, disponible en ligne et en différé, comporte 150 questions qui doivent être complétées en 4 heures. La certification CISA est reconnue dans le monde entier. Le passage de l'examen n'est pas compris dans le tarif : il se réserve directement auprès de ISACA. Nous vous indiquons la démarche.
MODALITÉS D'ÉVALUATION	Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques... Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

Besoin d'un parcours sur mesure ?

Crisalida Conseil & Formation construit avec vous des parcours adaptés à vos équipes, en inter, en intra ou à distance. Votre conseiller formation : crisalid@crisalida.ci.