Date de publication : 11/12/2025

Formation : CISA, Certified IS Auditor, préparation à la certification ISACA

Formation officielle ISACA

Formation pratique - 5j - 35h00 - Réf. CKA

Prix : 4000 CHF H.T.

4,2 / 5

Ce cours permet de préparer l'examen CISA®, Certified Information Systems Auditor, en couvrant la totalité du cursus CBK (Common Body of Knowledge), tronc commun de connaissances en sécurité défini par l'ISACA®, Information Systems Audit and Control Association. Cette formation est donnée en français et les supports officiels utilisés sont en anglais.

Objectifs pédagogiques

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

- Préparer l'examen de certification CISA, Auditeur Sécurité certifié ISACA
- Connaitre les cinq grands domaines sur lesquels porte la certification CISA®
- Comprendre les concepts relatifs à l'audit du SI et à la gouvernance des TI

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.

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.

Programme de la formation

PARTICIPANTS

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.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

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.

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.

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, ORSYS 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 AUX PERSONNES HANDICAPÉES

Pour toute question ou besoin relatif à l'accessibilité, vous pouvez joindre notre équipe PSH par e-mail à l'adresse psh-accueil@orsys.fr.

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.

Partenariat

Formation officielle accréditée par l'ISACA en partenariat exclusif avec ACG Cybersecurity

Options

Certification : 780 € HT

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.

Dates et lieux

CLASSE À DISTANCE
2026 : 29 juin, 12 oct., 14 déc.