

# Formation : CISM, Certified IS Manager, préparation à la certification ISACA

Formation officielle ISACA

Formation pratique - 4j - 28h00 - Réf. CKM

Prix : 3740 CHF H.T.

★★★★☆ 3,9 / 5

Cette formation a pour but de préparer les candidats à l'examen du CISM (Certified Information System Manager), la certification internationale délivrée par l'ISACA, examen qui se déroule chaque année en juin et décembre.

## Objectifs pédagogiques

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

- ✓ Acquérir les connaissances nécessaires à la réussite de l'examen CISM
- ✓ Maîtriser les concepts de la gestion de la sécurité de l'information
- ✓ Évaluer, concevoir, déployer, superviser et améliorer tout système de gestion de la sécurité de l'information
- ✓ Acquérir les connaissances et les concepts de base de l'audit des systèmes d'information

## Public concerné

Toutes personnes qui gèrent, conçoivent, supervisent et évaluent la fonction de sécurité de l'information d'une entreprise.

## Prérequis

Avoir cinq ans ou plus d'expérience dans la gestion de la sécurité de l'information.

## 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

Toutes personnes qui gèrent, conçoivent, supervisent et évaluent la fonction de sécurité de l'information d'une entreprise.

### PRÉREQUIS

Avoir cinq ans ou plus d'expérience dans la gestion de la sécurité de l'information.

### 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 : gouvernance de la sécurité de l'information

- Présentation de la gouvernance d'entreprise.
- Culture organisationnelle, structures, rôles et responsabilités.
- Exigences légales, réglementaires et contractuelles.
- Stratégie de sécurité de l'information.
- Cadres et normes de gouvernance de l'information.
- Planification stratégique.

## 2 Domaine 2 : gestion des risques liés à l'information

- Développement du processus continu de gestion des risques.
- Identification, analyse et évaluation des risques.
- Définition des stratégies de traitement des risques.
- Communication de la gestion des risques.

## 3 Domaine 3 : développement et gestion du programme de sécurité de l'information

- L'architecture en sécurité de l'information.
- Méthodes pour définir les mesures de sécurité requises.
- Gestion des contrats et des prérequis de sécurité de l'information.
- Métriques et évaluation de la performance en sécurité de l'information.
- Communications, rapports et gestion des performances du programme.

## 4 Domaine 4 : plan de gestion des incidents de sécurité de l'information

- Composantes d'un plan de gestion des incidents de sécurité.
- Concepts et pratiques en gestion des incidents de sécurité.
- Méthode de classification.
- Processus de notification et d'escalade.
- Techniques de détection et d'analyse des incidents.

## 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.

## Dates et lieux

**CLASSE À DISTANCE**

2026 : 2 juin, 20 oct., 1 déc.

### 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](mailto:psh-accueil@orsys.fr).