

CISM® : manager certifié en sécurité de l'information

| |
|--|
| Date et durée |
| Code formation : SEC19FR Durée : 5 jours Nombre d'heures : 35 heures |
| Formation avec certification |
| CISM® : Certified Information Security Manager |
| Description |
| <p>La certification CISM, délivrée par l'ISACA (Information Systems Audit and Control Association), est une certification professionnelle mondialement reconnue qui atteste de compétences avancées en management de la sécurité de l'information. Elle s'adresse aux professionnels qui gèrent, conçoivent, supervisent et évaluent la sécurité de l'information d'une entreprise, comme les responsables de la sécurité des systèmes d'information (RSSI), les consultants en sécurité et les auditeurs en sécurité.</p> <p>Cette formation CISM vous fournira les compétences et les connaissances nécessaires pour maîtriser les 4 domaines d'expertise couverts par la certification :</p> <ul style="list-style-type: none">• la gouvernance de la sécurité de l'information (stratégie de sécurité, politiques de sécurité, conformité réglementaire, etc.) ;• la gestion des risques liés à l'information et conformité (identification et évaluation des risques, gestion des risques, conformité aux normes et réglementations, etc.) ;• le développement et la gestion des programmes SI (conception et mise en œuvre de programmes de sécurité, gestion des ressources, etc.) ;• la gestion des incidents de sécurité de l'information (détection et réponse aux incidents, analyse forensique, etc.). <p>Grâce à une combinaison de cours théoriques, d'études de cas, d'exercices pratiques et d'un examen blanc, ce programme vous prépare efficacement au passage de l'examen CISM compris dans notre offre (<i>en savoir plus dans l'onglet certification</i>).</p> |
| Objectifs |
| <p>À l'issue de la formation CISM, vous atteindrez les objectifs suivants :</p> <ul style="list-style-type: none">• comprendre les 4 domaines de la gestion de la sécurité de l'information selon les exigences du CISM ;• maîtriser le vocabulaire et les modalités de l'examen de certification ;• découvrir l'ensemble des normes et procédures applicables au management de la sécurité de l'information ;• se préparer et réussir l'examen officiel CISM® (Certified Information Security Manager). |
| Points forts |
| <ul style="list-style-type: none">• Un formateur accrédité par l'ISACA.• Des exercices et cas pratiques. |

- Le passage d'un examen blanc.
- Un accès pendant 12 mois à la base de données d'ISACA « Questions, Answers & Explanations (QAE) » de 1 070 questions conçues pour vous préparer à l'examen CISM.
- Le coût de l'examen CISM® inclut dans le prix de notre formation.

Certification

Cette formation vous prépare au passage de l'examen de certification professionnelle Certified Information Security Manager® (CISM). L'inscription à l'examen est comprise dans le prix de notre formation, ainsi un voucher (code coupon) vous sera transmis en fin de la formation. Il vous permettra de planifier votre examen sur le site web de l'ISACA.

Modalité de l'examen CISM® (2025)

- **Type d'examen** : QCM de 150 questions
- **Durée** : 4h00
- **Lieu** : Examen surveillé en ligne
- **Livre ouvert** : Non
- **Langue** : Chinois simplifié, Anglais, Japonais et Espagnol
- **Note de passage** : Un score standardisé de 450 sur une échelle de 200 à 800 est requis pour réussir l'examen.

Exigences post-examen pour obtenir la certification CISM® :

Après avoir réussi l'examen, vous devez satisfaire les exigences suivantes :

- **Une expérience professionnelle de 5 ans*** minimum dans le domaine de la gestion de la sécurité de l'information, dont au moins 3 ans dans 3 des 4 domaines suivants :
 - la gouvernance de la sécurité de l'information ;
 - la gestion des risques liés à l'information et la conformité ;
 - le développement et la gestion des programmes de sécurité de l'information ;
 - la gestion des incidents de sécurité de l'information.

***Note** : si vous êtes titulaire d'un diplôme universitaire en sécurité de l'information (par exemple, un master en cybersécurité) ou de certaines certifications reconnues par l'ISACA (par exemple, CISSP et CISA), vous bénéficierez d'une dispense d'expérience d'un an.

- **Adhérer au Code d'éthique professionnelle de l'ISACA.**
- **Suivre une formation professionnelle continue** : vous devrez maintenir votre certification en accumulant des heures de CPE (20 heures par an et 120 heures par période de trois ans).

À savoir : la certification CISM® est valable pour une durée de 3 ans. Pour en savoir plus, consulter le guide du candidat aux examens de certification ISACA

Modalités d'évaluation

Travaux Pratiques
Etude de cas
Examen blanc

Pré-requis

Pour suivre cette formation certifiante, les prérequis suivants sont nécessaires :

- Une expérience professionnelle de 5 ans* minimum dans le domaine de la gestion de la sécurité de l'information, dont au moins 3 ans dans 3 des 4 domaines suivants :

- la gouvernance de la sécurité de l'information ;
- la gestion des risques liés à l'information et la conformité ;
- le développement et la gestion des programmes de sécurité de l'information ;
- la gestion des incidents de sécurité de l'information.

***Note :** *si vous êtes titulaire d'un diplôme universitaire en sécurité de l'information (par exemple, un master en cybersécurité) ou de certaines certifications reconnues par l'ISACA (par exemple, CISSP et CISA), vous bénéficierez d'une dispense d'expérience d'un an.*

- Une bonne compréhension des infrastructures réseau (TCP/IP, routage, pare-feu, VPN, etc.), des connaissances en sécurité des systèmes (configuration sécurisée, gestion des vulnérabilités, systèmes de détection d'intrusion, etc.) et des notions de cryptographie.
- Savoir lire et écrire l'anglais technique pour comprendre les supports de cours et passer l'examen officiel (*la formation est dispensée en français*).

Public

Cette formation s'adresse aux publics suivants :

- les professionnels de l'informatique, en particulier les cadres chargés de gérer la sécurité de l'information ;
- toute autre personne qui souhaite avoir une meilleure compréhension des risques liés à la sécurité de l'information d'une entreprise ou d'une organisation.

Cette formation s'adresse aux profils suivants

Administrateur réseaux - télécoms

Administrateur système

Ingénieur système

Ingénieur réseaux - télécoms

Auditeur interne / externe

Manager

Programme

Module 1 : gouvernance de la sécurité de l'information

- Concilier les stratégies de sécurité de l'information avec la stratégie de l'organisation.
- Développer une politique de sécurité de l'information performante.
- Répartir les rôles et les responsabilités au sein de la gouvernance.
- Réaliser un audit, information et communication autour de la gouvernance de la sécurité.

Module 2 : gestion des risques de l'information

- Mettre en place une approche systématique et analytique et un processus continu de gestion des risques.
- Identifier, analyser et évaluer les risques.
- Définir des stratégies de traitement des risques.
- Mettre en place une communication effective autour de la gestion des risques.

Module 3 : développement et gestion d'un plan de sécurité IT

- Comprendre l'architecture de la sécurité de l'information.
- Comprendre la méthodologie et les pratiques pour mettre en place des mesures de sécurité.
- Gérer les contrats et les prérequis de la sécurité de l'information.
- Utiliser les métriques et évaluer la performance de la sécurité.

Module 4 : gestion des incidents de la sécurité de l'information

- Comprendre le fonctionnement du plan de gestion des incidents de sécurité.
- Connaître les pratiques et techniques de la gestion des incidents de sécurité.
- Avoir une méthode de classification.
- Connaître les processus de notification et d'escalade.
- Détecter et analyser les incidents.

Module 5 : préparation à l'examen CISM

- Présentation des types de questions de l'examen.
- Passage d'un examen blanc complet (correction détaillée et analyse des résultats).
- Conseils et stratégies pour réussir l'examen (gestion du temps, techniques de lecture des questions et gestion du stress).

CISM est une marque déposée par [ISACA](#)