

Sécurité : Certified Information Security Manager (CISM)

Référence : **SECCISM**

Durée : **4 jours (28 heures)**

Certification : **CISM**

Connaissances préalables

- 1-Connaissances de base dans le fonctionnement des systèmes d'information
- 2-Afin d'obtenir la certification CISM, il faudra justifier de 5 ans d'expérience dans la gestion de la sécurité de l'informations. Des dérogations sont néanmoins possibles pour un maximum de 2 ans

Profil des stagiaires

- Consultants en sécurité
- Professionnels en sécurité
- RSSI
- Toute personne souhaitant acquérir des connaissances en la matière

Objectifs

- Découvrir et maîtriser les 4 grands domaines sur lesquels porte l'examen CISM
- Être capable d'assimiler le vocabulaire de la certification CISM et les idées directrices de l'examen
- Pouvoir s'entraîner au déroulement de l'épreuve et acquérir les stratégies de réponse au questionnaire
- Se préparer au passage de l'examen de certification CISM

Certification préparée

CISM - Certified Information Security Manager. L'examen CISM d'ISACA est un QCM comprenant 150 questions basées sur les 4 domaines : gouvernance de la sécurité de l'information, gestion des risques liés à l'information, développement et gestion de programmes de sécurité de l'information, gestion des incidents de sécurité de l'information. Pour en savoir plus sur ISACA [cliquez ici](#)

Méthodes pédagogiques

- Mise à disposition d'un poste de travail par participant
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques et de réflexions

Formateur

- Consultant-Formateur expert Management de la sécurité

Méthodes d'évaluation des acquis

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

Contenu du cours

1. Domaine 1 : Gouvernance de la sécurité de l'information

- Elaborer une stratégie de sécurité de l'information pour l'aligner sur la stratégie d'entreprise et de la direction
- Obtenir l'engagement de la haute direction et le soutien à la sécurité informatique dans toute l'entreprise
- Définir les rôles et les responsabilités dans la gouvernance de la sécurité de l'information
- Mettre en place des voies d'information et de communication concernant les activités de gouvernance de sécurité de l'information

2. Domaine 2 : Gestion des risques de l'information

- Expliquer l'importance de la gestion des risques en tant qu'outil pour répondre aux besoins de l'entreprise et développer un programme de gestion de la sécurité pour répondre à ces besoins
- Identifier, classer et répondre à un risque d'une manière appropriée, telle que définie par les directives de l'organisation
- Évaluer la pertinence et l'efficacité des contrôles de sécurité de l'information
- Signaler efficacement les risques liés à la sécurité de l'information

3. Domaine 3 : Développement et gestion de programmes de sécurité de l'information

- Aligner les exigences du programme de sécurité des informations sur celles des autres fonctions de l'entreprise
- Gérer les ressources du programme de sécurité de l'information
- Concevoir et mettre en oeuvre des contrôles de sécurité des informations
- Intégrer les exigences de sécurité de l'information dans les contrats, les accords et les processus de gestion tiers

4. Domaine 4 : Gestion des incidents de sécurité de l'information

- Comprendre les concepts et les pratiques de la gestion des incidents
- Identifier les composants d'un plan d'intervention en cas d'incident et évaluer son efficacité
- Comprendre les concepts clés de la planification de la continuité des activités, ou de la planification de la continuité des opérations et de la reprise après sinistre, ou du DRP

5. Exemple d'examen CISM

- L'inscription à l'examen se fait directement sur le site de l'ISACA
- Trois langues sont disponibles pour le passage de l'examen dont l'anglais (la langue française n'est pas disponible)

Notre référent handicap se tient à votre disposition au [01.71.19.70.30](tel:0171197030) ou par mail à referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.