Sécurité : Certified Information Security Manager (CISM)

Référence : **SECCISM** Durée : **3 jours** Certification : **CISM**

CONNAISSANCES PREALABLES

• 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 PREPAREE

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

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Management de la sécurité

METHODE D'EVALUATION DES ACQUIS

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

CONTENU DU COURS

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

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

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

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

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)