CRISC®, gestion des risques SI, préparation à la certification ISACA

Cours Pratique de 4 jours - 28h
Réf : CKR - Prix 0 : nous consulter

Ce cours est conçu pour les professionnels qui souhaitent réussir l'examen CRISC. Le programme couvre les quatre domaines clés traités dans l'examen : gouvernance, évaluation des risques informatiques, réponse aux risques et rapport, technologie et sécurité de l'information.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Maîtriser la démarche de gestion des risques selon le CRISC

Appliquer les meilleures stratégies de réponse aux risques qui pèsent sur le système d'information

Utiliser les meilleures pratiques de surveillance des risques

Définir des contrôles du système d'information

Utiliser les meilleures pratiques pour surveiller et maintenir ces contrôles

CERTIFICATION

L'examen consiste à répondre à 150 questions à choix multiples en anglais et en 4h00. Il est disponible en ligne et en différé.

LE PROGRAMME

dernière mise à jour : 12/2024

1) Domaine 1 : gouvernance

- Concepts, normes et cadres d'évaluation des risques.
- Stratégie organisationnelle, buts et objectifs.
- Structure organisationnelle, rôles et responsabilités.
- Culture organisationnelle et atouts.
- Politiques, normes et processus opérationnels.
- Gestion des risques d'entreprise, cadres de gestion des risques et trois lignes de défense.
- Profil de risque, appétence et tolérance au risque.
- Naviguer dans l'éthique de la gestion des risques et dans les exigences des lois, des réglementations et des contrôles.

2) Domaine 2 : évaluation des risques informatiques

- Événements à risque, modélisation des menaces et paysage des menaces.
- Analyse de vulnérabilité et de déficience de contrôle.
- Développement de scénarios de risque.
- Registre des risques.
- Méthodologies d'analyse des risques.
- Analyse de l'impact sur les activités.
- Risque inhérent, résiduel et actuel.

3) Domaine 3 : réponse aux risques et rapport

- Options de traitement des risques/de réponse aux risques.

PARTICIPANTS

Les personnes expérimentées dans la gestion des risques informatiques et la conception, la mise en œuvre, le suivi et la maintenance des contrôles SI.

PRÉREQUIS

Trois ans ou plus d'expérience dans la gestion des risques informatiques et le contrôle des SI.
Aucune renonciation ou substitution d'expérience acceptée.

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.

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 stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage 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 stagiaire 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

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

- Propriété du risque et du contrôle.
- Gestion des risques liés aux processus, aux tiers et aux sources émergentes.
- Types de contrôle, normes et cadres.
- Conception, sélection et analyse des contrôles.
- Mise en œuvre, tests et efficacité des contrôles.
- Plans de traitement des risques.
- Collecte, agrégation, analyse et validation de données.
- Techniques de surveillance et de reporting des risques et des contrôles.
- Mesures de performance, de risque et de contrôle.

4) Domaine 4 : technologie et sécurité de l'information

- Architecture d'entreprise.
- Gestion des opérations informatiques.
- Gestion de projet.
- Gestion de la reprise après sinistre (DRM).
- Gestion du cycle de vie des données.
- Cycle de vie du développement du système (SDLC).
- Technologies émergentes.
- Concepts, cadres et normes de sécurité de l'information.
- Formation de sensibilisation à la sécurité de l'information.
- Gestion de la continuité des activités.
- Principes de confidentialité et de protection des données.

LES DATES

Nous contacter