Préparation à la certification CRISC (Certified in Risk and Information Systems Control)

Durée: 5 Jours **Réf de cours: CRISC**

Résumé:

CRISC est la seule certification qui prépare et habilite les professionnels de l'informatique à relever les défis uniques de la gestion des risques informatiques et d'entreprise, et les positionne pour devenir des partenaires stratégiques de l'entreprise en aidant les entreprises à atteindre leurs objectifs commerciaux en concevant, en mettant en œuvre, en surveillant et en maintenant des contrôles des SI basés sur les risques, efficients et efficaces.
Le cours de préparation à l'examen CRISC est un programme de révision intensif de quatre jours destiné à préparer les personnes qui prévoient de passer l'examen Certified in Risk and Information System Controls™ (CRISC).
Le cours se concentre sur les points clés couverts dans le manuel de révision CRISC 7e édition et comprend des cours magistraux, des discussions de groupe, des exercices d'examen et des comptes rendus de réponses. Le cours s'adresse aux personnes ayant une connaissance et une expérience de l'informatique et de la gestion des risques d'entreprise.

Public visé:

Les participants qui cherchent à mieux comprendre l'impact des risques informatiques et la façon dont ils sont liés à leur organisation. Il s'adresse aux professionnels de l'audit, du risque et de la sécurité des TI/SI en milieu de carrière.

Objectifs pédagogiques:

- A l'issue de la formation, les participants seront capables de :
- Identifier la stratégie de gestion des risques informatiques à l'appui des objectifs commerciaux et de l'alignement avec la stratégie de gestion des risques d'entreprise (ERM).
- Analyser et évaluer les risques informatiques pour déterminer la probabilité et l'impact sur les objectifs de l'entreprise afin de permettre une prise de décision basée sur les risques.
- Déterminer les options de réponse aux risques et évaluer leur efficience et leur efficacité pour gérer les risques en conformité avec les objectifs commerciaux.
- Suivre en permanence les risques et les contrôles informatiques et en rendre compte aux parties prenantes concernées afin de garantir l'efficacité et l'efficience de la stratégie de gestion des risques informatiques et son alignement sur les objectifs commerciaux.

Pré-requis:

Il n'y a pas de conditions préalables pour passer l'examen CRISC ; cependant, pour obtenir la certification CRISC, vous devez remplir les conditions d'expérience requises par l'ISACA.

Test et certification

Cette formation prépare à la certification CRISC - Certified in Risk and Information Systems Control - examen passé ultérieurement. Frais d'examen en sus et démarche d'inscription auprès de l'ISACA à la charge du candidat sur :
https://www.isaca.org/credentialing/crisc/crisc-exam

Remarque : Trois années ou plus d'expérience en gestion des risques informatiques et en contrôle des SI. Aucune dispense ou substitution d'expérience

Contenu:

Cette mise à jour du programme de l'examen CRISC est basée sur les changements dans les pratiques de travail des professionnels du risque informatique ainsi que sur les dynamiques et les tendances du marché qui ont mis l'accent sur la gouvernance organisationnelle, la surveillance et le reporting continus des risques, la sécurité de l'information et la confidentialité des données pour une gestion efficace du risque informatique.

Ces énoncés et domaines sont le résultat de recherches approfondies et de validations de la part d'experts en matière de risques et de contrôles informatiques et d'éminents leaders du secteur dans le monde entier.

Vous trouverez ci-dessous les principaux domaines, sous-thèmes et tâches sur lesquels les candidats seront testés :

DOMAINE 1-Gouvernance 26%

GOUVERNANCE ORGANISATIONNELLE A

- Stratégie, buts et objectifs de l'organisation
- Structure, rôles et responsabilités de l'organisation
- Culture organisationnelle
- Politiques et normes
- Processus d'entreprise
- Actifs de l'organisation

GOUVERNANCE DES RISQUES B

- Gestion des risques de l'entreprise et cadre de gestion des risques
- Trois lignes de défense
- Profil de risques
- Appétence et tolérance aux risques
- Exigences légales, réglementaires et contractuelles
- Éthique professionnelle de la gestion des risques

DOMAINE 2-Évaluation des risques informatiques 20%

IDENTIFICATION DES RISQUES INFORMATIQUES A

- Événements à risque (par exemple, conditions contributives, perte de résultats)
- Modélisation et paysage des menaces
- Analyse de la vulnérabilité et des lacunes en matière de contrôle (par exemple, analyse des causes profondes)
- Développement de scénarios de risque

ANALYSE ET ÉVALUATION DES RISQUES INFORMATIQUES B

- Concepts, normes et cadres d'évaluation des risques
- Registre des risques
- Méthodologies d'analyse des risques
- Analyse de l'impact sur les affaires
- Risque inhérent et résiduel

DOMAINE 3 - Réponse aux risques et rapport 32%

RÉPONSE AU RISQUE A

- Traitement du risque / Options de réponse au risque
- Propriété des risques et des contrôles
- Gestion des risques par des tiers
- Gestion des problèmes, des constatations et des exceptions
- Gestion des risques émergents

CONCEPTION ET MISE EN ŒUVRE DU CONTRÔLE B

- Types, normes et cadres de contrôle
- Conception, sélection et analyse des contrôles
- Mise en œuvre des contrôles
- Test de contrôle et évaluation de l'efficacité

SUIVI DES RISQUES ET RAPPORTS C

- Plans de traitement des risques
- Collecte, agrégation, analyse et validation des données
- Techniques de suivi des risques et des contrôles
- Techniques de rapport sur les risques et les contrôles (cartes de pointage, tableaux de bord)
- Indicateurs clés de performance
- Indicateurs de risques clés (KRI)
- Indicateurs de contrôle clés (KCI)

DOMAINE 4 - Technologie et sécurité de l'information 22 %.

PRINCIPES DE TECHNOLOGIE DE L'INFORMATION A

- Architecture d'entreprises
- Gestion des opérations informatiques (par exemple, gestion du changement, actifs informatiques, problèmes, incidents)
- Gestion de projets
- Gestion de la reprise après sinistre (DRM)
- Gestion du cycle de vie des données
- Cycle de vie du développement des systèmes (SDLC)
- Technologies émergentes

PRINCIPES DE SÉCURITÉ DE L'INFORMATION B

- 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
- Classifications secondaires

Tâches de suivi

- Recueillir et examiner les informations existantes concernant les environnements commerciaux et informatiques de l'organisation.
- Identifier les impacts potentiels ou réels des risques informatiques sur les objectifs et les opérations de l'organisation.
- Identifier les menaces et les vulnérabilités des personnes, des processus et de la technologie de l'organisation.
- Évaluer les menaces, les vulnérabilités et les risques pour identifier les scénarios de risques informatiques.
- Établir la responsabilité en assignant et en validant les niveaux appropriés de risque et de propriété du contrôle.
- Établir et tenir à jour le registre des risques

informatiques, et l'intégrer au profil de risque de l'entreprise.
- Faciliter l'identification de l'appetence pour le risque et de la tolérance au risque par les principales parties prenantes.
- Promouvoir une culture consciente des risques en contribuant à l'élaboration et à la mise en œuvre d'une formation de sensibilisation à la sécurité.
- Effectuer une évaluation des risques en analysant les scénarios de risques informatiques et en déterminant leur probabilité et leur impact.
- Faire l'état des lieux des contrôles existants et évaluer leur efficacité pour l'atténuation des risques informatiques.
- Examiner les résultats de l'analyse des risques et de l'analyse des contrôles pour évaluer les écarts entre l'état actuel et l'état souhaité de l'environnement des risques informatiques.
- Faciliter la sélection des réponses recommandées aux risques par les principales parties prenantes.
- Collaborer avec les propriétaires de risques à l'élaboration de plans de traitement des risques.
- Collaborer avec les responsables des contrôles sur la sélection, la conception, la mise en œuvre et la maintenance des contrôles.
- Valider que les réponses aux risques ont été exécutées conformément aux plans de traitement des risques.
- Définir et établir des indicateurs clés de risque (KRI).
- Surveiller et analyser les indicateurs clés de risque (KRI).
- Collaborer avec les responsables des contrôles à l'identification des indicateurs clés de performance (KPI) et des indicateurs clés de contrôle (KCI).
- Suivre et analyser les indicateurs clés de performance (ICP) et les indicateurs clés de contrôle (ICC).
- Examiner les résultats des évaluations de contrôle pour déterminer l'efficacité et la maturité de l'environnement de contrôle.
- Communiquer les informations pertinentes sur les risques et les contrôles aux parties prenantes concernées afin de faciliter la prise de décision fondée sur les risques.
- Évaluer l'alignement des pratiques commerciales sur les normes de gestion des risques et de sécurité de l'information.

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• Modalités d'évaluation : le participant est invité à s'auto-évaluer par rapport aux objectifs énoncés.
• Chaque participant, à l'issue de la formation, répond à un questionnaire de satisfaction qui est ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.