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

Identifier, évaluer et répondre aux risques pour les atténuer

Présentiel ou en classe à distance

4 jours (28 h) | Prix inter : 3.250,00 € HT | Réf.: MG224

CRISC (Certified in Risk and Information Systems Control) est la seule certification permettant aux professionnels de l'informatique de relever les défis uniques de l'informatique et de la gestion des risques de l'organisation, en les positionnant pour qu'ils deviennent des partenaires stratégiques. Depuis sa création en 2010, près de 17 000 professionnels ont obtenu la certification CRISC, élue Gold Award du meilleur programme de certification professionnelle aux SC Magazine 2013 Awards. Cette formation est conçue pour couvrir l'intégralité du programme du CRISC et vous préparer à réussir l'examen.
Cette formation prépare à la certification Certified in Risk and Information Systems Control (CRISC).

A qui s'adresse cette formation ?

Pour qui

- Candidats à l'examen du CRISC, professionnels de l'informatique et des métiers ayant une expérience en gestion des risques d'au moins 3 à 5 ans

Prérequis

- Une expérience de base sur la gestion des risques est un plus pour suivre la formation
- Disposez-vous des connaissances nécessaires pour suivre cette formation ? Testez-vous !

Programme

1 - Introduction

2 - Réussir le CRISC

- Les prérequis pour la certification
- A propos de l'examen CGEIT
- Étapes pour la certification

3 - Domaine 1 : Identification des Risques TI

- Collecter et passer en revue les informations, y compris la documentation existante, concernant les environnements métier et informatiques, internes et externes de l'organisation afin d'identifier les impacts potentiels des risques informatiques sur les objectifs et les opérations de l'entité
- Identifier les menaces et vulnérabilités potentielles pour les personnes, les processus et la technologie de l'organisation afin de permettre l'analyse des risques informatiques
- Développer un ensemble complet de scénarios de risque informatique basés sur les informations disponibles pour déterminer l'impact potentiel sur les objectifs et les opérations de l'entité
- Identifier les principaux intervenants dans les scénarios de risque informatique pour aider à établir la responsabilité
- Établir un registre des risques informatiques pour avoir l'assurance que les scénarios de risques informatiques identifiés sont comptabilisés et intégrés dans le profil de risque de l'organisation
- Identifier l'appétit pour le risque et la tolérance définis par la direction et les principales parties prenantes afin de garantir l'alignement sur les objectifs de l'entité

- Collaborer à l'élaboration d'un programme de sensibilisation aux risques et organiser une formation pour s'assurer que les parties prenantes comprennent les risques et promouvoir une culture consciente des risques

4 - Domaine 2 : Évaluation des risques informatiques

- Analyser les scénarios de risque en fonction de critères organisationnels (structure organisationnelle, règles, normes, technologie, architecture, contrôles, etc.) afin de déterminer la probabilité et l'impact d'un risque identifié
- Identifier l'état actuel des contrôles existants et évaluer leur efficacité pour l'atténuation des risques informatiques
- Passer en revue les résultats de l'analyse des risques et des contrôles afin d'évaluer tout écart entre les états actuel et souhaité de l'environnement de risque informatique
- Obtenir l'assurance que la propriété des risques est attribuée au niveau approprié pour établir des lignes de responsabilité claires
- Communiquer les résultats des évaluations des risques à la haute direction et aux parties prenantes appropriées pour permettre une prise de décision basée sur les risques
- Mettre à jour le registre des risques avec les résultats de l'évaluation des risques

5 - Domaine 3 : Réponse aux risques et atténuation

- Consulter les responsables des risques pour sélectionner et aligner les réponses au risque recommandées sur les objectifs de l'organisation et permettre une prise de décision en connaissance de cause
- Consulter les responsables des risques ou les aider à prendre en charge l'élaboration de plans d'action pour faire en sorte que les plans incluent des éléments clés (par exemple, la réponse, le coût, la date cible)
- Consulter sur la conception et la mise en oeuvre ou l'ajustement des contrôles d'atténuation pour s'assurer que le risque est géré à un niveau acceptable
- Obtenir l'assurance que la propriété du contrôle est attribuée afin d'établir des lignes de responsabilité claires
- Assister les propriétaires de contrôle dans le développement de procédures de contrôle et de la documentation afin de permettre une exécution efficace du contrôle
- Mettre à jour le registre des risques afin de refléter les changements dans les risques et la réponse des risques de la direction
- Valider que les réponses aux risques ont été exécutées conformément aux plans d'action des risques

6 - Domaine 4 : Surveillance des risques et des contrôles

- Définir et établir des indicateurs clés de risque (KRI) et des seuils basés sur les données disponibles, afin de permettre le suivi de l'évolution du risque
- Surveiller et analyser les indicateurs de risque clés (KRI) pour identifier les changements ou les tendances du profil de risque informatique
- Rendre compte des changements ou des tendances liés au profil de risque informatique afin d'aider la direction et les parties prenantes concernées à prendre des décisions
- Faciliter l'identification des métriques et des indicateurs de performance clés (KPI) afin de permettre la mesure de la performance du contrôle
- Surveiller et analyser les indicateurs de performance clés (KPI) afin d'identifier les changements ou les tendances liés à l'environnement de contrôle et de déterminer l'efficience et l'efficacité des contrôles
- Passer en revue les résultats des évaluations de contrôle pour déterminer l'efficacité de l'environnement de contrôle
- Rendre compte de la performance, des changements ou des tendances du profil de risque global et de l'environnement de contrôle aux parties prenantes concernées pour permettre la prise de décision

7 - Administration et techniques pour l'examen

- Administration de l'examen
- Techniques pour l'examen
- Questions fréquentes

8 - Examen blanc

9 - Questions et conclusion

Les objectifs de la formation

- Connaître les exigences spécifiques liées à la réussite de l'examen et à l'obtention de la certification
- Pouvoir comprendre les concepts clés, les tâches et la connaissance d'un professionnel de la gestion des risques qui servent de bases à l'examen CRISC
- Découvrir les méthodes efficaces pour évaluer les questions d'examen et les réponses, y compris l'analyse et les explications
- Connaître les informations utiles sur la préparation et la gestion du temps à l'examen

Evaluation

- Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.

Les points forts de la formation

- Formation accréditée par ISACA et animée par un formateur accrédité par ISACA pour les ateliers de préparation au CRISC.
- Manuel officiel de préparation au CRISC fourni dans le cadre de la session, au format électronique.
- Copie intégrale des slides de présentation (ISACA) utilisées par votre formateur pendant la formation (au format électronique).
- En option au prix de 400 euros : Un pack de préparation à l'examen incluant le manuel officiel de l'ISACA et l'accès à la base officielle de questions pour une durée de 12 mois.
- L'inscription à l'examen se fait directement auprès de l'ISACA par le candidat avec son dossier https://www.isaca.org/credentialing/crisc/crisc-exam. L'examen se déroule sur 4 heures. Il est en anglais et comporte 150 questions à choix multiples.
- Les frais d'inscription à l'examen ne sont pas compris dans le prix de la formation.
- 90% des participants à cette formation se sont déclarés satisfaits ou très satisfaits au cours des 12 derniers mois.

Dates et villes 2026 - Référence MG224

Dernières places disponibles Session garantie

Lille

du 23 mars au 26 mars	du 26 mai au 29 mai	du 28 sept. au 1 oct.

A distance

du 23 mars au 26 mars	du 20 juil. au 23 juil.	du 30 nov. au 3 déc.
du 26 mai au 29 mai	du 28 sept. au 1 oct.	

Nantes

du 23 mars au 26 mars	du 20 juil. au 23 juil.	du 30 nov. au 3 déc.

Paris

du 23 mars au 26 mars	du 20 juil. au 23 juil.	du 30 nov. au 3 déc.
du 26 mai au 29 mai	du 28 sept. au 1 oct.	

Marseille

du 23 mars au 26 mars	du 26 mai au 29 mai	du 28 sept. au 1 oct.

Rennes

du 23 mars au 26 mars	du 20 juil. au 23 juil.	du 30 nov. au 3 déc.

Aix-en-Provence

du 23 mars au 26 mars	du 26 mai au 29 mai	du 28 sept. au 1 oct.

Toulouse

du 23 mars au 26 mars	du 20 juil. au 23 juil.	du 28 sept. au 1 oct.

Sophia Antipolis

du 26 mai au 29 mai	du 28 sept. au 1 oct.	du 30 nov. au 3 déc.

Bordeaux

du 26 mai au 29 mai	du 20 juil. au 23 juil.	du 30 nov. au 3 déc.

Rouen

du 26 mai au 29 mai	du 28 sept. au 1 oct.	du 30 nov. au 3 déc.

Lyon

du 26 mai au 29 mai	du 20 juil. au 23 juil.	du 30 nov. au 3 déc.

Strasbourg

du 26 mai au 29 mai	du 28 sept. au 1 oct.	du 30 nov. au 3 déc.