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

Identifier, évaluer et répondre aux risques pour les atténuer

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

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'entreprise, 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.

Référence	CRISC
Durée	4 jours (28h)
Tarif	3 150 €HT
Certification	- €HT

Objectifs

| 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.

Public

| 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

Programme de la formation

Introduction
Réussir le CRISC
| Les prérequis pour la certification
| A propos de l'examen CGEIT
| Étapes pour la certification

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'entreprise
| Identifier les menaces et vulnérabilités potentielles pour les personnes, les processus et la technologie de l'entreprise afin de permettre l'analyse des risques

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)
- du 15 au 18 septembre 2025
- du 24 au 27 novembre 2025

PARIS
- du 15 au 18 septembre 2025
- du 24 au 27 novembre 2025

AIX-EN-PROVENCE
- du 15 au 18 septembre 2025
- du 24 au 27 novembre 2025

BORDEAUX
- du 24 au 27 novembre 2025

GRENOBLE
- du 24 au 27 novembre 2025

LILLE
- du 24 au 27 novembre 2025

LYON
- du 24 au 27 novembre 2025

NANTES
- du 15 au 18 septembre 2025
- du 24 au 27 novembre 2025

RENNES
- du 15 au 18 septembre 2025
- du 24 au 27 novembre 2025

VOIR TOUTES LES DATES

HUB Formation - 14 avenue de l'Opéra - 75001 Paris
01 85 77 07 07 - www.hubformation.com - SIREN 525 287 785

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'entreprise
| 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'entreprise
| 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'entreprise
| 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

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

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'entreprise 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

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

Administration et techniques pour l'examen
| Administration de l'examen
| Techniques pour l'examen
| Questions fréquentes

Examen blanc
Questions et conclusion
| 9.1)

Certification

HUB Formation - 14 avenue de l'Opéra - 75001 Paris
01 85 77 07 07 - www.hubformation.com - SIREN 525 287 785

Cette formation prépare au passage de la certification suivante.
N'hésitez pas à nous contacter pour toute information complémentaire.

Risk and Information Systems Control
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.
Les formations préparant à l'examen sont animées par un formateur accrédité par ISACA pour les ateliers de préparation au CRISC.
Le manuel officiel de préparation au CRISC, au format électronique, est fourni pendant la formation.

| Durée : 4h00
| QCM de 150 questions

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.