CYBERSÉCURITÉ

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

4 jours (28h00) | CYB0012 | Num form : form-242 | Perfectionnement / Avancé

INFORMATIQUE / SÉCURITÉ IT / CYBERSÉCURITÉ

À l'issue de ce stage vous serez capable de :

- 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

Niveau requis :

- Une expérience de base sur la gestion des risques est un plus pour suivre la formation

Public concerné :

- 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

Programme :

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 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