CISA®, Certified Information Systems Auditor® + Practice Questions

Durée: 5 Jours **Réf de cours: CISAU** **Méthodes d'apprentissage: Intra-entreprise & sur-mesure**

Résumé:

CISA® - Certified Information Systems Auditor est mondialement reconnu pour l'audit, le contrôle et l'assurance des systèmes d'information, demandé et apprécié par les plus grandes marques mondiales. Il s'agit souvent d'une qualification obligatoire pour travailler en tant qu'auditeur informatique. Les professionnels CISA offrent la crédibilité nécessaire pour exploiter les normes, gérer les vulnérabilités, assurer la conformité, proposer des solutions, mettre en place des contrôles et apporter de la valeur aux organisations.
Cette formation CISA de 5 jours est une préparation à la certification CISA. Pendant cette formation, les partiicpants apprendront le processus d'audit informatique. Formation professionnelle continue (FPC) : 31. Questions pratiques (QAE = Questions, Réponses et Explications) : Accès pour 12 mois

Public visé:

Conçu pour les professionnels de l'audit, du contrôle et de l'assurance des systèmes d'information en milieu de carrière qui cherchent à développer leur carrière :Directeurs/managers/consultants en audit informatique Auditeurs informatiques Directeurs de la conformité, des risques et de la protection de la vie privée Directeurs/managers/consultants en informatique
Les grands rôles des CISA sont : Réduire les risques : Les CISA garantissent que les systèmes informatiques et commerciaux de l'organisation sont contrôlés, gérés et protégés de manière efficace. Créer un langage commun : Les CISA jouent le rôle de conseillers de confiance en s'assurant que le leadership, les structures organisationnelles et les processus nécessaires sont en place pour atteindre les objectifs commerciaux et soutenir la stratégie de l'entreprise. Favoriser la réussite de l'entreprise : Les régulateurs et les clients recherchent le titre de CISA et de nombreuses entreprises et agences gouvernementales l'exigent. Être prêt à déployer des contrôles préventifs : Des études ont montré que les entreprises perdent jusqu'à 5 % de leur chiffre d'affaires annuel en raison de fraudes et d'irrégularités. Cette réalité incite les dirigeants à embaucher des CISA pour mettre en œuvre des contrôles préventifs et fournir une assurance sur la sécurité de l'information et la gestion des risques..

Objectifs pédagogiques:

- A l'issue de la formation, les participants seront capables de :
- Appréhender les domaines sur lesquels porte la certification CISA®
- Décrire et comprendre lles concepts liés à l'audit du Système d'information
- Préparer l'examen de certification CISA, Auditeur Sécurité certifié ISACA

Pré-requis:

Il n'y a pas de conditions d'admission spécifiques pour participer à cette formation

Test et certification

- Cette formation prépare à la certification CISA, Auditeur Sécurité certifié ISACA
- ?Le bon d'examen n'est pas inclus dans le prix de la formation.
- 4 heures (240 minutes),150 questions à choix multiples. Outre la réussite de l'examen, des conditions supplémentaires sont requises pour l'obtention du certificat. Celles-ci peuvent être consultées à l'adresse suivante : https://www.isaca.org/credentialing/cisa/get-cisa-certified

Après cette formation, nous vous conseillons le(s) module(s) suivant(s):

CISSP Certification Preparation

Contenu:

Domaine 1- Processus d'audit des systèmes d'information

Planification

- Normes, lignes directrices et codes de déontologie en matière d'audit des SI
- Processus d'affaires
- Types de contrôles
- Planification de l'audit basée sur le risque
- Types d'audits et d'évaluations

Exécution

- Gestion du projet d'audit
- Méthodologie d'échantillonnage
- Techniques de collecte des preuves d'audit
- Analyse des données
- Techniques d'établissement de rapports et de communication
- Assurance qualité et amélioration du processus d'audit

Domaine 2 - Gouvernance et gestion des technologies de l'information

Gouvernance informatique

- Gouvernance informatique et stratégie informatique
- Cadres liés à l'informatique
- Normes, politiques et procédures informatiques
- Structure organisationnelle
- Architecture d'entreprise
- Gestion des risques de l'entreprise
- Modèles de maturité
- Lois, règlements et normes industrielles affectant l'organisation

Gestion des technologies de l'information

- Gestion des ressources informatiques
- Acquisition et gestion des fournisseurs de services informatiques
- Contrôle des performances informatiques et établissement de rapports
- Assurance et gestion de la qualité des technologies de l'information

Domaine 3 - Acquisition, développement et mise en œuvre des systèmes d'information ?

Acquisition et développement de systèmes d'information

- Gouvernance et gestion des projets
- Analyse de rentabilité et de faisabilité
- Méthodologies de développement des systèmes
- Identification et conception des contrôles

Mise en œuvre des systèmes d'information

- Méthodologies de test
- Gestion de la configuration et des versions
- Migration des systèmes, déploiement de l'infrastructure et conversion des données
- Revue post-implémentation

Domaine 4 - Exploitation des systèmes d'informtion et résilience de l'entreprise

Exploitation des systèmes d'information

- Composants technologiques communs
- Gestion des actifs informatiques
- Planification des tâches et automatisation des processus de production
- Interfaces de systèmes
- Informatique pour l'utilisateur final
- Gouvernance des données
- Gestion des performances des systèmes
- Gestion des problèmes et des incidents
- Gestion des changements, des configurations, des versions et des correctifs
- Gestion des niveaux de service informatique
- Gestion des bases de données

Résilience des entreprises

- Analyse d'impact sur les activités (BIA)
- Résilience des systèmes
- Sauvegarde, stockage et restauration des données
- Plan de continuité des activités (BCP)
- Plans de reprise après sinistre (DRP)??

Domaine 5 - Protection des actifs informationnels

Sécurité et contrôle du patrimoine informationnel

- Cadres, normes et lignes directrices en matière de sécurité du patrimoine informationnel
- Principes de protection de la vie privée
- Contrôles de l'accès physique et de l'environnement
- Gestion des identités et des accès
- Sécurité des réseaux et des points finaux

Classification des données

- Chiffrement des données et techniques liées au chiffrement
- Infrastructure à clé publique (PKI)
- Techniques de communication basées sur le web
- Environnements virtualisés
- Dispositifs mobiles, sans fil et Internet des objets (IoT)

Gestion des événements de sécurité

- Formation et programmes de sensibilisation à la sécurité
- Méthodes et techniques d'attaque des systèmes d'information
- Outils et techniques de test de sécurité
- Outils et techniques de contrôle de la sécurité
- Gestion des réponses aux incidents
- Collecte de preuves et criminalistique

Méthodes pédagogiques :

Les participants réalisent un test d'évaluation des connaissances en amont et en aval de la formation pour valider les connaissances acquises pendant la formation.
Support de cours officiel remis aux participants

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.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement