

Durée : 5 jours

Depuis 1978, le CISA (Certified Information System Auditor) est considéré comme la norme mondiale pour les professionnels de l'audit, du contrôle et de la sécurité des systèmes d'information (SI). Les compétences techniques et les pratiques que le CISA promeut et évalue sont la pierre angulaire du succès sur le terrain. Ce cours de 5 jours permet aux participants d'acquérir les compétences et les connaissances attendues d'un professionnel de l'audit, du contrôle et de la sécurité des systèmes d'information de classe mondiale.

Audience

Ce cours s'adresse aux candidats à l'examen du CISA ayant une expérience en Audit des Systèmes d'Information d'au moins 3 à 5 ans.

Objectifs

A la fin de cette session, les participants comprendront :

- Les exigences spécifiques liées à la réussite de l'examen et à l'obtention de la certification,
- Les concepts clés, les tâches et la connaissance d'un auditeur des systèmes d'information qui servent de bases à l'examen CISA et qui s'alignent sur les domaines suivants :
 - Le processus de vérification des systèmes d'information,
 - La gouvernance et le management des TI,
 - L'acquisition, le développement et la mise en œuvre des systèmes d'information,
 - L'exploitation des systèmes d'information, la maintenance et la gestion des services,
 - La protection des actifs informationnels
- Les méthodes efficaces pour évaluer les questions d'examen et les réponses, y compris l'analyse et les explications,
- Les informations utiles sur la préparation et la gestion du temps à l'examen.

Contenu du cours

1. Bienvenue & Introduction

2. Réussir le CISA

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

3. Domaine 1 : Processus d'audit du SI

- **Planification**
 - Normes, directives et codes d'éthique relatif à l'audit du SI
 - Processus métiers
 - Types de contrôles
 - Planification de l'audit basée sur les risques
 - Types d'audit et d'évaluation
- **Exécution**
 - Gestion de projet d'un audit
 - Méthode d'échantillonnage
 - Techniques de collecte d'évidences
 - Analyse des données
 - Rapports et communication

- Assurance qualité et amélioration du processus d'audit

4. Domaine 2 : Gouvernance et Management des TI

- **Gouvernance et stratégie informatique**
 - Cadres pour l'informatique
 - Normes, politiques et procédures pour les TI
 - Structures organisationnelles
 - L'architecture d'entreprise
 - La gestion du risque d'entreprise
 - Modèles de maturité
 - Lois, réglementations et normes
- **Management des TI**
 - Gestion des ressources informatiques
 - Acquisition et gestion des fournisseurs
 - Surveillance des performances informatiques et rapports
 - Assurance qualité et gestion de la qualité des services TI

5. Domaine 3 : Acquisition, développement et mise en œuvre des SI

• **Acquisition et développement des SI**

- Gouvernance et gestion de projet
- Cas d'affaire et analyse de faisabilité
- Méthodologies de développement de systèmes
- Identification et conception des contrôles
- **Mise en œuvre des SI**
 - Méthodologies de test
 - Gestion des configurations et des versions
 - Migration de systèmes, déploiement d'infrastructures et conversion de données
 - Revue post-implémentation

6. Domaine 4 : Opérations informatiques et résilience métier

- **Exploitation des systèmes d'information**
 - Composants technologiques communs
 - Gestion des actifs informatiques
 - Automatisation des processus de planification et de production
 - Interfaces système
 - Informatique utilisateur
 - Gouvernance des données

- Gestion de la performance 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 métiers**
 - Analyse de l'impact métier
 - Résilience du système
 - Sauvegarde, stockage et restauration des données
 - Plan de continuité d'activité
 - Plan de reprise après sinistre
- 7. Domaine 5 : Protection des actifs informationnels**
- **Cadres, normes et directives des sécurité des actifs informationnels**
 - Principe de confidentialité
 - Accès physique et contrôles environnementaux
 - Gestion des identités et des accès
 - Sécurité des réseaux et des terminaux
 - Classification des données
 - Chiffrement des données et techniques liées au chiffrement
 - Infrastructure à clé publique
 - Technologies de communication basées sur le web
 - Environnements virtualisés
 - Dispositifs mobiles, sans fil et internet
 - **Gestion des événements de sécurité**
 - Programmes et formations 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 surveillance de la sécurité
 - Gestion de la réponse aux incidents
 - Collecte de preuves et investigations technico-légales
- 8. Administration et techniques pour l'examen**
- Administration de l'examen
 - Techniques pour l'examen
 - Questions fréquentes
- 9. Examen blanc**
- 10. Questions & Conclusion**

Les plus de cette session :



Formation accréditée par ISACA et animée par un formateur accrédité par ISACA pour les ateliers de préparation au CISA



Manuel officiel de préparation au CISA fourni dans le cadre de la session, au format électronique

Abonnement à la base officielle de questions pour une durée de 12 mois fourni dans le cadre de la session

Copie intégrale des slides de présentation utilisées pendant la formation par votre formateur (au format électronique)

Voucher permettant de passer l'examen dans un centre PSI dans les 12 mois suivant la formation.