Cybersecurity Audit Certificate

Durée : 2 Jours

Ce n'est pas seulement le coût élevé pour une organisation en cas de violation, mais aussi le caractère inévitable d'une attaque qui rend la cybersécurité essentielle. Avec le nombre croissant de cyber-menaces, il est essentiel que le plan d'audit de chaque organisation intègre la cybersécurité. Par conséquent, les auditeurs sont de plus en plus tenus de vérifier les processus, les politiques et les outils de cybersécurité afin de garantir que leur entreprise dispose des contrôles appropriés. Les vulnérabilités en matière de cybersécurité peuvent représenter des risques graves pour l'ensemble de l'organisation, rendant le besoin d'auditeurs informatiques parfaitement familiarisés avec l'audit en cybersécurité plus grand que jamais.

Le nouveau programme de certification en audit de cybersécurité de l'ISACA fournit aux professionnels de l'audit et de la vérification les connaissances nécessaires pour exceller dans les audits de cybersécurité. Il apporte aux professionnels de la sécurité une meilleure compréhension du processus d'audit et aux professionnels des risques informatiques une compréhension des cyber-risques et des contrôles d'atténuation.

Audience

Le programme de certification en audit de cybersécurité s'adresse spécifiquement aux :

- Professionnels de l'audit informatique et aux entreprises ayant besoin de conseils supplémentaires en matière d'audit de cybersécurité,
- Professionnels de la sécurité qui ont besoin de mieux comprendre le processus d'audit,
- Professionnels du risque et de l'assurance qui ont besoin d'une connaissance approfondie des cyber-risques et des contrôles d'atténuation appropriés.

Objectifs

A l'issue de cette session de deux jours, les participants seront capables de :

- Comprendre les cadres de sécurité pour identifier les meilleures pratiques,
- Définir la gestion des menaces et des vulnérabilités,
- Évaluer les menaces à l'aide d'outils de gestion des vulnérabilités,
- Construire et déployer des processus d'autorisation sécurisés,
- Expliquer tous les aspects de la gouvernance de la cybersécurité,
- Distinguer les technologies de pare-feu et de sécurité réseau,
- Améliorer les pratiques de gestion des actifs, des configurations, des changements et des correctifs,
- Gérer les identités et les accès aux informations de l'entreprise,
- Identifier les contrôles de sécurité des applications,
- Identifier les exigences réglementaires cyber et légales pour faciliter les évaluations de conformité,
- Identifier les faiblesses des stratégies et des contrôles liés au Cloud,
- Effectuer des évaluations de la cybersécurité et des évaluations externes des risques,
- Identifier les avantages et les risques de la conteneurisation.

Contenu du cours

1. Bienvenue & Présentations

2. Module 1 : Introduction

- Protection des actifs numériques,
- Lignes de défense,
- Rôle de l'Audit,
- Objectifs de l'audit,
- Périmètre de l'audit.

3. Module 2 : Gouvernance de la cybersécurité

- Rôles et responsabilités en matière de cybersécurité,
- Cadres de sécurité,
- Buts et objectifs de l'organisation de la sécurité,
- Politique et normes de cybersécurité,
- Exigences Cyber et légales / réglementaires,
- Classification des actifs informationnels,
- Assurance en matière de cybersécurité,
- Évaluation des risques de cybersécurité,
- Sensibilisation à la cybersécurité,
- Médias sociaux - Risques et contrôles,
- Évaluation par une tierce partie,
- Les fournisseurs de services,
- Gestion des risques de la chaîne d'approvisionnement,
- Mesure de performance.

Cybersecurity Audit Certificate

4. Module 3 : Opérations de cybersécurité

- Concepts et Définitions,
- Gestion des menaces et des vulnérabilités,
- Gestion des identités et des accès aux informations de l'entreprise,
- Gestion des configurations et des actifs,
- Gestion des changements,
- Gestion des correctifs,
- Sécurité réseau,
- Création et déploiement de processus d'autorisation sécurisé pour les technologies de l'information,
- Gestion des incidents,
- Protection des points d'accès client,
- Sécurité des applications,
- Sauvegarde et restauration des données,
- Conformité de la sécurité,
- Cryptographie.

5. Module 4 : Sujets sur la technologie de cybersécurité

- Technologies de pare-feu et de sécurité réseau,
- Gestion des incidents de sécurité et des évènements (SIEM),
- Technologie sans fil,
- L'infonuagique,
- Sécurité mobile,
- Internet des objets (IoT),
- Sécurité de la virtualisation,
- Systèmes de contrôle industriels (ICS).

6. Questions et Conclusion

Les plus de cette session :

- Formation accréditée par ISACA et animée par un formateur accrédité par ISACA pour les ateliers de préparation du programme Cybersecurity Audit Certificate.
- Manuel officiel de préparation au programme de certification Cybersecurity Audit fourni dans le cadre de la session, au format électronique
- Copie intégrale des slides de présentation utilisées par votre formateur pendant la formation (au format électronique)
- Voucher permettant de passer l'examen en ligne dans les 12 mois suivant la formation.