DIGITAL ACT® ACADEMY

CISSP®

Certified Information Systems Security Professional

1. Présentation

Géré par **(ISC)²** -International **I**nformation **S**ystems **S**ecurity **C**ertification **C**onsortium-, la certification **CISSP®** -**C**ertified **I**nformation **S**ystems **S**ecurity **P**rofessional- est historiquement, une des premières certifications de cybersécurité car elle a vu le jour aux États-Unis, au début des années 1990.

Désignée comme la meilleure certification au monde en cybersécurité par FORBES en 2019, le CISSP® est l'une des certifications les plus difficiles au monde à obtenir. Début 2020, le CISSP® est reconnu comme un mastère en cybersécurité, à date, il s'agit de la seule certification au monde en cybersécurité à avoir reçu ce niveau de reconnaissance.

A travers une session de cinq (5) jours, les candidat(e)s se prépareront à la certification CISSP® en approfondissant ses compétences, tant au niveau technique qu'au niveau de l'analyse des risques et de l'audit des systèmes dans une optique de gouvernance des systèmes d'information.

2. Objectifs

- Appréhender les exigences liées à la réussite de l'examen ;
- Appliquer les méthodes liées aux domaines des technologies de l'information et de la sécurité ;
- Aligner les objectifs opérationnels de l'organisation avec les fonctions de sécurité ;
- Déterminer comment protéger les actifs de l'organisation tout au long de leur cycle de vie ;
- Tirer parti des concepts et normes pour concevoir, mettre en œuvre, surveiller et sécuriser l'IT afin d'appliquer divers niveaux de confidentialité, d'intégrité et de disponibilité ;
- Appliquer les principes de conception de la sécurité pour sélectionner les mesures d'atténuation ;
- Expliquer l'importance de la cryptographie et les services de sécurité à l'ère du digital ;
- Évaluer les éléments de sécurité physique par rapport aux besoins de sécurité de l'information ;
- Évaluer les éléments qui composent la communication et la sécurité par rapport aux besoins ;
- Tirer parti des concepts et de l'architecture qui définissent la technologie associée ;
- Déterminer les modèles de contrôle d'accès pour répondre aux exigences de sécurité ;
- Appliquer des contrôles d'accès pour répondre aux besoins de sécurité des informations ;
- Différencier les principales méthodes de stratégies de test et d'audit ;
- Appliquer des contrôles de sécurité et des contre-mesures appropriés ;
- Évaluer les risques des systèmes d'information pour les efforts opérationnels d'une organisation ;
- Déterminer les contrôles appropriés pour atténuer les menaces et vulnérabilités spécifiques ;
- Appliquer les concepts de sécurité des systèmes d'information pour atténuer le risque de vulnérabilités des logiciels et des systèmes.

3. Public cible

Cette formation s'adresse aux professionnels impliqués dans la sécurité de l'information, nous pouvons citer parmi eux : directeur des systèmes d'information, directeur de la sécurité de l'information, directeur de la technologie, directeur de la sécurité, responsable de la sécurité de l'information, consultants.

4. Durée

05 jours

5. Prérequis

Pour suivre cette formation, il est recommandé que les candidat(e)s disposent d'une expérience professionnelle dans au moins 2, des 8 domaines du CBK® -Common Body of Knowledge-.

Sur le plan technique, il est recommandé d'avoir des connaissances de base sur les réseaux et les systèmes d'exploitation ainsi qu'en sécurité de l'information.

Sur le plan fonctionnel, il est recommandé d'avoir des connaissances de base autour des normes en audit et en continuité des activités business.

6. Certification

L'examen CISSP® est inclus dans le coût de la formation et est disponible en huit (8) langues, dont le français. Un voucher électronique sera remis aux candidat(e)s afin de s'enregistrer en ligne sur le portail de (ISC)².

L'examen a une durée de trois (3) heures et se décline en un QCM de 100-150 couvrant les huit domaines suivants du CBK® :

Domaine 1 : Gestion de la sécurité et des risques pour 15%
Domaine 2 : La sécurité des actifs informationnels pour 10%
Domaine 3 : Ingénierie de la sécurité pour 13%
Domaine 4 : Sécurité des réseaux et des communications pour 13%
Domaine 5 : Gestion des identités et des accès pour 13%
Domaine 6 : Évaluation de la sécurité et tests pour 12%
Domaine 7 : Sécurité opérationnelle pour 13%
Domaine 8 : Sécurité du développement logiciel pour 11%

Il est à noter que les candidat(e)s devront passer leur examen dans un centre agréé Pearson Vue.

7 Programme

Domaine 1 Gestion de la sécurité et des risques -15%-

Domaine 2 La sécurité des actifs informationnels -10%-

Domaine 3 Ingénierie de la sécurité -13%-

Domaine 4 Sécurité des réseaux et des communications -13%-

Domaine 5 Gestion des identités et des accès -13%-

Domaine 6 Évaluation de la sécurité et des tests -12%-

Domaine 7 Sécurité opérationnelle -13%-

Domaine 8 Sécurité du développement logiciel -11%-

Examen blanc

Conclusion