# FORMATION

# CISSP (Certified Information Systems Security Professional),

## Hôtel « NOVOTEL Mohamed V» Tunis
## Du 9 au 13 Mai 2022

**Introduction**

La formation couvre l'ensemble des 8 domaines du CBK (Common Body of Knowledge), tronc commun de connaissances en sécurité défini par ISC2®. Le CBK inclus les connaissances en sécurité de l'information dans les huit domaines suivants : Sécurité et management des risques, Sécurité des actifs, Engineering de la sécurité, Sécurité des réseaux et des communications, Management des identités et des accès, Evaluation de la sécurité et test, Sécurité des opérations, Sécurité du développement logiciel.

**Objectifs de la Formation**

- Maîtriser les connaissances en sécurité de l'information dans les huit domaines du CBK,
- Comprendre les besoins en sécurité de l'information pour toute l'organisation,
- Acquérir les connaissances nécessaires pour conseiller une organisation sur les meilleures pratiques en management de la sécurité de l'information.

**Participants :**

Auditeurs confirmés ou informaticiens (DSI, RSSI, Managers, Ingénieurs, Experts de la sécurité et Consultants) qui souhaitent obtenir la certification CISSP (Certified Information System Security Professional) délivrée par l'ISC2, et préparer l'examen.

**Pré -requis :**

- Une expérience dans le domaine des réseaux et de la sécurité,
- La compréhension de l'anglais technique est nécessaire car le support de cours fourni aux participants est en anglais

**Bénéfices attendus de la formation :**

- Reconnaissance Internationale des compétences en sécurité de l'information,
- Savoir dialoguer avec le management pour la mise en œuvre des mesures de sécurité,
- Appréhender le rôle du RSSI dans l'organisation.

**Mode:** Formation inter – entreprises.

**Programme:** Le programme du séminaire suit les 8 domaines définis pour l'examen :

**Jour 1** :

- Domaine 1 : **Sécurité et management des risques**

  - Comprendre et appliquer les concepts de confidentialité, intégrité et disponibilité
  - Appliquer les principes de gouvernance de la sécurité
  - Conformité
  - Comprendre les questions légales et réglementaires concernant la sécurité de l'information dans un contexte global
  - Comprendre l'éthique professionnelle
  - Développer et implémenter une politique de sécurité, des standards, des procédures et des guidelines

- Comprendre les exigences de continuité d'activité
- Contribuer aux politiques de sécurité du personnel
- Comprendre et appliquer les concepts de management des risques
- Comprendre et appliquer le modèle de menace
- Intégrer les considérations de risque de sécurité dans la stratégie d'acquisition
- Etablir et gérer la sensibilisation, la formation et l'éducation à la sécurité de l'information

- Domaine 2 : **Sécurité des actifs**

- Classification de l'information et support des actifs
- Déterminer et maintenir la propriété
- Protéger la confidentialité
- Assurer la rétention appropriée
- Déterminer les mesures de sécurité des données
- Etablir les exigences de manipulation

**Jour 2** :

- Domaine 3 : **Engineering de la sécurité**

- Implémenter et gérer les processus d'engineering en utilisant les principes de conception sécurisée
- Comprendre les concepts fondamentaux des modèles de sécurité
- Sélectionner les mesures et contre-mesures sur la base des modèles d'évaluation de la sécurité des systèmes
- Comprendre les possibilités de sécurités offertes par les systèmes d'information
- Evaluer et réduire les vulnérabilités de sécurité des architectures, des conceptions, des solutions
- Evaluer et réduire les vulnérabilités de sécurité des systèmes web
- Evaluer et réduire les vulnérabilités de sécurité des systèmes mobiles
- Evaluer et réduire les vulnérabilités de sécurité des systèmes embarqués
- Appliquer la cryptographie
- Appliquer les principes de sécurité au site et à la conception de l'installation
- Concevoir et implémenter la sécurité physique

- Domaine 4 : **Sécurité des réseaux et des communications**

- Appliquer les principes de conception sécurisée à l'architecture réseau
- Sécuriser les composants réseau
- Concevoir et établir des canaux de communication sécurisés
- Prévenir ou limiter les attaques réseau

**Jour 3** :

- Domaine 5 : **Management des identités et des accès**

- Contrôle d'accès physique et logique aux actifs
- Gérer l'identification et l'authentification des personnes et des équipements
- Intégrer l'identité en tant que service

- Intégrer des services d'identité tiers
- Intégrer et gérer les mécanismes d'autorisation
- Prévenir ou réduire les attaques au contrôle d'accès
- Gérer le cycle de vie des identités et du provisioning des accès

- Domaine 6 : **Evaluation de la sécurité et test**

- Concevoir et valider les stratégies d'évaluation et de test de sécurité
- Conduire des tests de mesures de sécurité
- Collecter les données des processus de sécurité
- Analyser et reporter les résultats des tests
- Conduire ou faciliter les audits internes ou third-party

**Jour 4** :

- Domaine 7 : **Sécurité des opérations**

- Comprendre et supporter les investigations
- Comprendre les exigences des types d'investigations
- Réaliser les activités de monitoring et de logging
- Sécuriser le provisioning des ressources
- Comprendre et appliquer les concepts fondamentaux de sécurité des opérations
- Utiliser les techniques de protection de ressources
- Gérer les incidents
- Opérer et maintenir des mesures de sécurité préventives
- Implémenter et supporter le management des patchs et vulnérabilités
- Comprendre et participer aux processus de gestion des changements
- Implémenter des stratégies de reprise
- Implémenter des stratégies de reprise après sinistre
- Tester les plans de reprise après sinistre
- Participer au Plan de Continuité d'Activité et aux exercices
- Implémenter et manager la sécurité physique
- Adresser les problèmes de sécurité du personnel

**Jour 5** :

- Domaine 8 : **Sécurité du développement logiciel**

- Comprendre et appliquer la sécurité dans le cycle de vie de développement logiciel
- Appliquer les mesures de sécurité dans les environnements de développement
- Evaluer l'efficacité de la sécurité du logiciel
- Evaluer l'impact la sécurité du logiciel acquis

Dans chaque exposé, l'accent sera mis sur les éléments organisationnels et technologiques fondamentaux.

**Méthode :**

- Ensemble d'exposés couvrant chaque domaine du programme de l'examen,

- A la fin de chaque exposé, les participants doivent s'entraîner à répondre à un ensemble de questions portant sur le thème de l'exposé. Ces questions sont issues des précédentes sessions du CISSP (ou d'examens comparables),
- Simulation partielle de l'examen (examen blanc) effectuée en fin de formation.

## Formateur

Sofiane CHAFFAI, de Nationalité Algérienne, Ingénieur en electronique de formation et spécialiste en sécurité de l'information et en gestion des risques. Il travaille en tant que consultant auditeur GRC. Sofiane est certifié CISSP, CISA, Prince2, et ISO 27001 LA & LI. Il est certifié trainer auprès de PECB et ISC2 et est membre du conseil consultatif de ISC2 EMEA ; il participe au développement du programme du chapitre.

## Examen :

Depuis avril 2018, l'examen CISSP en ligne (CAT : *computerized adaptive testing*) est disponible pour tous les examens en anglais. Dans les autres langues, les examens CISSP sont gérés de façon linéaire et fixe. Le passage de l'examen a lieu dans un centre de test Pearson Vue.

***Examen en langue anglaise***

- Durée : 3 heures
- Nombre de questions : entre 100 et 150 questions (le nombre de questions est variable car il dépend des questions et réponses précédentes)
- Score requis : 700/1000

***Examen en langue française***

- Durée : 6 heures
- Nombre de questions : 250
- Type de questions : choix multiples et questions avancées innovantes
- Score requis : 700/1000

Les conditions pour être certifié sont la réussite à l'examen, la justification de cinq années d'expérience professionnelle dans au moins deux des huit domaines du programme, l'adhésion au code déontologique et l'approbation d'une personne certifiée (« endorsement »).

Les poids des domaines à l'examen

- Sécurité et management des risques (domaine 1) 15%,
- Architectures et ingénierie (domaine 3) 13%,
- Sécurité des réseaux et des communications (domaine 4) 14%,
- Evaluation et test (domaine 6) 12%,
- Sécurité des opérations (domaine 7) 13%.
- Gestion des actifs (domaine 2) 10%
- Gestion des identités et des accès (domaine 5) 13%
- Sécurité du développement logiciel (domaine 8) 10%