Se Préparer à la Certification Internationale

CISSP (Certified Information Systems Security Professional),

Du 24 au 28 Juin 2019

Hôtel « NOVOTEL Mohamed V» Tunis

Introduction

Cette formation a pour but de préparer les candidats à l'examen du CISSP (Certified Information Systems Security Professional), la certification internationale délivrée par l'(ISC)². L'examen est devenu CBT (Computer Based testing) depuis juin 2012.

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.

Tout au cours de la semaine, les participants sont invités à répondre à des questions, en groupe et individuellement, sur chacun des domaines et similaires à l'examen officiel.

Objectifs de la Formation

- Acquérir les connaissances nécessaires à la réussite de l'examen CISSP® ,
- 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 Consultants) qui souhaitent obtenir la certification CISSP (Certified Information System Security Professional) délivrée par l'ISC2, et préparer l'examen.

Examen :

L'examen se passe en mode CBT (Computer Based Test) et dure entre 3 et 6 heures dans un centre pearson vue sis à

Université Centrale de Tunis

C'est un questionnaire constitué de 250 questions portant sur l'ensemble des domaines relevant de la sécurité du système d'information. Réussite à l'examen avec au moins 700 points (*).

(*) : La certification CISSP® n'est délivrée par ISC2 qu'à condition de prouver une expérience d'au moins 5 ans dans au moins deux domaines de la sécurité (exigence ramenée à 4 ans si présentation de diplôme universitaire).

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.

Demande d'inscription

Formation *se préparer à la certification CISSP*

du 24 au 28 Juin 2019

Inscrivez-vous dès maintenant en complétant ce bulletin d'inscription – L'envoyer Par Fax + 216 71 89 23 48 ou Par mail : contact@bit.tn

M./ Mme	Prénom Nom	Fonction	E-mail / GSM

Entreprise :

Adresse :

Code postal : Ville :

Téléphone : Fax :

Email : Site Web :

Les frais d'inscription à la formation et à l'examen de certification sont d'environ **5000 DT HT* (TVA 19%)** par personne.

NB : Les places sont limitées

Tunis, le ……

Signature et Cachet

*Conditions Générales d'inscription

Votre inscription sera définitive après réception de ce formulaire dûment rempli ainsi que du règlement du montant total de la formation **au plus tard une semaine avant le début de la session**. Elle sera prise en compte dans la limite des places disponibles.

Pour discuter d'une offre de groupe ou pour plus d'amples détails sur la formation, merci de nous consulter par:

Email : contact@bit.tn
Phone # : +216 71 892 348 / 71 892 352 / 94 70 77 37

Lieu de formation : Hôtel « NOVOTEL » Tunis

Etrangers intéressés par la formation :

- Nous pouvons vous conseiller pour votre hébergement. Merci de nous contacter.
- Le paiement des frais de participation se fait au plus tard une semaine avant le démarrage de la session par virement bancaire.

Calcul des coûts:

Le prix inclus :

- La participation à la formation.
- Le passage d'un examen de certification
- Les supports électroniques du cours
- Pauses café et déjeuner

Mode de paiement :

- Par chèque au nom de Business and Information Technology
- Par virement bancaire au compte ATB :
  - RIB : 0109 0125 1107 0030 3949
  - IBAN : TN59 0109 0125 1107 0030 3949

Cette Formation est éligible à la ristourne de la TFP. Numéro d'enregistrement MFPE : 11116912

Annulation de session:

Nous nous réservons le droit d'annuler une session lorsque le nombre de participants est insuffisant.

Annulation d'inscription:

Tout désistement devra nous être notifié au moins une semaine avant le début de la session (annulation avec remboursement sans frais). Au-delà de ce délai, le montant prévu pour la session vous sera intégralement facturé.