Session de Préparation Approfondie à la Certification CISSP®

Du 26 au 30 mai 2014
Hôtel NOVOTEL Mohamed V - Tunis

Objectifs de la Formation

Préparer les candidats au passage du Certificat CISSP de (ISC)² avec les meilleures chances de réussite compte tenu de leur niveau de connaissances et de leur expérience dans les dix domaines clés

Pré-requis

- ✓ si possible 5 années d'expérience professionnelle dans le domaine de l'Informatique
- ✓ avec au moins deux domaines (voir ci-après les 10 domaines) bien maitrisés

Public visé

Cette formation s'adresse aux administrateurs de réseaux, consultants, conseillers en gouvernance de la sécurité , gestionnaires de la sécurité, responsables de la protection des actifs informationnels et tout autre professionnel dont le développement de carrière nécessite la certification *CISSP®*.

Informations Générales sur la Formation

- ✓ La formation est donnée en français, Il est toutefois demandé aux candidats une maitrise de l'anglais suffisante pour lire le contenu des slides
- ✓ Un support de cours en anglais (langue recommandée pour le passage de l'examen) et d'autres documents électroniques seront remis à chaque participant
- ✓ Chaque session est limitée à un maximum de **12 personnes**

Formateur

- ✓ L'animateur**,** Noureddine LABANI , Expert en sécurité des Systèmes d'Information, est titulaire des plus importantes certifications et a une longue expérience technique dans le domaine, lui conférant les compétences et la légitimité nécessaires.

- ✓ Il a les certifications suivantes : **Master SSI, CISSP, CISM, CISA, CBCP, CEH, Lead Auditor ISO 27001, Risk Manager ISO 27005,**

- ✓ Noureddine LABANI intervient comme consultant sur des missions de gouvernance de la sécurité, d'accompagnement à l'implémentation de SMSI conformes aux exigences de la norme ISO./CEI 27001 : 2005, de management de risques de sécurité du SI, de
définition de Politique de Sécurité du SI, d'audit de sécurité, de gestion de projet sécurité, de veille et de conseil en sécurité des SI mais aussi d'assistance et de sensibilisation des métiers à la SSI.

- ✓ Depuis plus de deux ans, Noureddine LABANI, s'occupe de management de la sécurité informatique au sein d'une importante banque d'investissement en tant que RSI Adjoint.

Programme détaillé de la Formation (5 jours)

Jour 1 :

Domaine 1 : Management de la Sécurité

- Introduction et Objectifs du management de la sécurité de l'information
  - Concepts : Disponibilité, Intégrité, Confidentialité
- Approches de sécurité
- Concepts de management des risques de sécurité de l'information
- Processus de management des risques de sécurité de l'information
- Politique, Standards, Baselines, Directives et Procédures.
- Classification des Actifs
- Formation et Sensibilisation à la Sécurité Informatique
- Questions d'entrainement pour l'examen

Domaine 2 : Architecture et Modèles de Sécurité

- Introduction et Objectifs de l'architecture et modèles de sécurité
- Menaces à la sécurité des architectures
- Architecture physique de l'Ordinateur
- Architecture de la sécurité
- Modèles de sécurité
- Modes de sécurité opérationnelle
- Méthodes d'Evaluation et critères des systèmes
  - ✓ Le Livre Orange (TCSEC)
  - ✓ Le Livre rouge (TNI)
  - ✓ ITSEC
  - ✓ Les Critères Communs (CC)

- ✓ Comparaison des niveaux d'évaluation des systèmes
- ✓ Certification et Accréditation.

- Questions d'entrainement pour l'examen

Jour 2 :

Domaine 3 : Contrôle d'accès

- Introduction et Objectifs du contrôle d'accès
- Types de Contrôles d'Accès,
- Services de Contrôle d'Accès (IAAA)
- Techniques de Contrôle d'Accès
- Politique de Contrôle d'Accès
- Meilleures pratiques (gestion des mots de passe, …)
- Questions d'entrainement pour l'examen
-

Domaine 4 : Sécurité du développement logiciel

- Introduction et Objectifs de la sécurité du développement logiciel
- Processus de Développement des Applications
  - Cycle de vie du développement des applications
  - Contrôle administratif
  - Modèles de développement de logiciels
  - Contrôle des changements
  - Langage de programmation
  - Assembleur, compilateur et interpréteur
  - Programmation orientée objet (OOP)
  - Informatique répartie
- Gestion de base de données
  - o Système de gestion de base de données
  - o Modèles de base de données
  - o Langage d'interface de la base de données
  - o Entrepôt de données et exploration de données
- Intelligence artificielle
  - o Système expert
  - o Réseau neuronal artificiel
- Questions d'entrainement pour l'examen

Jour 3 :

Domaine 5 : Sécurité des opérations

- Introduction et Objectifs de la sécurité des opérations
- Principes généraux de sécurité des opérations
  - Privilège minimum
  - Besoin d'en connaître
  - Fonctions privilégiées
  - Respect de la vie privée
  - Exigences juridiques
  - Activités illégales
  - Traitement des informations délicates
- Menaces à la sécurité des opérations

    - Le matériel
    - Le logiciel
  - Les opérations
  - Les données et leur support
  - Equipements de télécommunications
  - Le système de soutien
  - Perte accidentelle
  - Le personnel
  - Espionnage industriel
  - Pirates et intrus
  - Activités inappropriées
- Catégories et types de mesures de sécurité
    - Types de contrôles
    - Contrôles organisationnels
    - Contrôles techniques
    - Contrôles physiques
- Questions d'entrainement pour l'examen

Domaine 6 : Cryptographie

- Introduction et Objectifs du la cryptographie
- Historique de la Cryptographie et Encadrement légal
- Technologie de sécurité et outils
- Conditions d'efficacité des outils
- Cryptanalyse et attaques
- Questions d'entrainement pour l'examen

Jour 4 :

Domaine 7 : Sécurité physique

- Introduction et Objectifs de la Sécurité Physique
- Besoins et exigences des entreprises
- Environnement et Menaces
  - Différents types
  - 7 sources différentes
  - Spécifique - Feu
  - Spécifique - Environnement opérationnel
- Contrôles organisationnels
- Contrôles techniques
- Contrôles physiques
- Questions d'entrainement pour l'examen

Domaine 8 : Sécurité des Télécommunications et des Réseaux

- Introduction et Objectifs de la sécurité des Télécommunications et des Réseaux
- Télécommunications, réseaux et Internet
  o Réseaux de données
  o Protocoles de réseaux
  o Menaces liées aux réseaux
  o Systèmes de callback et authentification
  o Système d'authentification centralisée

- Coupe-feu et sécurité du périmètre
- Filtrage de contenu et inspection
- Détection des intrusions
- Réseaux Privés virtuels (VPN)
- Disponibilité des ressources
- Journaux d'audit de sécurité
- Examens réguliers de la sécurité
- Estimation des vulnérabilités

• Questions d'entrainement pour l'examen

Jour 5 :

Domaine 9 : Continuité des activités

- Introduction et Objectifs de la continuité des activités
- Différences entre BCP et DRP
- Définition d'un sinistre
- Environnement et menaces
- Le processus BCP
  - Phase 1 : Management du projet BCP et initiation
  - Phase 2 : Business Impact Analysis (BIA)
  - Phase 3 : Stratégies de reprise
  - Phase 4 : Développement du plan et Implémentation
  - Phase 5 : Test, Maintenance, Sensibilisation et Formation
    - _ Objectifs et Types de test
    - _ Maintenance
    - _ Sensibilisation et Formation
- L'activation du BCP
- Questions d'entrainement pour l'examen

Domaine 10 : Loi, investigations et éthique

- Introduction et Objectifs du domaine Loi, investigations et éthique
- Environnement et menaces
- Loi
  - Droit international
  - Droit civil
  - Common Law

Demande d'inscription

à la formation de préparation à la certification CISSP®

du 26 au 30 Mai 2014

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 sont à **2800 DT*** HT par personne hors frais de certification. Soit pour un montant total de : ……..... DT / HT pour ……. personne(s).

L'inscription à l'examen de certification coute 599$ / **NB : Le nombre de places est limité**

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.

10% de remise si inscription au moins 1 mois avant la formation

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 à Mohamed V - 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.
- Les supports de cours + 1 flash USB par participant
- Pauses café et déjeuner

Mode de paiement :

- Par chèque au nom de Business and Information Technology
- Par virement bancaire au compte :
  - RIB : 04 103 003 0021292560
  - IBAN : TN59 04 103 003 0021292560

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.