Tél : +352 27 39 351
Fax : +352 27 39 52 68
Email : formation@oxiane.lu

CISSP – (Certified Information Systems Security Professional)

CISSP est la certification professionnelle internationale la plus connue dans le monde de la sécurité des systèmes d'information. Le programme de certification géré par ISC² (International Information Systems Security Certification Consortium) est réparti en 10 thèmes qui couvrent tous les aspects de la Sécurit des Systèmes d'Information, qui sont dans un référentiel appellé CBK (Common Body of Knowledge), disponible dans le livre » Official ISC² Guide to the CISSP Exam (ISC² Press) « .

Détails

- Code : CISSP
- Durée : 5 jours (35 heures)

Public

- Consultants en Sécurité
- Directeurs sécurité
- Ingénieurs Sécurité
- IT Security Officers
- Members of the Information Security Team
- Professionnels de l'informatique
- Professionnels de la sécurité informatique
- Professionnels de l'IT

Pré-requis

Objectifs

- Préparation à l'examen CISSP® v2015 L'examen de certification n'est pas inclus avec la formation. Il faut s'inscrire sur le site officiel de l'(ISC)2®. L'examen est planifié par l'étudiant à la date de son choix La certification CISSP® est basée sur un questionnaire à choix multiples de 250 questions concernant les 8 domaines Durée : 6 heures L'examen du CISSP est disponible en anglais avec la traduction en français

Programme

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 assets

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

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

Tél : +352 27 39 351
Fax : +352 27 39 52 68
Email : formation@oxiane.lu

- 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'architectures réseau
- Sécuriser les composants réseau
- Concevoir et établir des canaux de communication sécurisés
- Prévenir ou limiter les attaques réseau

Domaine 5 : Management des identités et des accès

- Contrôle d'accès physique et logique aux assets
- 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

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

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.

Modalités

- Type d'action :Acquisition des connaissances
- Moyens de la formation :Formation présentielle – 1 poste par stagiaire – 1 vidéo projecteur – Support de cours fourni à chaque stagiaire
- Modalités pédagogiques :Exposés – Cas pratiques – Synthèse
- Validation :Exercices de validation – Attestation de stages