Formation **CISSP (Certified Information Systems Security Professional), avec certification**

Cette formation CISSP constitue une préparation à la certification maintenue par l'International Information Systems Security Certification Consortium (ISC)². Elle permettra aux participants d'acquérir l'ensemble des connaissances et compétences nécessaires à l'obtention du titre de Certified Information Systems Security Professional (CISSP), internationalement reconnu et valorisé dans le monde de la sécurité de l'information. Pour suivre cette formation, il est fortement recommandé d'être dans la phase finale de préparation au passage de l'examen. Notamment, les participants devront avoir lu et s'être approprié le CBK officiel ("Official ISC² Guide to the CISSP Exam" - (ISC)² Press). L'examen de certification CISSP s'effectuera en différé, dans un centre PearsonVue autorisé par l'(ISC)².

Durée
5 jours

Objectifs pédagogiques

- Acquérir une vision globale des enjeux et aspects de la sécurité IT
- Comprendre les thèmes, domaines et rubriques du Common Body ok Knowledge (CBK®)
- Être en mesure d'optimiser les opérations de sécurité d'une organisation
- Se préparer et passer l'examen de certification CISSP de l'ISC²

Public
Managers, Risk managers, Administrateurs systèmes et réseaux, Responsables de la sécurité des systèmes d'information (RSSI), Auditeurs, Ingénieurs télécoms et réseaux

Prérequis
Avoir lu le CBK ("Official ISC² Guide to the CISSP Exam - (ISC)² Press). Les candidats à l'examen de certification doivent également avoir un minimum de 5 ans d'expérience cumulée de travail rémunéré dans au moins deux des huit domaines du CBK de CISSP. Pour en savoir plus, rendez-vous sur le site de l'ISC².

Programme de formation

Introduction à la formation CISSP

Présentation et objectifs pédagogiques de cette formation CISSP
Les 8 domaines du CISSP Common Body of Knowledge (CBK)

Gestion du risque et de la sécurité

Comprendre, adhérer et promouvoir l'éthique professionnelle
Comprendre et appliquer les concepts de sécurité
Evaluer et appliquer les principes de gouvernance de sécurité
Déterminer la conformité et les autres exigences
Comprendre les problèmes juridiques et réglementaires relatifs à la sécurité informatique dans un contexte holistique
Comprendre les exigences relatives aux types d'enquêtes (c.-à-d., les normes administratives, criminelles, civiles, réglementaires, industrielles)
Développer, documenter et mettre en œuvre une politique, des normes, des procédures et des directives de sécurité
Identifier, analyser et hiérarchiser les exigences de Continuité Commerciale (BC)
Contribuer et appliquer les politiques et les procédures de sécurité du personnel
Comprendre et appliquer les concepts de gestion du risque
Comprendre et appliquer les concepts et méthodologies de modélisation des menaces
Appliquer les concepts de Gestion des Risques de la Chaîne d'Approvisionnement (SCRM)
Établir et maintenir un programme de sensibilisation, d'éducation et de formation à la sécurité

Sécurité des biens

Identifier et classifier les informations et les biens
Etablir les exigences de traitement de l'information et des biens
Provisionner les ressources en toute sécurité
Gérer la durée de vie des données
Garantir une rétention appropriée des bien (EOL, EOS...)
Déterminer les exigences en terme de contrôle et de conformité de la sécurité des données

Architecture et ingénierie de la sécurité

Rechercher, mettre en œuvre et gérer des processus d'ingénierie en utilisant des principes de conception sécurisée
Comprendre les concepts fondamentaux des modèles de sécurité (p.ex., Biba, Star Model, Bell-LaPadula)
Sélectionner les contrôles en fonction des exigences de sécurité des systèmes
Comprendre les capacités de sécurité des Systèmes Informatiques (IS) (p.ex., protection de la mémoire, Trusted Platform Module (TPM), cryptage / décryptage)
Évaluer et atténuer les vulnérabilités des architectures, des conceptions et des éléments de solution de la sécurité
Sélectionner et déterminer des solutions cryptographiques
Comprendre les méthodes attaques cryptanalytiques
Appliquer les principes de sécurité à la conception du site et des infrastructures
Concevoir les contrôles de sécurité du site et des infrastructures

Sécurité des réseaux et de la communication

Évaluer et mettre en œuvre les principes de conception sécurisée dans les architectures de réseau
Sécuriser les composants réseau
Mettre en œuvre des canaux de communication sécurisés selon la conception

Gestion des identités et des accès (IAM)

Contrôler l'accès physique et logique aux biens
Gérer l'identification et l'authentification des personnes, des appareils et des services
Identité fédérée avec un service tiers
Mettre en œuvre et gérer les mécanismes d'autorisation
Gérer le cycle de vie de l'approvisionnement des identités et des accès
Mettre en œuvre les systèmes d'authentification

Evaluation et tests de sécurité

Concevoir et valider des stratégies d'évaluation, de test et d'audit
Conduire des tests de contrôle de sécurité
Recueillir des données de processus de sécurité (p.ex., techniques et administratives)
Analyser la sortie de test et générer un rapport
Conduire ou faciliter des audits de sécurité

Opérations de sécurité

Comprendre et se conformer aux instructions
Conduire des activités de journalisation et de surveillance
Effectuer la gestion de la configuration (CM) (p.ex., approvisionnement, base de référence, automatisation)
Appliquer les concepts d'opérations de sécurité de base
Appliquer la protection des ressources
Conduire la gestion des incidents
Faire fonctionner et maintenir des mesures de détection et de prévention
Mettre en œuvre et prendre en charge la gestion des correctifs et des vulnérabilités
Comprendre et participer aux processus de gestion du changement
Mettre en œuvre des stratégies de récupération
Mettre en œuvre des processus de Reprise après Sinistre (DR)
Tester les Plans de Reprise après Sinistre (DRP)
Participer à la planification et aux exercices de Continuité Commerciale (BC)
Mettre en œuvre et gérer la sécurité physique
Répondre aux problèmes de sécurité et de sûreté du personnel

Sécurité du développement logiciel

Comprendre et intégrer la sécurité dans le Cycle de Vie du Développement Logiciel (SDLC)
Identifier et appliquer les contrôles de sécurité dans les écosystèmes de développement logiciel
Évaluer l'efficacité de la sécurité logicielle
Évaluer l'impact sur la sécurité des logiciels acquis
Définir et appliquer des directives et des normes de codage sécurisé

Préparation à l'examen de certification CISSP

Révisions, questions/réponses selon les besoins des apprenants
Trucs et astuces pour réussir l'examen de certification
Lectures recommandées

Modalités d'évaluation CISSP

Langues disponibles : Français, Allemand, Portugais, Espagnol, Japonais, Chinois et Coréen
Durée de l'examen : 6h
Nombre de questions : 250
Types de questions : Questions à choix multiple et de technologie avancée
Note nécessaire pour réussir l'examen : 700 points sur 1000