Organisme de formation professionnelle continue
Numero agrément 91 30 03332 30
France : +33 (0)188 24 70 33 / 34
Site : www.oo2.fr
Mail : contact@oo2.fr

CISSP-ISSEP® : ingénieur de la sécurité des systèmes d'information

Date et durée

Code formation : CIS03FR
Durée : 5 jours
Nombre d'heures : 35 heures

Formation avec préparation à la certification

CISSP® : Certified Information Systems Security Professional

Description

Un **ingénieur en sécurité des systèmes d'information (ISSEP)** est un professionnel CISSP expert dans la mise en œuvre des principes et des processus d'ingénierie des systèmes dans le but de concevoir des solutions sécurisées. Son rôle est d'analyser les besoins organisationnels, de définir des exigences de sécurité, de concevoir des architectures de sécurité, de **développer des modèles sécurisés**, de déployer la sécurité et de gérer les évaluations de sécurité des SI dans les secteurs public et privé.
En suivant cette **formation CISSP Concentration**, vous aborderez en détail 5 domaines inclus dans le corpus de connaissances (CBK®) de l'ISC2®. Ainsi, vous pourrez maitriser toutes les activités du domaine de l'ingénierie de la sécurité. Dans chaque **cours CISSP-ISSEP**, les domaines suivants seront couverts :

- Domaine 1 : les fondamentaux de l'ingénierie en sécurité des systèmes ;
- Domaine 2 : la management des risques ;
- Domaine 3 : la planification et la conception de la sécurité ;
- Domaine 4 : la mise en œuvre, la vérification et la validation des systèmes ;
- Domaine 5 : les opérations sécurisées, la gestion des changements et la suppression.

À l'issue de cette formation de 5 jours, vous serez en outre préparé pour **passer l'examen (ISC)² CISSP-ISSEP**. Cet examen que vous pourrez passer dans notre centre Pearson VUE vous permettra d'obtenir le titre de **Certified Information Systems Security Engineering Professional** (*pour plus d'informations, consultez l'onglet Certification*).

En partenariat avec ISC2®, Oo2 vous garantit un contenu de formation officiel et actualisé. Les cours sont dispensés par un formateur expert en sécurité informatique et agréé pour dispenser cette formation CISSP-ISSEP.

Objectifs

A l'issue de la **formation CISSP-ISSEP**, vous serez capable de valider les objectifs de compétences suivants :

- mettre en pratique les bases de l'ingénierie de la sécurité des systèmes ;
- mettre en pratique les processus standards d'ingénierie de la sécurité des systèmes ;
- utiliser une méthode de développement adaptée pour chaque système ;
- effectuer la maintenance technique des systèmes ;
- contribuer aux opérations d'acquisition ;
- concevoir des systèmes et des réseaux de confiance (TSN) ;
- appliquer les principes du management des risques de sécurité ;
- savoir gérer les risques pour chaque système ;
- analyser le cadre organisationnel et opérationnel ;
- mettre en pratique les principes de sécurité des systèmes ;
- définir des exigences système ;
- créer une architecture et un système de sécurité fiable et performant ;
- implémenter, adapter et faire évoluer des solutions de sécurité ;
- analyser et valider les solutions de sécurité mise en place ;
- élaborer une stratégie d'opérations sécurisées ;
- participer aux opérations de sécurisation, à la gestion du changement et aux processus d'élimination ;
- être bien préparé pour le passage l'examen officiel CISSP-ISSEP.

Points forts

Un formateur agréé (ISC)², des supports de cours officiels, une préparation complète pour le passage de la certification CISSP-ISSEP, des conseils et des quiz d'évaluations pour chacun des 5 domaines abordés.

Certification

Cette formation qui vous prépare à l'examen CISSP-ISSEP, vous permettra d'obtenir le titre de **Certified Information Systems Security Engineering Professional** délivrée par notre partenaire *(ISC)² ®. Il convient si vous êtes un professionnel de la sécurité des systèmes d'information et que vous êtes titulaire de la certification CISSP - Certified Information Systems Security Professional.*
Le CISSP-ISSEP atteste de votre **maitrise des principes et des processus de l'ingénierie des systèmes** pour le développement de systèmes sécurisés. De plus, il démontre que vous possédez les connaissances et les compétences requises pour intégrer la sécurité dans les projets, les applications, les processus opérationnels et tous les systèmes d'information.

Information sur l'examen CISSP-ISSEP :

- Durée : 3 heures max
- Langue de l'examen : anglais
- Nombre de questions :125
- Format des questions : choix multiple
- Note de passage : 700 sur 1000 points

A savoir : *après avoir passé l'examen CISSP-ISSEP et obtenu la certification, vous devez renouveler votre certification tous les 3 ans. Pour cela, vous devez obtenir 20 crédits de formation professionnelle continue (FPC) chaque année. Vous pouvez utiliser ces 20 crédits dans le cadre de votre exigence de formation continue CISSP, à condition que les crédits soient spécifiques à l'architecture de sécurité.*
Pour passer l'examen de certification CISSP-ISSEP, vous pouvez vous rendre dans notre centre Pearson VUE Oo2 Formations.

Modalités d'évaluation

Quiz / QCM
Travaux Pratiques

Pré-requis

Suivre la **formation CISSP-ISSEP** nécessite les prérequis suivants :

- détenir le titre professionnel CISSP à jour et justifier de 2 ans d'expérience professionnelle cumulée dans un ou plusieurs des 6 domaines du corpus de connaissances (ISC)² CBK.

Pour obtenir la certification CISSP, vous pouvez suivre notre formation :

Les formations ci-dessous sont recommandées.

CISSP® : devenir expert en sécurité des SI

Public

Cette formation s'adresse aux publics suivants :

- les ingénieurs systèmes expérimentés, les responsables sécurité des systèmes d'information, les analystes en sécurité de l'information ou tout autre tout professionnel de l'ingénierie de la sécurité des systèmes d'information.

Cette formation s'adresse aux profils suivants

Ingénieur système
Analyste cybersécurité

Programme

Domaine 1 : compréhension des bases de l'ingénierie de la sécurité des SI

- Les concepts de fiabilité et les hiérarchies de l'ingénierie de la sécurité des systèmes.
- Les relations entre les systèmes et les processus d'ingénierie de la sécurité.
- Les principes de conception de la sécurité structurelle.
- L'identification de l'autorité de sécurité organisationnelle.
- Les éléments de la politique de sécurité des systèmes.
- Les principes de conception (ouvert, propriétaire, et modulaire).
- Les tâches et les activités de sécurité.
- La vérification des exigences de sécurité durant tout le processus.
- Les méthodes d'intégration de l'assurance qualité logicielle.
- Les processus de planification de projet.
- Les processus d'évaluation et de contrôle du projet.
- Les processus de gestion des décisions.
- Les processus de gestion des risques.
- Les processus de gestion de la configuration.
- Les processus de gestion de l'information.
- La mise en œuvre des processus de mesure.
- La mise en œuvre des processus d'assurance qualité.
- L'identification des opportunités d'automatisation des processus de sécurité.
- La préparation des exigences de sécurité pour les acquisitions.
- La préparation du processus de sélection.

- La participation à la gestion des risques de la chaîne. d'approvisionnement (Supply Chain Risk Management).
- L'élaboration et à la révision de la documentation contractuelle.
- La conception de systèmes et de réseaux de confiance (Trusted Systems and Networks).

Domaine 2 : mise en œuvre du management des risques

- L'alignement de la gestion des risques de sécurité sur celle de l'entreprise (Enterprise Risk Management).
- L'intégration de la gestion des risques à tous les stades du cycle de vie
- La définition du contexte du risque.
- L'identification des risques pour la sécurité du système.
- La réalisation d'une analyse des risques.
- La réalisation d'une évaluation des risques.
- Les recommandations relatives aux options de gestion des risques.
- La mise à disposition de documents sur les conclusions et les décisions liées aux risques.
- La fixation du niveau de tolérance au risque des parties prenantes.
- L'identification des exigences de remédiation et des autres changements de système.
- La fixation des options de traitement des risques.
- L'évaluation des options de traitement des risques suggérées.
- Les recommandations relatives aux options de traitement des risques.

Domaine 3 : conception et planification de la sécurité

- La compréhension des besoins des parties prenantes.
- L'identification des contraintes et des hypothèses pertinentes.
- L'évaluation et la documentation des menaces.
- La définition des besoins de protection du système.
- La création de plans de test de sécurité (STP).
- Les méthodes de résilience pour répondre aux menaces (concepts de défense en profondeur).
- L'identification des valeurs par défaut à sécurité intégrée.
- La diminution des points de défaillance uniques (SPOF).
- La compréhension du concept de moindre privilège.
- La compréhension de l'économie des mécanismes.
- La compréhension du principe de séparation des tâches (SoD).
- Le développement du contexte de sécurité du système.
- L'identification des fonctions au sein du système et du concept de sécurité des opérations (CONOPS).
- La mise à jour de la documentation des exigences de sécurité du système.
- L'analyse des exigences de sécurité du système.
- Le développement de l'analyse fonctionnelle et de l'allocation.
- Le maintien de la traçabilité entre la conception spécifiée et les exigences du système.
- La mise en place des composants de la conception du système de sécurité.
- La réalisation d'études de compromis.
- L'évaluation de l'efficacité de la protection.

Domaine 4 : mise en œuvre, vérification et validation des systèmes

- La mise en œuvre et l'intégration de la sécurité des systèmes.
- La conduite des activités de déploiement de la sécurité des systèmes.
- La vérification de la sécurité des systèmes.
- La validation de la sécurité afin de prouver que les contrôles de sécurité respectent les exigences de sécurité des parties prenantes.

Domaine 5 : sécurisation des opérations, gestion du changement et suppression

- La définition des exigences pour le personnel chargé des opérations.

- La communication continue avec les parties prenantes sur les questions de sécurité du système.
- L'élaboration de solutions et de processus de surveillance continue.
- Le soutien du processus de réponse aux incidents.
- La mise en place d'une stratégie de maintenance sécurisée.
- La participation à la revue des changements.
- L'indentification des impacts liés aux changements.
- La vérification et la validation des changements.
- La mise à jour de la documentation sur l'évaluation des risques.
- L'identification des exigences de sécurité de suppression.
- L'élaboration d'une stratégie de suppression sécurisée.
- L'élaboration de procédures de déclassement et de suppression.
- L'audit des résultats du processus de déclassement et de suppression.

Contenu de formation proposé en partenariat avec (ISC)² ®
CISSP® et CISSP-ISSEP® sont des marques déposées de l'International Information Systems Security Certification.