CISSP-ISSMP® : manager de la sécurité des systèmes d'information

Date et durée
Code formation : CIS04FR Durée : 5 jours Nombre d'heures : 35 heures
Formation avec préparation à la certification
CISSP® : Certified Information Systems Security Professional
Description

Un **professionnel du management de la sécurité des systèmes d'information** (ISSMP) est une personne certifié CISSP qui se spécialise. Il est chargé d'établir, de présenter et de gérer des programmes de sécurité de l'information. En outre, il ou elle possède des compétences avancées en matière de gouvernance et de leadership. Les objectifs d'un CISSP-ISSMP consiste à orienter les **programmes de sécurité** en fonction de la mission, des objectifs et des stratégies des entreprises en vue de répondre aux exigences financières et opérationnelles tout en prenant en compte les risques identifiés.
En suivant cette **formation de 5 jours**, vous serez en mesure de maîtriser tous les aspects de la gestion de la sécurité de l'information. Elle est destinée aux cadres dirigeants qui sont responsables de la mise en place, de la présentation et de la gestion de leur programme de sécurité. Toutefois, elle s'adresse également à ceux qui souhaitent **devenir Chief Technology Officer (CTO), Chief Information Officer (CIO)** et tout autre professionnel de la gestion chargé de la sécurité de l'information ou de la sécurité informatique. A ce titre, le programme de formation CISSP-ISSMP couvre les 6 domaines suivants :

- le leadership et le management d'entreprise ;
- la gestion du cycle de vie des systèmes ;
- le management du risque ;
- l'Intelligence des menaces et la gestion des incidents ;
- la gestion des situations d'urgence ;
- la gestion de la conformité juridique, déontologique et sécuritaire.

Après avoir suivi cette formation CISSP-Concentration, vous serez en mesure de **passer l'examen CISSP-ISSAP (ISC)²**. Il vous permettra d'obtenir le titre de **Certified Information Systems Security Professional Management** (*pour plus d'informations, voir 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-ISSMP.

Objectifs

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

- comprendre quel est l'importance de la sécurité dans la culture, la vision et la mission d'une entreprise ;
- adapter un plan de sécurité à la gouvernance d'une entreprise ;
- élaborer et déployer des stratégies de sécurité de l'information ;
- élaborer et assurer le maintien d'une politique de sécurité ;
- identifier les normes spécifiques en vigueur ;
- traiter les exigences de sécurité dans les contrats et les accords ;
- organiser des formations de sensibilisation à la sécurité ;
- concevoir, évaluer et communiquer des mesures de sécurité ;
- établir, négocier et superviser le budget alloué à la sécurité ;
- assurer la gestion des programmes de sécurité ;
- mettre en œuvre les principes de management de projet et de développement de produits ;
- gérer la mise en œuvre de la sécurité dans le cycle de développement des systèmes ;
- implanter les nouvelles solutions commerciales et les technologies les plus récentes dans une architecture de sécurité ;
- concevoir et gérer des programmes de gestion des vulnérabilités ;
- gérer les questions de sécurité relatives au contrôle des changements ;
- concevoir et gérer un programme de gestion des risques ;
- procéder à des évaluations des risques ;
- gérer les risques de sécurité au niveau de la chaîne d'approvisionnement ;
- concevoir et gérer un programme de renseignement sur les menaces ;
- développer et gérer un programme de traitement et d'investigation des incidents ;
- promouvoir l'élaboration de plans d'urgence ;
- concevoir des stratégies de récupération ;
- assurer la continuité d'un plan d'urgence, d'un plan de continuité des opérations, d'un plan de continuité des activités et d'un plan de reprise après sinistre ;
- traiter les processus de réponse et de reprise après sinistre ;
- identifier les impacts relatifs aux lois et aux réglementations en matière de sécurité de l'information ;
- se conformer au code de déontologie de $(ISC)^2$ pour le management ;
- garantir la conformité selon les réglementations en vigueur et les bonnes pratiques industrielles ;
- assurer la coordination des auditeurs et des régulateurs en vue de faciliter les processus d'audit interne et externe ;
- documenter et assurer la gestion des exceptions de conformité ;
- être bien préparé pour le passage l'examen officiel CISSP-ISSMP.

Points forts

Un formateur agréé (ISC)², des supports de cours officiels, une préparation complète pour le passage de la certification CISSP-ISSMP, des conseils et des quiz d'évaluations pour chacun des 6 domaines abordés.

Certification

Cette formation qui vous prépare à l'examen CISSP-ISSMP, vous permettra d'obtenir le titre de **Certified Information Systems Security Professional Management** 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-ISSMP démontre votre expertise dans la mise en œuvre, la présentation et la gestion de **programmes de sécurité de l'information**. En outre, il atteste de vos solides **compétences en management et en leadership**, que vous soyez à la tête d'une équipe de gestion des incidents ou d'une équipe d'atténuation des défaillances.

Information sur l'examen CISSP-ISSMP :

- 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-ISSMP 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-ISSMP, vous pouvez vous rendre dans notre centre Pearson VUE Oo2 Formations.

Modalités d'évaluation

Quiz / QCM
Travaux Pratiques

Pré-requis

Suivre la **formation CISSP-ISSMP** 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 directeurs des systèmes d'information (CIO et DSI), les responsables de la sécurité de l'information, les directeurs des nouvelles technologies (CTO) ou encore tout les hauts responsables de la sécurité des SI.

Cette formation s'adresse aux profils suivants

Manager
Directeur des Systèmes d'Information (DSI)

Programme

Domaine 1 : leadership et management d'entreprise

- La vision et les objectifs d'un programme de sécurité de l'information.
- L'alignement de la sécurité sur les objectifs et les valeurs de l'entreprise.
- La corrélation entre la sécurité et l'ensemble des processus opérationnels.
- La corrélation entre la culture organisationnelle et la sécurité.
- L'identification et la connaissance de la structure de gouvernance d'une entreprise.
- La validation des rôles des principales parties prenantes.
- La validation des sources et des restrictions d'autorisation.
- La défense et l'obtention des appuis organisationnels pour les mesures de sécurité.
- L'identification des exigences de sécurité liées aux projets d'entreprise.
- L'évaluation de la capacité à mettre en application des stratégies de sécurité.
- La mise en place des stratégies de sécurité.
- La revue et la continuité des stratégies de sécurité.
- La préconisation de concepts, de techniques d'architecture et et de méthode d'ingénierie pour la sécurité.
- L'identification des normes externes à appliquer.
- L'identification des exigences relatives à la classification et à la protection des données.
- L'élaboration de politiques internes.
- La promotion et l'obtention d'un appui administratif pour les politiques.
- L'élaboration de procédures, de normes et de lignes directrices.
- La révision périodique du cadre de la politique de sécurité.
- L'évaluation des accords de gestion des services
- (risque et finance).
- La gestion des services intégrés (infrastructure, services cloud, etc.).
- La gestion des effets liés aux changements organisationnels (fusion, acquisition et externalisation).
- La garantie que les déclarations et les exigences de conformité sont présentes dans les accords accords contractuels.
- Le suivi et le respect de la conformité des accords contractuels.
- La promotion des programmes de sécurité envers les principales parties prenantes.
- L'identification des besoins et la création de programmes de formation par secteur visé.
- La surveillance et le rapport sur l'efficacité de la sensibilisation à la sécurité et des programmes de formation.
- L'identification des indicateurs clés de performance (KPI).
- L'association KPI au niveau des risques de l'entreprise.
- L'utilisation d'outils pour gérer le développement et les opérations du programme de sécurité.
- La préparation et la garantie du financement annuel.
- L'ajustement du budget basé sur l'évolution des risques et du contexte des attaques informatiques.
- La gestion et le compte rendu des responsabilités financières.
- La définition des rôles et des responsabilités.
- La gestion des responsabilités de l'équipe.
- La création de relations transversales.
- La résolution des conflits entre la sécurité et les autres parties prenantes.
- L'identification des goulots d'étranglement et des obstacles.
- L'intégration des contrôles de sécurité dans les processus du service RH.
- L'intégration de la sécurité dans le cycle de vie d'un projet.
- L'identification et la mise en œuvre d'une méthodologie de gestion de projet adaptée.
- L'analyse de la relation entre le temps, la portée et le coût d'un projet.

Domaine 2 : gestion du cycle de vie des systèmes

- L'intégration des points de contrôle de sécurité de l'information et des spécifications au sein du cycle de vie.
- La mise en place de contrôles de sécurité dans le cycle de vie du système.
- La mise en place des processus de gestion de la configuration pour la sécurité.
- L'intégration de la sécurité dans les nouvelles initiatives commerciales et technologiques existantes.
- L'impact des nouvelles initiatives commerciales au niveau de la sécurité.
- L'identification, la classification et la hiérarchisation des actifs, des systèmes et des services basées sur la criticité pour l'entreprise.
- La classification des menaces et des vulnérabilités par ordre de priorité.
- La gestion des tests de sécurité.
- La gestion de l'atténuation ou de la correction des vulnérabilités en fonction du risque.
- L'intégration des exigences de sécurité dans le processus de contrôle des changements.
- L'identification et la coordination avec les parties prenantes.
- La gestion de la documentation et du suivi.
- Le suivi de la mise en œuvre des politiques.

Domaine 3 : gestion des risques

- Les objectifs d'un programme de gestion des risques.
- La communication et la validation des objectifs de gestion des risques avec les responsables du risque et les autres parties prenantes.
- La champ d'application du programme de gestion des risques pour l'entreprise.
- L'identification de la tolérance et de la capacité de l'entreprise à supporter les risques de sécurité.
- L'obtention et la vérification de l'inventaire des actifs de l'entreprise.
- La réalisation d'une analyse des risques organisationnels.
- La fixation des contre-mesures ainsi que des contrôles compensatoires et d'atténuation.
- La réalisation d'une analyse coûts-avantages et des options de traitement des risques.
- L'identification des facteurs de risque.
- L'identification des exigences relatives aux risques pour la sécurité de la chaîne d'approvisionnement.
- L'intégration des risques de sécurité dans la chaîne d'approvisionnement pour le management.
- La validation du processus de contrôle des risques de sécurité au sein de la chaîne d'approvisionnement.
- La surveillance et la revue des risques de sécurité dans la chaîne d'approvisionnement.

Domaine 4 : renseignements sur les menaces et gestion des incidents

- L'agrégation des données sur les menaces issues de multiples sources de renseignements sur les menaces.
- La réalisation d'une analyse de base du trafic réseau, des données et du comportement des utilisateurs.
- La détection et l'analyse des modèles de comportement anormal.
- La réalisation d'une modélisation des menaces.
- L'identification et la classification des types d'attaques.
- La corrélation entre les événements de sécurité et les données sur les menaces.
- La mise en place d'alertes exploitables à destination des ressources concernées.
- La mise à jour de la documentation du programme.
- La mise en place d'un processus de gestion des cas de réponse aux incidents.
- La constitution d'une équipe de réponse aux incidents.
- La mise en pratique des méthodes de gestion des incidents.
- La création et le maintien d'un processus de traitement des incidents
- et d'un processus d'enquête.
- La quantification et le compte rendu de l'impact financier et opérationnel des incidents et des enquêtes aux parties prenantes.
- La réalisation d'une analyse des causes profondes.

Domaine 5 : management des incidents de sécurité

- L'identification et l'analyse des aspects du plan de continuité des opérations ainsi que du plan de continuité des activités.
- L'identification et l'analyse les aspects du plan de reprise après sinistre.
- La coordination des plans de gestion de crise avec les parties prenantes clés.
- La création des plans de communication de crise internes et externes.
- La définition et la communication des rôles et des responsabilités en cas d'urgence.
- L'identification et l'analyse de l'impact des mesures d'urgence sur les processus et les priorités de l'entreprise.
- La gestion des dépendances des tiers en cas d'urgence.
- La préparation d'un plan de succession pour la gestion de la sécurité.
- L'identification et l'analyse des solutions alternatives.
- Les recommandations et la gestion des stratégies de reprise.
- L'attribution des rôles et des responsabilités en matière de reprise.
- La planification des tests, des évaluations et des modifications.
- La fixation des possibilités de résistance et de résilience.
- La gestion du processus de mise à jour du plan.
- La déclaration d'un incident.
- La mise en œuvre du plan.
- La reprise des activités courantes.
- La mise à jour du plan en fonction des leçons apprises.

Domaine 6 : droit, éthique et gestion de la conformité de la sécurité

- L'identification des réglementations applicables en matière de protection de la vie privée (RGPD).
- L'identification des instances juridiques dont relèvent les organisations et les utilisateurs qui exercent leurs activités.
- L'identification des lois relatives à l'exportation.
- L'identification des lois sur la propriété intellectuelle.
- L'identification des normes industrielles en vigueur.
- L'identification et la formulation des conseils sur les risques de non-conformité.
- L'adhésion au code d'éthique de l'(ISC)2 relatif au management.
- La communication sur les mesures à mettre en place à la direction de l'entreprise.
- L'évaluation et la sélection du ou des cadres de conformité.
- La mise en place du ou des cadres de conformité.
- La création et le suivi des mesures de conformité.
- La planification d'un audit.
- La coordination des activités d'audit.
- L'évaluation et la validation des résultats de l'audit.
- La formulation des réponses.
- La validation des mesures d'atténuation et de remédiation.
- L'identification et la documentation des contrôles compensateurs ainsi que des moyens de contournement.
- Le compte-rendu et la validation de la renonciation aux risques.

Contenu de formation proposé en partenariat avec (ISC)² ®