

Préparation à la certification CISSP

5 jours (35 heures)

Perfectionnement

Présentiel

à partir de

4 200 € HT par personne (TVA en vigueur)

Contenu mis à jour le 30/09/2026. Document téléchargé le 01/10/2026.

Objectifs

A l'issue de cette formation, vous serez capable de :

- Appliquer les concepts et méthodes fondamentaux liés aux domaines des technologies de l'information et de la sécurité
- Aligner les objectifs opérationnels globaux de l'organisation avec les fonctions et les mises en oeuvre de la sécurité
- Protéger les actifs de l'organisation au cours de leur cycle de vie
- Exploiter les concepts, principes, structures et normes utilisés pour concevoir, mettre en oeuvre, surveiller et sécuriser les systèmes d'exploitation, les équipements, les réseaux, les applications et les contrôles utilisés pour appliquer divers niveaux de confidentialité, d'intégrité et de disponibilité
- Appliquer les principes de conception de la sécurité pour choisir les mesures d'atténuation appropriées des vulnérabilités présentes dans les types et les architectures de systèmes d'information courants
- Expliquer l'importance de la cryptographie et des services de sécurité qu'elle peut fournir à l'ère du numérique et de l'information
- Evaluer les éléments de sécurité physique par rapport aux besoins des systèmes d'information
- Evaluer les éléments qui composent la sécurité des communications et des réseaux par rapport aux besoins de sécurité de l'information
- Exploiter les concepts et l'architecture qui définissent les systèmes et les protocoles de technologie et de mise en oeuvre associés aux couches 1 à 7 du modèle OSI (Open Systems Interconnection) pour répondre aux besoins de sécurité de l'information
- Déterminer les modèles de contrôle d'accès appropriés pour répondre aux besoins de sécurité de l'entreprise
- Appliquer les modèles de contrôle d'accès physique et logique pour répondre aux besoins de sécurité de l'information
- Différencier les principales méthodes de conception et de validation des stratégies de test et d'audit qui répondent aux exigences de sécurité de l'information
- Appliquer les contrôles et contre-mesures de sécurité appropriés pour optimiser la fonction et la capacité de fonctionnement d'une organisation

- Evaluer les risques liés aux systèmes d'information pour les activités opérationnelles d'une organisation
- Déterminer les contrôles appropriés pour atténuer les menaces et les vulnérabilités spécifiques
- Appliquer les concepts de sécurité des systèmes d'information pour atténuer le risque de vulnérabilité des logiciels et des systèmes tout au long du cycle de vie des systèmes
- Passer l'examen CISSP.

Les compétences visées par cette formation font l'objet d'une évaluation.

À qui s'adresse cette formation ?

Directeurs de l'information, responsables de la sécurité de l'information, responsables de la technologie, responsables / agents de la conformité, architectes de l'information, spécialistes / gestionnaires de l'information, consultants en matière de risques liés à l'information, administrateurs de la sécurité, architectes / analystes de la sécurité, consultants en sécurité, directeurs de la sécurité, ingénieurs en systèmes de sécurité.

Prérequis

Avoir une bonne connaissance des systèmes d'information ainsi qu'une expérience technique et managériale approfondie pour concevoir, développer et gérer la posture de sécurité globale d'une organisation. La lecture du support de cours officiel de l'ISC (CBK) est fortement recommandée.

Le CV de l'apprenant est demandé en amont de la formation pour justifier de son expérience.

Programme

1 Pendant votre formation

Préparation à la certification CISSP

Sécurité et gestion des risques

- Comprendre, adhérer et promouvoir l'éthique professionnelle
- Comprendre et appliquer les concepts de sécurité
- Evaluer et appliquer les principes de gouvernance de la sécurité
- Déterminer la conformité et les autres exigences
- Comprendre les questions juridiques et réglementaires relatives à la sécurité de l'information dans un contexte global
- Comprendre les exigences relatives aux types d'enquêtes

- Elaborer, documenter et mettre en oeuvre une politique, des normes, des procédures et des directives en matière de sécurité
- Identifier, analyser et classer par ordre de priorité les besoins en matière de Business Continuity (CB)
- Contribuer aux politiques et procédures de sécurité du personnel et les faire respecter
- Comprendre et appliquer les concepts
 - De gestion des risques
 - De méthodologies de modélisation des menaces
- Appliquer les concepts de la Supply Chain Risk Management (SCRM)
- Etablir et maintenir un programme de sensibilisation, d'éducation et de formation à la sécurité

Sécurité des actifs

- Identifier et classer les informations et les actifs
- Etablir les exigences en matière de traitement des informations et des actifs
- Fournir des ressources en toute sécurité
- Gérer le cycle de vie des données
- Assurer une conservation appropriée des actifs
 - End-of-Life (EOL)
 - End-of-Support (EOS)
- Déterminer les contrôles de sécurité des données et les exigences de conformité

Architecture et ingénierie de la sécurité

- Rechercher, mettre en oeuvre et gérer des processus d'ingénierie en utilisant des principes de conception sécurisés
- Comprendre les concepts fondamentaux des modèles de sécurité (Biba, Star Model, Bell-La Padula...)
- Sélectionner les contrôles en fonction des exigences de sécurité des systèmes
- Comprendre les capacités de sécurité des systèmes d'information (la protection de la mémoire, Trusted Platform Module, le cryptage / décryptage...)
- Evaluer et atténuer les vulnérabilités des architectures de sécurité, des conceptions et des éléments de solution
- Sélectionner et déterminer les solutions cryptographiques
- Comprendre les méthodes d'attaques cryptographiques
- Appliquer les principes de sécurité à la conception des sites et des installations
- Concevoir des contrôles de sécurité pour les sites et les installations

Sécurité des communications et des réseaux

- Evaluer et mettre en oeuvre les principes de conception sécurisée dans les architectures de réseau
- Sécuriser les composants de réseau
- Mettre en oeuvre des canaux de communication sécurisés conformément à la conception

Gestion des identités et des accès (IAM)

- Contrôler l'accès physique et logique aux actifs

- Gérer l'identification et l'authentification des personnes, des appareils et des services
- Identité fédérée avec un service tiers
- Mettre en oeuvre et gérer les mécanismes d'autorisation
- Gérer le cycle de vie du provisionnement des identités et des accès
- Mettre en oeuvre des systèmes d'authentification

Evaluation et test de sécurité

- Concevoir et valider des stratégies d'évaluation, de test et d'audit
- Effectuer des tests de contrôle de la sécurité
- Collecter des données sur les processus de sécurité (techniques et administratifs...)
- Analyser les résultats des tests et générer un rapport
- Conduire ou faciliter les audits de sécurité

Opérations de sécurité

- Comprendre et respecter les enquêtes
- Mener des activités de journalisation et de surveillance
- Effectuer la gestion de la configuration (provisionnement, "baselining", automatisation)
- Appliquer les concepts fondamentaux des opérations de sécurité
- Appliquer la protection des ressources
- Gérer les incidents
- Exploiter et assurer la maintenance des mesures de détection et de prévention
- Mettre en oeuvre et soutenir la gestion des correctifs et des vulnérabilités
- Comprendre et participer aux processus de gestion du changement
- Mettre en oeuvre des stratégies de récupération
- Mettre en oeuvre des processus de reprise après sinistre (Disaster Recovery)
- Tester les plans de reprise après sinistre (Disaster Recovery Plans)
- Participer à la planification et aux exercices de continuité des activités (Business Continuity)
- Mettre en oeuvre et gérer la sécurité physique
- Répondre aux préoccupations en matière de sûreté et de sécurité du personnel

Sécurité du développement de logiciel

- Comprendre et intégrer la sécurité dans le cycle de vie du développement de logiciel (Software Development Life Cycle)
- Identifier et appliquer les contrôles de sécurité dans les écosystèmes de développement de logiciel
- Evaluer
 - L'efficacité de la sécurité logicielle
 - L'impact sur la sécurité des logiciels acquis
- Définir et appliquer des directives et des normes de codage sécurisé

Passage de la certification

- Cette formation comprend le voucher nécessaire à l'inscription et au passage (ultérieur) de l'examen
- Ce dernier ne pourra être passé qu'en présentiel uniquement, dans un centre Pearson Vue Select agréé
- Le format de l'examen (en anglais) sera sous forme de questionnaire en ligne et durera en moyenne 3h00
- Il s'agit d'un QCM de 100 à 150 questions (70% de bonnes réponses sont nécessaires pour l'obtention de la certification)

Financement

Plusieurs dispositifs de financement sont accessibles via les OPCO (Opérateurs de Compétences), organismes agréés par le ministère du Travail dont le rôle est d'accompagner, collecter et gérer les contributions des entreprises au titre du financement de la formation professionnelle.

Pour plus d'information, une équipe de gestionnaires SKOLAE Formation spécialisée vous accompagne dans le choix de vos formations et la gestion administrative.

[Nous contacter pour en savoir plus →](#)

Modalités pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2I, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

* nous consulter pour la faisabilité en distanciel

** ratio variable selon le cours suivi

Accessibilité aux personnes en situation de handicap

Détails de la session

Du 2 novembre 2026 au 6 novembre 2026 (5 jours / 35 heures)

Paris La Défense

Du 2 novembre 2026 au 6 novembre 2026 **Paris La Défense**

- 2 novembre 2026 9h00 – 15h00
- 3 novembre 2026 9h00 – 15h00
- 4 novembre 2026 9h00 – 15h00
- 5 novembre 2026 9h00 – 15h00
- 6 novembre 2026 9h00 – 15h00