

# Préparation à la Certification CISSP (Information Systems Security Professionnal)

La certification des professionnels de la Sécurité de l'information

 Présentiel ou en classe à distance



5 jours (35 h)

Prix inter : 4.090,00 € HT  
Forfait intra : 12.390,00 € HT

Réf.: MG211

La certification de référence CISSP® (Certified Information Systems Security Professional) est indépendante, pragmatique et internationalement reconnue. Créée et maintenue par des professionnels de la sécurité informatique en exercice, elle permet d'étalonner son niveau de compétence selon 3 axes : les connaissances techniques, les capacités d'analyse des risques et les aptitudes à l'audit des systèmes. La certification CISSP n'atteste pas seulement d'une bonne connaissance des technologies, elle démontre surtout une réelle capacité à les imbriquer et à les assembler pour répondre au mieux aux besoins des entreprises et organisations en matière de sécurité.

Cette formation prépare à la certification Certified Information Systems Security Professional (CISSP).

## A qui s'adresse cette formation ?



### Pour qui

- RSSI, DSI
- Consultants / Auditeurs
- Administrateurs Système et réseaux



### Prérequis

- Justifier de cinq ans d'expérience professionnelle minimum dans au moins 2 des 8 domaines du CBK®
- **Disposez-vous des connaissances nécessaires pour suivre cette formation ? Testez-vous !**

## Programme

### 1 - Sécurité des informations et gestion des risques

- Les concepts de confidentialité, intégrité et disponibilité
- Les principes de gouvernance de la sécurité
- La conformité
- Les questions légales et réglementaires concernant la sécurité de l'information dans un contexte global
- L'éthique professionnelle
- La politique de sécurité, les standards, les procédures et les guidelines
- Les exigences de continuité d'activité
- Les politiques de sécurité du personnel
- Les concepts de management des risques
- Le modèle de menace
- Les considérations de risque de sécurité dans la stratégie d'acquisition
- La sensibilisation, la formation et l'éducation à la sécurité de l'information

### 2 - La sécurité des assets

- Classification de l'information et support des assets
- Le maintien de la propriété
- Protéger la confidentialité
- Assurer la rétention appropriée

- Les mesures de sécurité des données
- Les exigences de manipulation

### **3 - Ingénierie de la sécurité**

- Les processus d'engineering et les principes de conception sécurisée
- Comprendre les concepts fondamentaux des modèles de sécurité
- Les mesures et contre-mesures
- Les possibilités de sécurités offertes par les systèmes d'information
- Les vulnérabilités de sécurité des architectures, des conceptions, des solutions
- Evaluer et réduire les vulnérabilités de sécurité des systèmes web, mobiles et des systèmes embarqués
- La cryptographie
- Les principes de sécurité au site et à la conception de l'installation
- La sécurité physique

### **4 - Sécurité des télécommunications et des réseaux**

- 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

### **5 - La gestion des identités et des accès**

- Contrôle d'accès physique et logique aux assets
- Gérer l'identification et l'authentification des personnes et des équipements
- L'identité en tant que service
- Les services d'identité tiers
- Les mécanismes d'autorisation
- Les attaques au contrôle d'accès
- Le cycle de vie des identités et du provisionnement des accès

### **6 - Évaluation de la sécurité et tests**

- Les stratégies d'évaluation et de test de sécurité
- Tests de mesures de sécurité
- Les données des processus de sécurité
- Les résultats des tests
- Les audits internes ou third-party

### **7 - Continuité des opérations et plan de reprise**

- Les investigations
- Les exigences des types d'investigations
- Les activités de monitoring et de logging
- Le provisionnement des ressources
- Les concepts fondamentaux de sécurité des opérations
- Les techniques de protection de ressources
- La gestion de incidents
- Opérer et maintenir des mesures de sécurité préventives
- La gestion des patches et vulnérabilités
- Les processus de gestion des changements
- Les stratégies de reprise
- Les stratégies de reprise après sinistre
- Les plans de reprise après sinistre
- Le Plan de Continuité d'Activité
- La gestion de la sécurité physique
- Les problèmes de sécurité du personnel

### **8 - La sécurité du développement logiciel**

- La sécurité dans le cycle de vie de développement logiciel
- Les mesures de sécurité dans les environnements de développement
- L'efficacité de la sécurité du logiciel
- Evaluer l'impact de la sécurité d'un logiciel acquis



### **Les objectifs de la formation**

- Connaître les thèmes, les domaines et rubriques du Common Body of Knowledge (CBK®)
- Maîtriser les fondamentaux de la sécurité des SI
- Se préparer à l'examen de certification CISSP



## Evaluation

- Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.



## Les points forts de la formation

- Le contenu de la formation est sans cesse remanié et mis à jour pour refléter les dernières évolutions des questions de sécurité, des préoccupations et des contre-mesures actuelles.
- La formation est un véritable lieu d'échange où chaque participant est appelé à intervenir sur différents sujets des domaines du CBK.
- L'inscription à l'examen n'est pas comprise dans le prix de la formation, pour passer la certification, chaque participant doit s'inscrire sur le site de l'ISC2 et déposer un dossier d'éligibilité.
- 87% des participants à cette formation se sont déclarés satisfaits ou très satisfaits au cours des 12 derniers mois.



## Dates et villes 2026 - Référence MG211



Dernières places disponibles



Session garantie

### Rouen

du 26 janv. au 30 janv.

du 8 juin au 12 juin

du 5 oct. au 9 oct.

### Nantes

du 26 janv. au 30 janv.

du 8 juin au 12 juin

du 5 oct. au 9 oct.

### A distance

du 26 janv. au 30 janv.

du 8 juin au 12 juin

du 5 oct. au 9 oct.

du 23 mars au 27 mars

du 20 juil. au 24 juil.

du 14 déc. au 18 déc.

### Paris

du 26 janv. au 30 janv.

du 8 juin au 12 juin

du 5 oct. au 9 oct.

du 23 mars au 27 mars

du 20 juil. au 24 juil.

du 14 déc. au 18 déc.

### Lyon

du 26 janv. au 30 janv.

du 8 juin au 12 juin

du 5 oct. au 9 oct.

### Rennes

du 26 janv. au 30 janv.

du 8 juin au 12 juin

du 5 oct. au 9 oct.

## Bordeaux

du 26 janv. au 30 janv.

du 8 juin au 12 juin

du 5 oct. au 9 oct.

## Sophia Antipolis

du 26 janv. au 30 janv.

du 8 juin au 12 juin

du 5 oct. au 9 oct.

## Strasbourg

du 26 janv. au 30 janv.

du 8 juin au 12 juin

du 5 oct. au 9 oct.

## Aix-en-Provence

du 23 mars au 27 mars

du 20 juil. au 24 juil.

du 14 déc. au 18 déc.

## Lille

du 23 mars au 27 mars

du 20 juil. au 24 juil.

du 14 déc. au 18 déc.

## Marseille

du 23 mars au 27 mars

du 20 juil. au 24 juil.

du 14 déc. au 18 déc.

## Toulouse

du 23 mars au 27 mars

du 20 juil. au 24 juil.

du 14 déc. au 18 déc.