FORMATION PRATIQUE · PRÉPARATION À LA CERTIFICATION

CISSP, sécurité des SI, préparation à la certification ISC2

Certification **ISC2** — CISSP® · Préparation à l'examen

DURÉE	MODALITÉ	RÉFÉRENCE	PRIX
5 jours 35h00 de formation	**Pratique** Présentiel / à distance	**CIS** Certification ISC2	**2 650 000 FCFA** H.T. par participant

Ce stage détaille les concepts de sécurité pour l'obtention de la certification CISSP. Il vous préparera au passage de l'examen en couvrant l'ensemble du Common Body of Knowledge (CBK), le tronc commun de connaissances en sécurité défini par l'International Information Systems Security Certification Consortium ISC2.

01 Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- Connaître le Common Body of Knowledge de la sécurité IT
- Développer une vision globale des enjeux de sécurité IT
- Approfondir les connaissances des huit domaines du CISSP
- Se préparer à l'examen de certification du CISSP

02 Le programme en bref

01 Sécurité du SI et le CBK de l'ISC2

02 Gestion de la sécurité et sécurité des opérations

03 Architecture, modèles de sécurité et contrôle d'accès

04 Cryptographie et sécurité des développements

05 Sécurité des télécoms et des réseaux

06 Continuité des activités, loi, éthique et sécurité physique

PUBLIC CONCERNÉ

Responsables de la sécurité des SI ou toute autre personne jouant un rôle dans la politique de sécurité des SI.

PRÉREQUIS

Connaissances de base sur les réseaux et les systèmes d'exploitation ainsi qu'en sécurité de l'information. Connaissances de base des normes en audit et en continuité des affaires.

VOS FORMATEURS

Des consultants spécialistes du domaine, validés par notre équipe pédagogique, avec cinq à dix ans d'expérience terrain au minimum.

02 Programme détaillé

6 modules · 5 jours · 35h00

1 Sécurité du SI et le CBK de l'ISC2

- La sécurité des Systèmes d'Information.
- Le pourquoi de la certification CISSP.
- Présentation du périmètre couvert par le CBK.

2 Gestion de la sécurité et sécurité des opérations

- Pratiques de gestion de la sécurité. La rédaction de politiques, directives, procédures et standards en sécurité.
- Le programme de sensibilisation à la sécurité, pratiques de management, gestion des risques, etc.
- Sécurité des opérations : mesures préventives, de détection et correctives, rôles et responsabilités des acteurs.
- Les meilleures pratiques, la sécurité lors de l'embauche du personnel, etc.

3 Architecture, modèles de sécurité et contrôle d'accès

- Architecture et modèles de sécurité : architecture de système, modèles théoriques de sécurité de l'information.
- Les méthodes d'évaluation de systèmes, modes de sécurité opérationnels, etc.
- Systèmes et méthodologies de contrôle d'accès. Les catégories et types de contrôles d'accès.
- Accès aux données et aux systèmes, systèmes de prévention des intrusions (IPS) et de détection d'intrusions (IDS).
- Journaux d'audit, menaces et attaques reliés au contrôle des accès, etc.

4 Cryptographie et sécurité des développements

- Cryptographie. Les concepts, cryptographie symétrique et asymétrique.
- Les fonctions de hachage, infrastructure à clé publique, etc.
- Sécurité des développements d'applications et de systèmes. Les bases de données, entrepôts de données.
- Le cycle de développement, programmation orientée objet, systèmes experts, intelligence artificielle, etc.

5 Sécurité des télécoms et des réseaux

- Sécurité des réseaux et télécoms. Les notions de base, modèle TCP/IP, équipements réseaux et de sécurité.
- Les protocoles de sécurité, les attaques sur les réseaux, sauvegardes des données, technologies sans fil, VPN...

6 Continuité des activités, loi, éthique et sécurité physique

- Continuité des opérations et plan de reprise en cas de désastre.
- Le plan de continuité des activités, le plan de rétablissement après sinistre.
- Les mesures d'urgence, programme de formation et de sensibilisation, communication de crise, exercices et tests.
- Loi, investigations et éthique : droit civil, criminel et administratif, propriété intellectuelle.
- Le cadre juridique en matière d'investigation, règles d'admissibilité des preuves, etc.
- La sécurité physique. Les menaces et vulnérabilités liées à l'environnement d'un lieu, périmètre de sécurité.
- Les exigences d'aménagement, surveillance des lieux, protection du personnel, etc.

03 Informations pratiques

Horaires

Les cours ont lieu de 9h à 12h30 et de 14h à 17h30. Les participants sont accueillis à partir de 8h45. Les pauses et déjeuners sont offerts.

Pour les formations de 4 ou 5 jours, quelle que soit la modalité, les sessions se terminent à 16h le dernier jour.

Solutions de financement

Plusieurs solutions existent pour financer votre formation et dépendent de votre situation professionnelle. Découvrez-les sur notre page « Comment financer sa formation » ou contactez votre conseiller formation.

DATES ET LIEUX — 2026

CLASSE À DISTANCE

14 déc. 2026

MOYENS PÉDAGOGIQUES ET TECHNIQUES

Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les formations pratiques, études de cas ou présentation de cas réels pour les séminaires de formation. À l'issue de chaque formation ou séminaire, Crisalida fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques. Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ (PSH)

Notre référent handicap répond à toute question ou besoin d'aménagement : **crisalid@crisalida.ci**.

CERTIFICATION	Pour passer la certification, vous devez vous inscrire sur le site de l'ISC2 et déposer un dossier d'éligibilité (justifier d'au moins cinq années d'expérience professionnelle cumulée dans au moins deux des huit domaines du programme d'examen ISC2 CISSP). Le passage de l'examen n'est pas compris dans le tarif : il se réserve directement auprès de ISC2. Nous vous indiquons la démarche.
MODALITÉS D'ÉVALUATION	Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques... Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

Besoin d'un parcours sur mesure ?
Crisalida Conseil & Formation construit avec vous des parcours adaptés à vos équipes, en inter, en intra ou à distance.
Votre conseiller formation : crisalid@crisalida.ci.