Date de publication : 25/02/2026

Formation : Certified Information Systems Security Professional (CISSP), préparation à la certification ISC2

Formation officielle ISC2

Formation pratique - 5j - 35h00 - Réf. CIQ

Prix : 4250 € H.T.

NEW

Ce cours couvre l'ensemble du Common Body of Knowledge (CBK) défini par ISC2 et vous prépare à l'examen CISSP, référence internationale en sécurité des systèmes d'information.

Objectifs pédagogiques

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

- Concevoir et piloter un programme global de sécurité de l'information aligné sur les objectifs métier
- Identifier, analyser, évaluer et traiter les risques cyber dans un contexte organisationnel complexe
- Définir et mettre en œuvre une gouvernance de la sécurité intégrée à la stratégie de l'organisation
- Sélectionner et déployer des contrôles de sécurité adaptés aux exigences opérationnelles et réglementaires
- Superviser les opérations de sécurité, la gestion des incidents et la continuité d'activité
- Intégrer la sécurité dans les architectures IT, réseaux et cycles de développement logiciel
- Adopter le raisonnement "manager / décideur" attendu par ISC2 pour réussir l'examen CISSP

Public concerné

Responsables, directeurs, architectes, ingénieurs, analystes, auditeurs et consultants impliqués dans la sécurité des systèmes d'information et des infrastructures réseau. ici

PARTICIPANTS

Responsables, directeurs, architectes, ingénieurs, analystes, auditeurs et consultants impliqués dans la sécurité des systèmes d'information et des infrastructures réseau. ici

PRÉREQUIS

Justifier d'au moins cinq années d'expérience professionnelle cumulée dans au moins deux des huit domaines du programme d'examen ISC2 CISSP.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

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.

Prérequis

Justifier d'au moins cinq années d'expérience professionnelle cumulée dans au moins deux des huit domaines du programme d'examen ISC2 CISSP.

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.

Programme de la formation

1 Domaine 1 : sécurité et gestion des risques

- Éthique professionnelle et Code d'éthique ISC2.
- Principes fondamentaux de la sécurité de l'information.
- Gouvernance de la sécurité et rôles organisationnels.
- Conformité règlementaire et cadres juridiques.
- Enjeux légaux, réglementaires et contractuels.
- Types d'enquêtes et processus associes.
- Politiques, normes, procédures et lignes directrices de sécurité.
- Continuité d'activité et analyse d'impact métier (BIA).
- Sécurité des ressources humaines.
- Gestion du risque : identification, analyse, traitement.
- Modélisation des menaces.
- Gestion des risques de la chaîne d'approvisionnement.
- Sensibilisation, formation et culture sécurité.

2 Domaine 2 : sécurité des actifs

- Identification et classification des actifs.
- Propriété et responsabilité des informations.
- Exigences de protection des données.
- Gestion du cycle de vie des données.
- Conservation, archivage et destruction sécurisée.
- Contrôles de sécurité et conformité des données.

3 Domaine 3 : architecture et ingénierie de sécurité

- Principes de conception et d'ingénierie sécurisées.
- Mode les de sécurité et concepts fondamentaux.
- Sélection des contrôles de sécurité systèmes.
- Sécurité des composants mate riels et logiciels.
- Vulnérabilité s des architectures et conceptions.
- Cryptographie : principes, usages et gouvernance.
- Menaces et attaques cryptographiques.
- Sécurité physique des sites et infrastructures.

4 Domaine 4 : sécurité des communications et des réseaux

- Principes de conception sécurisée des réseaux.
- Sécurisation des équipements et infrastructures réseau.
- Segmentation, isolation et défense en profondeur.
- Canaux de communication sécurisés.

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, ORSYS 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 AUX PERSONNES HANDICAPÉES

Pour toute question ou besoin relatif à l'accessibilité, vous pouvez joindre notre équipe PSH par e-mail à l'adresse psh-accueil@orsys.fr.

5 Domaine 5 : gestion des identités et des accès (IAM)

- Contrôle d'accès physique et logique.
- Identification et authentification.
- Fédérations d'identités et services tiers.
- Autorisation et gestion des droits.
- Cycle de vie des identités et des accès.
- Mécanismes d'authentification.

6 Domaine 6 : évaluation et tests de sécurité

- Stratégies de tests et d'audit de sécurité.
- Tests techniques et organisationnels.
- Collecte et analyse des résultats.
- Rédaction de rapports de sécurité.
- Audits internes et externes.

7 Domaine 7 : opérations de sécurité

- Enquêtes et investigations.
- Journalisation et surveillance.
- Gestion des configurations.
- Opérations de sécurité quotidiennes.
- Protection des ressources.
- Gestion des incidents de sécurité.
- Détection et prévention.
- Gestion des vulnérabilités et correctifs.
- Gestion du changement.
- Continuité d'activité et reprise après sinistre.
- Sécurité physique et environnementale.
- Sécurité du personnel.

8 Préparation à l'examen CISSP

- Présentation de l'examen CISSP (CAT).
- Méthodologie de réponse aux questions.
- Gestion du temps et pièges fréquents.
- Quiz d'évaluation et questions type examen.
- Conseils d'experts certifies CISSP.

Partenariat

Formation officielle dispensée par ACG Cybersecurity, ISC2 Official Training Partner

Options

Certification : 750 € HT

L'examen officiel se déroule en anglais en distanciel et en différé, sous forme d'un QCM d'une durée de 3 heures, comprenant 100 à 150 questions, avec un score minimum requis de 700/1000.

Dates et lieux

CLASSE À DISTANCE
2026 : 15 juin, 31 août, 2 nov.

PARIS LA DÉFENSE
2026 : 15 juin, 31 août, 2 nov.