Organisme de formation professionnelle continue
Numero agrément 91 30 03332 30
France : +33 (0)188 24 70 33 / 34
Site : www.oo2.fr
Mail : contact@oo2.fr

# Devenir responsable de la sécurité de l'information certifié (C|CISO)

## Date et durée

Code formation : SEC21FR
Durée : 5 jours
Nombre d'heures : 35 heures

## Formation avec certification

C|CISO : Certified Chief Information Security Officer

## Description

Le titre de CCISO (*Certified Chief Information Security Officer*) est une **certification individuelle de haut niveau** dans le domaine de la cybersécurité. Elle atteste des compétences d'un responsable de la sécurité de l'information chargé de concevoir et de mettre en œuvre une stratégie de gestion alignée sur les objectifs organisationnels de l'entreprise.
Pour devenir certifié CISO, vous devez posséder de **solides connaissances techniques**, des années d'expérience professionnelle et la capacité de promouvoir la sécurité informatique au sein de toute organisation. Dans ce contexte, cette formation vous prépare à l'examen de certification C|CISO délivré par le EC-Council.
Elle vous permettra d'aborder en détail **les 5 domaines de la sécurité de l'information** sur lesquels se base l'examen *(plus d'infos dans l'onglet certification)*. Ainsi, vous développerez une profonde compréhension de l'audit de sécurité, de la gouvernance, du contrôle et de la gestion, de la planification financière stratégique et bien plus encore.

## Objectifs

A l'issue de la **formation CCISO**, vous atteindrez les objectifs suivants :

- maîtriser les 5 domaines de compétences du programme Certified Chief Information Security Officer (CCISO) ;
- évaluer vos connaissances et vos compétence en sécurité de l'information ;
- comprendre la procédure de certification et les éléments constitutifs de l'examen ;
- réussir l'examen 712-50 et obtenir la certification C|CISO du EC-Council.

*Oo2 est accrédité par EC-Council pour dispenser la formation CCISO. Ce statut garantit la prestation d'un formateur agréé, des supports de cours officiels et des examens de certifications organisés immédiatement en fin de formation.*

Points forts

Une formation qualifiante pour maîtriser les 5 domaines de la sécurité de l'information, des travaux pratiques, un perfectionnement de compétences et une bonne préparation à la certification CCISO.

Certification

## Conditions d'éligibilité

Cette formation de préparation à l'examen CCISO vous permet de vous inscrire à l'examen officiel sur la plateforme ECC Exam du EC-Council. Toutefois, vous devrez **justifier de 5 ans d'expérience professionnelle** dans au moins 3 des 5 domaines de compétence abordés dans cette formation pour recevoir le titre de Certified Chief Information Security Officer (C|CISO).
Si vous n'avez pas le nombre d'années d'expérience exigé, vous pouvez quand même obtenir la certification Associate C|CISO.
En savoir +

## Détails de l'examen C|CISO

**Code de l'examen** : 712-50
**Nombres de questions** : 150 QCM
**Durée** : 2 heures 30
**Validité de la certification :** 3 ans (renouvelable)

Modalités d'évaluation

Quiz / QCM
Travaux Pratiques

Pré-requis

Suivre la **formation CCISO** nécessite le prérequis suivant :

- entre 2 et 5 ans d'expérience minimum dans au moins 1 des 5 domaines aborder pendant ces cours. (requis pour le passage de l'examen CCISO).

Public

**Cette formation s'adresse aux publics suivants :**

- les professionnels informatique ayant une bonne expérience en matière de sécurité de l'information et qui souhaitent approfondir ou valider leurs compétences ;
- les responsables ou les directeurs de la sécurité des systèmes d'information (RSSI) qui souhaitent se préparer à la certification C|CISO (Certified Chief Information Security Officer).

Cette formation s'adresse aux profils suivants

Directeur des Systèmes d'Information (DSI)
Analyste cybersécurité
Architecte informatique / SI

Responsable sécurité informatique
Chef de projet / Responsable de projet
Auditeur interne / externe

Programme

### Domaine 1 :  gouvernance, risques et conformité

- La structure d'un programme de gestion de la sécurité de l'information.
- L'adaptation des stratégies opérationnelles de l'entreprise avec la gouvernance SI.
- La gestion des risques.
- Les lois et les réglementations en gouvernance SI.
- Les procédures de mise en conformité.

### Domaine 2 : contrôles de sécurité de l'information et gestion des audits

- La conception, le déploiement et la gestion des contrôles de sécurité.
- La compréhension des types de contrôles de sécurité et de leurs objectifs.
- La mise en œuvre de systèmes d'assurance pour les contrôles.
- La compréhension des processus de gestion des audits.

### Domaine 3 : gestion et opérations du programme de sécurité

- Les mesures nécessaires pour mettre en place le programme de sécurité des systèmes d'information.
- L'estimation et le contrôle des coûts et du budget des projets.
- La gestion des équipes de projet SI.
- La résolution des conflits et la communication.
- La surveillance de la performance du programme.

### Domaine 4 : compétences clés en sécurité de l'information

- La mise en place du contrôle d'accès.
- L'ingénierie social, les attaques de phishing et le vol d'identité.
- La sécurité physique.
- La reprise après sinistre et la planification de la continuité des activités.
- La gestion des pare-feu et des systèmes de détection et de prévention.
- Les vulnérabilités et les attaques des réseaux sans fil.
- Les virus et autres menace informatique.
- Les bonnes pratique de codage sécurisé et la sécurité des APIs Web.
- Le renforcement de la sécurité des systèmes d'exploitation.
- Les technologies de chiffrement
- L'évaluation de la vulnérabilité et les tests de pénétration.
- La création d'un programme de gestion contre les menaces.
- La réponse aux incidents et la criminalistique informatique.
- La sécurité des applications, de la virtualisation et du cloud computing.
- Les technologies transformatrices.

### Domaine 5 : planification stratégique, finance, achats et gestion des tiers

- La planification stratégique de la sécurité.
- L'alignement des objectifs de l'entreprise sur la tolérance au risque.
- Les nouvelles tendances en matière de sécurité.
- Les indicateurs clés de performance (KPI).
- La planification financière.

- L'élaboration d'analyses de rentabilité en matière de sécurité.
- L'analyse, l'anticipation et l'élaboration d'un budget prévisionnel.
- Le retour sur investissement (ROI) et l'analyse des coûts.
- La gestion de la force de vente.
- Les contraintes relatives à l'intégration de la sécurité dans les accords contractuels et les processus de passation de marchés.