

Chief Information Security Officer (CISO)

Date et durée
Code formation : SEC24FR Durée : 4,5 jours Nombre d'heures : 31 heures
Formation avec certification
PECB Certified Chief Information Security Officer
Description
<p>Le RSSI (Responsable de la Sécurité des Systèmes d'Information), ou CISO (Chief Information Security Officer), est essentiel à la protection des données d'une organisation. Garant de la confidentialité, de l'intégrité et de la disponibilité des informations, il définit la politique de sécurité, gère les risques, assure la conformité (RGPD, etc.), sensibilise les employés et supervise la gestion des incidents. Expert technique, managérial et juridique, il communique efficacement à tous les niveaux de l'entreprise.</p> <p>Cette formation PECB CISO est un programme intensif conçu pour vous permettre d'acquérir les compétences essentielles pour piloter la sécurité de l'information de votre organisation. Vous acquerez une expertise approfondie dans des domaines clés, tels que la conception et la mise en œuvre de programmes de sécurité efficaces, la gestion des risques et la conformité aux normes et réglementations (RGPD, ISO 27001, etc.). Vous maîtriserez également la mise en place de mesures de sécurité robustes, la gestion des incidents et la formation à la sensibilisation à la sécurité pour vos équipes.</p> <p>À l'issue de ces cours de RSSI, vous serez prêt à passer l'examen de certification PECB CISO, une certification reconnue internationalement qui attestera de votre expertise et renforcera votre crédibilité auprès de vos pairs et de votre employeur (<i>en savoir plus dans l'onglet certification</i>).</p>
Objectifs
<p>À l'issue de la formation PECB CISO, vous atteindrez les objectifs suivants :</p> <ul style="list-style-type: none">• comprendre les principes clés et les concepts essentiels de la sécurité de l'information ;• connaître les responsabilités du Responsable de la Sécurité des Systèmes d'Information (RSSI), les enjeux éthiques et les défis liés à cette fonction ;• créer un programme de sécurité de l'information adapté aux besoins spécifiques de l'organisation ;• appliquer les cadres, lois et réglementations en vigueur, et mettre en œuvre des politiques de sécurité efficaces pour garantir la conformité ;• identifier, analyser, évaluer et traiter les risques liés à la sécurité de l'information de manière méthodique et performante ;• se préparer efficacement à l'examen PECB Certified Chief Information Security Officer (CISO).
Points forts

- **Apprenez auprès d'experts reconnus** : nos formateurs et formatrices sont des experts chevronnés dans le domaine de la sécurité de l'information, possédant une expérience significative en entreprise et une connaissance approfondie des dernières tendances.
- **Mettez en pratique vos connaissances** : immergez-vous dans des situations concrètes grâce à des exercices de type dissertation, des QCM et une documentation complète de 450 pages, conçue pour vous préparer aux défis du terrain.
- **Validez votre engagement professionnel** : obtenez 31 crédits de Développement Professionnel Continu (DPC), attestant de votre investissement dans votre carrière et de votre maintien à niveau.
- **Passez la certification PECB CISO sans frais supplémentaires** : la certification PECB CISO, reconnue internationalement, est incluse dans le prix de la formation. En cas d'échec, bénéficiez d'une deuxième chance gratuite dans les 12 mois.
- **Développez votre réseau professionnel** : élargissez votre cercle de contacts en échangeant avec d'autres participants et en rencontrant des experts de la sécurité de l'information, créant ainsi des opportunités de collaboration et d'évolution.

Certification

Cette formation vous permet de passer la certification professionnelle **PECB Chief Information Security Officer (CISO)**. Un code coupon vous sera fourni à la fin du cours afin que vous puissiez programmer votre examen en ligne.

Modalité de l'examen PECB CISO :

L'examen PECB Chief Information Security Officer, **disponible en français, consiste à répondre à un QCM de 80 questions pendant 3 heures** maximum. Il remplit les exigences relatives au programme d'examen et de certification du PECB. Il couvre les domaines de compétences suivants :

- les concepts fondamentaux de la sécurité de l'information ;
- le rôle du RSSI dans un programme de sécurité de l'information ;
- la sélection d'un programme de conformité en matière de sécurité, gestion des risques, architecture et conception de la sécurité ;
- les aspects opérationnels des mesures de sécurité de l'information, de la gestion des incidents et de la gestion des changements ;
- la promotion d'une culture de la sécurité de l'information ;
- le contrôle et l'amélioration d'un programme de sécurité de l'information ;

Après réussite de votre examen, vous pourrez demander l'une des certifications suivantes en fonction de votre expérience professionnelle :

Qualifications	Examens	Expérience professionnelle	Expérience projet SM	Autres exigences
PECB Certified Information Security Officer	Examen PECB Chief Information Security Officer	Aucune	Aucune	Signer le Code de déontologie de PECB
PECB Certified Chief Information Security Officer	Examen PECB Chief Information Security Officer	5 ans dont 2 ans d'expérience en en gestion de la sécurité de l'information	Activités de projet totalisant 300 heures	Signer le Code de déontologie de PECB

Pour en savoir plus sur les modalités, consulter le [règlement d'examen PECB](#) ainsi que le [règlement de certification PECB](#).

Modalités d'évaluation

Quiz / QCM
Travaux Pratiques

Pré-requis

Suivre cette formation nécessite le prérequis suivant :

- des connaissances préalables sur les principes fondamentaux de la sécurité de l'information, tels que les menaces, les vulnérabilités et les risques.

Public

Cette formation s'adresse aux professionnels de la sécurité de l'information qui souhaitent développer leurs compétences en gestion et en leadership, notamment :

- les responsables de la sécurité de l'information ;
- les responsables informatiques ;
- les architectes, analystes et auditeurs de sécurité ;
- les professionnels de la gestion des risques et de la conformité ;
- les RSSI expérimentés ;
- les cadres (DSI, PDG ou directeur d'exploitation) ;
- tout professionnel aspirant à des postes de direction dans la sécurité de l'information.

Programme

Jour 1 : comprendre les fondamentaux de la sécurité de l'information et le rôle d'un RSSI

- Introduction à la sécurité de l'information (enjeux, défis et tendances actuelles).
- Les principes fondamentaux de la sécurité de l'information (confidentialité, intégrité, et disponibilité (CIA)).
- L'identification des menaces et des vulnérabilités (évaluation des risques).
- Le rôle du RSSI (responsabilités, compétences et qualités essentielles).
- L'intégration de l'éthique et du professionnalisme dans la sécurité de l'information.

Jour 2 : élaborer un programme de conformité, gérer les risques, architecturer et concevoir la sécurité

- Les cadres de référence pour la sécurité de l'information (ISO 27001, NIST, etc.).
- Les lois et les réglementations en matière de sécurité de l'information (RGPD, etc.).
- La création d'un programme de conformité (politiques, procédures et contrôles).
- La mise en œuvre de la gestion des risques (identification, analyse, évaluation et traitement).
- L'application de l'architecture et la conception de la sécurité (principes et bonnes pratiques).

Jour 3 : mettre en place des mesures de sécurité, gérer les incidents et les changements

- Le choix des mesures de sécurité techniques (pare-feu, antivirus, chiffrement, etc.).
- La définition des mesures de sécurité organisationnelles (politiques, procédures, formation, etc.).
- La mise en place des mesures de sécurité physiques (contrôle d'accès, surveillance, etc.).
- La gestion des incidents de sécurité (détection, analyse, réponse et récupération).
- La gestion des changements (processus et bonnes pratiques pour minimiser les risques).

Jour 4 : promouvoir la sensibilisation à la sécurité, assurer la surveillance et soutenir l'amélioration continue

- La mise en œuvre de la sensibilisation à la sécurité de l'information : importance et méthodes efficaces.

- La surveillance et le mesurage de la sécurité (indicateurs clés de performance (KPI)).
- L'encouragement à l'amélioration continue de la sécurité (identification des points faibles et actions correctives).
- Le développement du leadership et la communication dans la sécurité de l'information.

Jour 5 (demi-journée) : réussir l'examen de certification PECB CISO

- Révision des points clés abordés tout au long de la formation.
- Présentation détaillée de l'examen (structure, format et thématiques abordées).
- Conseils et astuces pour réussir l'examen (méthodologie, gestion du temps, etc.).

PECB

Contenu de formation proposé en partenariat avec [PECB](#)