



## PECB Certified Lead Cybersecurity Manager

**Maîtriser la capacité à mettre en œuvre et à gérer un programme de cybersécurité basé sur les bonnes pratiques du secteur.**

### **Pourquoi devriez-vous y participer ?**

De nos jours, les organisations sont affectées par l'évolution constante du paysage numérique et sont constamment confrontées à de nouvelles menaces et à des cyberattaques complexes et sophistiquées. Il existe un besoin pressant de personnes qualifiées capables de gérer et de mettre en œuvre efficacement des programmes de cybersécurité solides pour contrer ces menaces. Notre formation Lead Cybersecurity Manager a été développée pour répondre à ce besoin.

En suivant la formation PECB Certified Lead Cybersecurity Manager, les participants apprendront les concepts fondamentaux de la cybersécurité, les stratégies, les méthodologies et les techniques utilisées pour établir et gérer effectivement un programme de cybersécurité conformément aux lignes directrices des normes internationales de cybersécurité, telles que la norme ISO/IEC 27032 et le Cadre de cybersécurité du NIST. En outre, cette formation permet aux participants d'améliorer la préparation et la résilience de leur organisation face aux cybermenaces. Les participants seront bien préparés pour soutenir les efforts constants de leur organisation en matière de cybersécurité et apporter une contribution précieuse dans le paysage actuel de la cybersécurité en constante évolution.



## À qui s'adresse la formation ?

Cette formation est destinée aux :

- Managers et dirigeants impliqués dans la gestion de la cybersécurité
- Personnes chargées de la mise en œuvre pratique des stratégies et mesures de cybersécurité
- Professionnels de l'informatique et de la sécurité qui souhaitent faire progresser leur carrière et contribuer plus efficacement aux efforts de cybersécurité
- Professionnels responsables du management des risques de cybersécurité et de la conformité au sein des organisations
- Cadres dirigeants ayant un rôle crucial dans les processus décisionnels liés à la cybersécurité

## Programme de la formation

Durée : 5 jours

### Jour 1 | Introduction à la cybersécurité et lancement de la mise en œuvre d'un programme de cybersécurité

- Objectifs et structure de la formation
- Normes et cadres réglementaires
- Concepts fondamentaux de la cybersécurité
- Programme de cybersécurité
- L'organisation et son contexte
- Gouvernance en matière de cybersécurité

### Jour 2 | Rôles et responsabilités en matière de cybersécurité, management des risques et mécanismes d'attaque

- Rôles et responsabilités en matière de cybersécurité
- Gestion des actifs
- Management du risque
- Mécanismes d'attaque

### Jour 3 | Mesures, communication, sensibilisation et formation en matière de cybersécurité

- Mesures de cybersécurité
- Communication sur la cybersécurité
- Sensibilisation et formation

### Jour 4 | Gestion des incidents de cybersécurité, surveillance et amélioration continue

- État de préparation des TIC pour la continuité d'activité
- Gestion des incidents de cybersécurité
- Tests de cybersécurité
- Évaluation et rapports sur les performances et les métriques en matière de cybersécurité
- Amélioration continue
- Clôture de la formation

### Jour 5 | Examen de certification



## Objectifs de la formation

À l'issue de cette formation, vous pourrez :

- Expliquer les concepts fondamentaux, les stratégies, les méthodologies et les techniques utilisés pour mettre en œuvre et gérer un programme de cybersécurité
- Expliquer le lien entre la norme ISO/IEC 27032, le Cadre de cybersécurité du NIST et d'autres normes et cadres pertinents
- Comprendre le fonctionnement d'un programme de cybersécurité et ses composantes
- Accompagner une organisation dans le fonctionnement, le maintien et l'amélioration continue de son programme de cybersécurité

## Examen

Durée : 3 heures

L'examen « PECB Certified Lead Cybersecurity Manager » est conforme aux exigences du Programme d'examen et de certification (PEC) de PECB. Il couvre les domaines de compétences suivants :

- Domaine 1** | Concepts fondamentaux de la cybersécurité
- Domaine 2** | Lancement du programme de cybersécurité et de la gouvernance en matière de cybersécurité
- Domaine 3** | Définition des rôles et responsabilités en matière de cybersécurité et management des risques
- Domaine 4** | Sélection des mesures de cybersécurité
- Domaine 5** | Mise en place des programmes de communication et de formation en matière de cybersécurité
- Domaine 6** | Intégration du programme de cybersécurité dans la gestion de la continuité d'activité et la gestion des incidents
- Domaine 7** | Évaluation des performances et amélioration continue du programme de cybersécurité

Pour des informations spécifiques sur les types d'examens, les langues disponibles et d'autres détails, veuillez consulter [la liste des examens du PECB](#) et [les règles et politiques d'examen](#).



## Certification

Après avoir réussi l'examen, vous pourrez demander l'une des certifications indiquées dans le tableau ci-dessous. Un certificat vous sera délivré si vous remplissez toutes les exigences relatives à la certification sélectionnée.

Certification	Examen	Expérience professionnelle	Expérience dans la gestion des projets de la cybersécurité	Expérience en gestion des risques
<b>PECB Certified Provisional Cybersecurity Manager</b>	Examen PECB Certified Provisional Cybersecurity Manager	Aucune	Aucune	Signer le Code de déontologie de PECB
<b>PECB Certified Cybersecurity Manager</b>	Examen PECB Certified Cybersecurity Manager	Deux ans : Au moins un an d'expérience professionnelle dans le domaine de la cybersécurité	Au moins 200 heures	Signer le Code de déontologie de PECB
<b>PECB Certified Lead Cybersecurity Manager</b>	Examen PECB Certified Cybersecurity Manager	Cinq ans : Au moins deux ans d'expérience professionnelle dans le domaine de la cybersécurité	Au moins 300 heures	Signer le Code de déontologie de PECB
<b>PECB Certified Senior Lead Cybersecurity Manager</b>	Examen PECB Certified Cybersecurity Manager	Dix ans : Au moins sept ans d'expérience professionnelle dans le domaine de la cybersécurité	Au moins 1000 heures	Signer le Code de déontologie de PECB

Pour plus d'informations sur les certifications en cybersécurité et le processus de certification PECB, veuillez consulter les [Politiques et règlements relatifs à la certification](#).

## Informations générales

- Les frais d'examen et de certification sont inclus dans le prix de la formation
- Les participants recevront des supports de formation complets, avec plus de 400 pages de contenu comprenant des exemples pratiques, des exercices et des quiz
- Les participants qui suivent la formation recevront une attestation d'achèvement de formation valant 31 unités de FPC (Formation professionnelle continue)
- Les candidats qui ont suivi toute la formation, mais n'ont pas réussi l'examen peuvent le repasser gratuitement dans les 12 mois suivant la date de l'examen initial