# 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 organismes sont affectés par l'évolution constante du paysage numérique et sont constamment confrontés à de nouvelles menaces et à des cyberattaques de plus en plus complexes et perfectionnées. Le besoin en personnel qualifié capable de gérer et de mettre en œuvre efficacement des programmes de cybersécurité robustes pour contrer ces menaces est pressant. La formation « Lead Cybersecurity Manager » que nous proposons a été conçue pour répondre à ce besoin.

Les participants à la formation PECB Certified Lead Cybersecurity Manager acquièrent les concepts, stratégies, méthodologies et techniques fondamentaux de la cybersécurité utilisés pour établir et gérer efficacement un programme de cybersécurité basé sur les directives des normes internationales de cybersécurité, tels que la norme ISO/IEC 27032 et le cadre de cybersécurité du NIST. De plus, cette formation renforce la capacité des participants à améliorer la préparation et la résilience de leur organisme face aux cybermenaces. Les participants sont ainsi mieux préparés à soutenir les efforts continus de leur organisme en matière de cybersécurité et à apporter une contribution précieuse dans le paysage actuel de la cybersécurité, qui est e constante évolution.

## À qui s'adresse la formation ?

Cette formation s'adresse :

- Aux responsables et dirigeants impliqués dans la gestion de la cybersécurité
- Aux personnes chargées de la mise en œuvre pratique des stratégies et des mesures de cybersécurité
- Aux professionnels de l'informatique et de la sécurité désireux de booster leur carrière et de contribuer plus efficacement aux efforts de cybersécurité
- Aux professionnels chargés de gérer le risque de cybersécurité et la conformité au sein des organismes
- Aux cadres dirigeants qui ont un rôle crucial dans les processus de prise de décision liés à la cybersécurité

## Programme de la formation

**Durée : 5 jours**

### Jour 1 | Introduction to cybersecurity and initiation of a cybersecurity program implementation

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

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

- Rôles et responsabilités en matière de cybersécurité
- Gestion des biens
- Gestion des risques
- Les mécanismes d'attaque

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

- Mesures de cybersécurité
- Communication relative à la cybersécurité
- Sensibilisation et formation

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

- État de préparation des TIC pour la continuité d'activité
- Management des incidents de cybersécurité
- Tests de cybersécurité
- Mesurer et rendre compte des performances et des paramètres 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, les participants seront capables de :

- Expliquer les concepts fondamentaux, les stratégies, les méthodologies et les techniques utilisés pour mettre en œuvre et gérer un programme de cybersécurité
- Expliquer la corrélation entre la norme ISO/IEC 27032, le cadre de cybersécurité du NIST ainsi que d'autres normes et cadres pertinents
- Comprendre le fonctionnement d'un programme de cybersécurité et ses composantes
- Soutenir un organisme dans l'exploitation, la maintenance et l'amélioration continue de son programme de cybersécurité

## Examen

**Durée : 3 heures**

L'examen de certification « PECB Certified ISO/IEC 27001 Lead Auditor » répond pleinement aux exigences du Programme d'examen et de certification PECB (ECP, Examination and Certification Program). L'examen couvre les domaines de compétence 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 gestion des risques** |
| **Domaine 4** | **Sélection des mesures de cybersécurité** |
| **Domaine 5** | **Mise en place de programmes de communication et de formation en matière de cybersécurité** |
| **Domaine 6** | **Intégration du programme de cybersécurité dans la gestion de la continuité des activités et le management des incidents** |
| **Domaine 7** | **Évaluation des performances du programme de cybersécurité et amélioration continue de celui-ci** |

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

Une fois l'examen réussi, vous pouvez demander l'un des titres figurant dans le tableau ci-dessous. Vous recevrez une certification une fois que vous aurez rempli toutes les conditions requises pour le titre sélectionné.

| Titre de compétence | Examen | Expérience professionnelle | Expérience en projet de cybersécurité | Autres exigences |
|---|---|---|---|---|
| **PECB Certified Provisional Cybersecurity Manager** | Examen PECB Certified Provisional Cybersecurity Manager | Aucune | Aucune | Signer le Code de déontologie de PECB |
| **PECB Certified Lead Cybersecurity Manager** | Examen PECB Certified Provisional 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 |

Pour plus d'informations sur les certifications en cybersécurité et le processus de certification PECB, veuillez vous référer aux règles et politiques de certification.

## Informations générales

- Les frais de certification et d'examen sont inclus dans le prix de la formation.
- Les participants recevront des supports de formation complets, comprenant plus de 400 pages de contenu, y compris des exemples pratiques, des exercices et des quiz.
- Une attestation de suivi de cours valant 31 crédits CPD (Continuing Professional Development) sera délivrée aux participants ayant suivi la formation.
- Les candidats qui ont suivi la formation, mais n'ont pas réussi l'examen peuvent le repasser sans frais supplémentaires dans un délai de 12 mois à compter de la date de l'examen initial.