



## Lead Cybersecurity Manager selon l'ISO 27032

### Date et durée

Code formation : ISO27032M

Durée : 5 jours

Nombre d'heures : 35 heures

### **Formation avec certification**

### **PECB Certified Lead Cybersecurity Manager**

### Description

De nos jours, les technologies de l'information évoluent et **les menaces de cyberattaques sont de plus en plus nombreuses et nuisibles**. L'actualité informatique prouve qu'aucun organisme, ni aucun gouvernement, ne sont à l'abri d'une cyberattaque. Une attaque informatique peut avoir des conséquences désastreuses sur le fonctionnement et la confidentialité d'un organisme. Ainsi, il est primordial de **savoir gérer efficacement un programme de cybersécurité** dans une entreprise.

La formation Lead Cybersecurity Manager vous permet d'approfondir vos connaissances en matière de cybersécurité. Elle vous familiarise avec **les concepts de base, les stratégies, les méthodologies** et les techniques essentielles à la création et à la gestion d'un programme de cybersécurité performant. Axée sur les normes internationales telles que **l'ISO/IEC 27032:2023 et le NIST Cybersecurity Framework**, cette formation vous aidera à renforcer l'état de préparation et la résilience de votre entreprise face aux cyber-menaces.

A l'issue de ces cours de cybersécurité, vous serez également prêt pour **passer l'examen PECB Certified Provisional Cybersecurity Manager**. Cet examen en ligne vous permettra de recevoir une des 2 certifications associées, en fonction de votre expérience (*en savoir dans l'onglet certification*).

### Objectifs

A l'issue de la **formation PECB Lead Cybersecurity Manager**, vous atteindrez les objectifs suivants :

- comprendre et décrire les concepts fondamentaux, les stratégies, les méthodes et les techniques nécessaires à la mise en œuvre et la gestion d'un programme de cybersécurité ;
- connaître les synergies entre la norme ISO/IEC 27032:2023, le cadre de cybersécurité du NIST et d'autres normes et référentiels applicables ;
- comprendre le processus et les éléments techniques d'un programme de cybersécurité ;
- savoir accompagner une entreprise dans l'exploitation, la maintenance et l'amélioration continue de son programme de cybersécurité ;
- réussir l'examen PECB Certified Provisional Cybersecurity Manager et obtenir votre certification.

### Points forts

Travaux pratiques basés sur des cas réels avec une documentation de 400 pages ; 31 crédits CPD ; Examen de certification PECB compris dans le prix de la formation ; En cas d'échec, repassez-le sans frais dans les 12 mois.

### Certification

L'examen se déroule **entièrement en ligne**, vous offrant la flexibilité de le programmer à la date et à l'heure de votre choix. Il s'agit d'un examen de type "essay type" : vous devrez rédiger des réponses structurées aux différentes questions posées. Cette formation vous prépare à passer l'examen **PECB Certified Provisional Cybersecurity Manager**, lequel remplit les exigences rigoureuses du programme d'examen et de certification du PECB. Le cursus couvre les 7 domaines de compétences suivants :

- les concepts fondamentaux de la cybersécurité ;
- le lancement d'un programme de cybersécurité et sa gouvernance ;
- la définition des rôles et des responsabilités en matière de cybersécurité et la gestion des risques
- la sélection des mesures de cybersécurité ;
- la mise en œuvre de programmes de communication et de formation en matière de cybersécurité ;
- l'intégration d'un programme de cybersécurité dans le cadre de la continuité des activités et de la gestion des incidents ;
- l'évaluation des performances d'un programme de cybersécurité et l'amélioration continue de ses performances.

Après avoir réussi cet **examen de 3 heures**, vous pourrez demander les 2 certifications suivantes en fonction de votre expérience professionnelle :

| Qualification                                           | Examen                                                  | Expérience professionnelle                                        | Expérience en projet de cybersécurité     | Autres exigences                      |
|---------------------------------------------------------|---------------------------------------------------------|-------------------------------------------------------------------|-------------------------------------------|---------------------------------------|
| <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 Lead Cybersecurity Manager</b>        | Examen PECB Certified Provisional Cybersecurity Manager | 5 ans dont 2 ans d'expérience dans le domaine de la cybersécurité | 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

Etude de cas

#### Pré-requis

Pour suivre la **formation Lead Cybersecurity Manager** il faut avoir des notions de base en sécurité des SI ou en cybersécurité.

#### Public

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

- les managers et responsables qui participent à la gestion des activités de cybersécurité ;
- les personnes chargées de mettre en œuvre des stratégies et des mesures de cybersécurité ;
- les professionnels en informatique et en sécurité qui souhaitent booster leur carrière pour pouvoir participer efficacement à la mise en place de mesures de cybersécurité ;
- les responsables des risques et de la conformité informatique ;
- les dirigeants amenés à prendre des décisions importantes en matière de cybersécurité.

**Cette formation s'adresse aux profils suivants**

## **Programme**

### **Jour 1 : introduction à la cybersécurité et à l'implantation d'un programme**

- Les objectifs et le déroulement de la formation.
- Les normes et les réglementations en cybersécurité.
- Les concepts fondamentaux de la cybersécurité.
- Qu'est-ce qu'un programme de cybersécurité ?
- L'organisme et son contexte.
- Qu'est-ce que la gouvernance de la cybersécurité ?

### **Jour 2 : compréhension des rôles et des responsabilités, de la gestion des risques et des mécanismes d'attaque**

- Les rôles et les responsabilités de chacun en matière de cybersécurité.
- La gestion des actifs.
- La gestion des risques.
- Les mécanismes d'attaque.

### **Jour 3 : compréhension des mesures de sécurité, de la communication, de la sensibilisation et de la formation**

- Le choix et la mise en place de mesures de cybersécurité.
- La mise en place d'un programme de communication.
- La sensibilisation et la mise en place d'un programme de formation pour le personnel.

### **Jour 4 et 5 : gestion des incidents, suivi et amélioration continue**

- La préparation des technologies de l'information et de la communication (TIC) pour la continuité des activités.
- La gestion des incidents de cybersécurité.
- Les tests de cybersécurité.
- L'évaluation et la rédaction de rapports sur les performances et les paramètres de la sécurité informatique.
- La mise en place d'un processus d'amélioration continue.
- Préparation au passage de l'examen PECB Certified Provisional Cybersecurity Manager.

**A savoir : l'examen et le support du cours PECB Lead Cybersecurity Manager sont disponibles en français et en anglais.**

# PECB

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