

# ISO 27032 - Lead Cybersecurity Manager

Référence : SECLCM

Durée : 5 jours

Certification : ISO 27032

Code CPF : RS4316

## CONNAISSANCES PREALABLES

- Aucune.

## PROFIL DES STAGIAIRES

- 1- Les professionnels en cybersécurité. • 2- Les experts de la sécurité de l'information. • 3- Les responsables de projet souhaitant gérer un programme de cybersécurité. • 4- Les experts techniques souhaitant se préparer à occuper une fonction en cybersécurité. • 5- Les personnes responsables du développement d'un programme de cybersécurité.

## OBJECTIFS

- Comprendre et acquérir des connaissances générales en matière de composants et de fonctionnement d'un programme de cybersécurité en conformité avec la norme ISO/IEC 27032 et au cadre de cybersécurité NIST. • Expliquer le but, le contenu et le lien entre la norme ISO/IEC 27032 et le cadre de cybersécurité NIST, ainsi qu'avec d'autres normes et cadres de fonctionnement. • Maîtriser les concepts, les approches, les normes, les méthodes et les techniques permettant d'établir, mettre en oeuvre et gérer efficacement un programme de cybersécurité au sein d'une organisation. • Etre en mesure d'interpréter les exigences de la norme ISO/IEC 27032 dans un contexte spécifique d'une organisation. • Acquérir l'expertise nécessaire pour planifier, mettre en oeuvre, gérer, contrôler et maintenir un programme de cybersécurité, selon la norme ISO/IEC 27032 et le cadre de cybersécurité NIST. • Développer l'expertise nécessaire pour conseiller une organisation en matière de meilleures pratiques de gestion de la cybersécurité. • Renforcer les compétences personnelles qui sont nécessaires pour l'établissement et le maintien d'un programme de cybersécurité.

## CERTIFICATION PREPAREE

- Certification PECB : Fondamentaux de la cyber sécurité. Pour en savoir plus sur cette certification, [cliquez ici](#) et accédez aux informations complètes fournies par France Compétences

## METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

## FORMATEUR

Consultant-Formateur expert Management de la sécurité

## METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

## CONTENU DU COURS

### JOUR 1 : Introduction à norme ISO 27032, initiation d'un programme de cybersécurité

- Objectifs et structure de la formation
- Cadre normatif et réglementaire
- Concepts fondamentaux et définitions de la cybersécurité

- Programme de cybersécurité
- Initiation d'un programme de cybersécurité
- Analyse de l'organisation
- Leadership

## **JOUR 2 : Politiques de cybersécurité, gestion des risques et mécanismes d'attaque**

- Politiques de cybersécurité
- Gestion des risques en cybersécurité
- Mécanismes d'attaque

## **JOUR 3 : Mesures de cybersécurité, coordination et partage de l'information**

- Mesures de cybersécurité
- Coordination et partage de l'information
- Programme de formation et de sensibilisation

## **JOUR 4 : Gestion des incidents, surveillance et amélioration continue**

- Continuité des activités
- Gestion des incidents de cybersécurité
- Tests dans la cybersécurité
- Mesure de la performance
- Réaction et récupération suite aux incidents de cybersécurité
- Amélioration continue
- Schéma de certification Lead Manager
- Clôture de la formation

## **JOUR 5 : Examen de certification**

- L'examen "PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager " répond aux exigences du programme d'examen et de certification PECB (Examination and Certification Program (ECP))
- Il couvre les domaines de compétence suivants :  
Domaine 1 : Concepts fondamentaux ayant trait à la cybersécurité - Domaine 2 : Rôles et responsabilités des parties prenantes - Domaine 3 : Gestion des risques en cybersécurité - Domaine 4 : Mécanismes d'attaque et mesures de cybersécurité - Domaine 5 : Partage de l'information et coordination - Domaine 6 : Intégration d'un programme de cybersécurité
- L'examen est disponible en Français et dure 3 heures