PECB BEYOND RECOGNITION

PECB CERTIFIED ISO/IEC 27032
Lead Cybersecurity Manager

Maîtriser la mise en œuvre et le management d'un programme de cybersécurité basé sur la norme ISO/IEC 27032

Pourquoi devriez-vous y participer ?

La formation ISO/IEC 27032 Lead Cybersecurity Manager vous permettra de développer les connaissances et les compétences nécessaires pour accompagner une organisation dans la mise en œuvre et la gestion d'un programme de cybersécurité en conformité avec la norme ISO/IEC 27032 et le Cadre de Cybersécurité NIST. Cette formation est conçue de manière à vous doter de connaissances approfondies en matière de cybersécurité, et vous permettra de maîtriser la relation entre la cybersécurité et d'autres types de sécurité des technologies de l'information, ainsi que le rôle des parties prenantes dans la cybersécurité.

Après avoir maîtrisé l'ensemble des concepts relatifs à la cybersécurité, vous pouvez vous présenter à l'examen et postuler au titre de « PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager ». En étant titulaire d'une certification de PECB, vous démontrerez que vous disposez des connaissances pratiques et des compétences professionnelles pour soutenir et diriger une équipe dans la gestion de la cybersécurité.

À qui s'adresse la formation ?

- Professionnels de la cybersécurité
- Experts en sécurité de l'information
- Professionnels souhaitant gérer un programme de cybersécurité
- Responsables du développement d'un programme de cybersécurité
- Spécialistes des TI
- Conseillers spécialisés dans les TI
- Professionnels des TI souhaitant accroître leurs connaissances et compétences techniques

Programme de la formation

Durée : 5 jours

Jour 1 | Introduction à la cybersécurité et aux notions connexes, selon la recommandation de la norme ISO/IEC 27032

- Objectifs et structure du cours
- Normes et cadres réglementaires
- Notions fondamentales de la cybersécurité
- Programme de cybersécurité
- Lancer un programme de cybersécurité
- Analyser l'organisme
- Leadership

Jour 2 | Politiques de cybersécurité, management du risque et mécanismes d'attaque

- Politiques de cybersécurité
- Gestion du risque de la cybersécurité
- Mécanismes d'attaque

Jour 3 | Mesures de contrôle de cybersécurité, partage et coordination de l'information

- Mesures de contrôle de cybersécurité
- Partage et coordination de l'information
- Programme de formation et de sensibilisation

Jour 4 | Gestion des incidents, suivi et amélioration continue

- Continuité des activités
- Management des incidents de cybersécurité
- Intervention et récupération en cas d'incident de cybersécurité
- Conclusion de la formation
- Tests en cybersécurité
- Mesure de la performance
- Amélioration continue

Jour 5 | Examen de certification

Objectifs d'apprentissage

- Acquérir des connaissances approfondies sur les composantes et les opérations d'un programme de cybersécurité en conformité avec l'ISO/IEC 27032 et le cadre de cybersécurité NIST
- Comprendre la corrélation entre ISO 27032, le cadre de cybersécurité NIST et les autres normes et cadres réglementaires
- Maîtriser les concepts, approches, normes, méthodes et techniques pour établir, mettre en œuvre et gérer efficacement un programme de cybersécurité au sein d'un organisme
- Apprendre à interpréter les exigences d'ISO/IEC 27032 dans le contexte spécifique d'un organisme
- Maîtriser l'expertise nécessaire pour planifier, mettre en œuvre, gérer, contrôler et maintenir un programme de cybersécurité tel que spécifié dans ISO/IEC 27032 et le cadre de cybersécurité NIST
- Acquérir les compétences pour conseiller un organisme sur les bonnes pratiques de management de la cybersécurité

Examen

Durée : 3 heures

L'examen « PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager » remplit les exigences relatives au programme d'examen et de certification de PECB. L'examen couvre les domaines de compétences suivants :

Domaine 1 | Principes et concepts fondamentaux de la cybersécurité

Domaine 2 | Rôles et responsabilités des parties prenantes

Domaine 3 | Gestion des risques liés à la cybersécurité

Domaine 4 | Mécanismes d'attaque et contrôles en cybersécurité

Domaine 5 | Partage de l'information et coordination

Domaine 6 | Intégrer le programme de cybersécurité dans le management de la continuité des activités

Domaine 7 | Gestion des incidents de cybersécurité et mesure de la performance.

Pour de plus amples informations concernant l'examen, veuillez consulter Politiques et règlement relatifs à l'examen

Certification

Après avoir réussi l'examen, vous pouvez demander l'une des qualifications mentionnées sur le tableau ci-dessous. Un certificat vous sera délivré si vous remplissez toutes les exigences relatives à la qualification sélectionnée.

Pour de plus amples informations concernant les certifications ISO/IEC 27032 et le processus de certification PECB, veuillez cliquer sur Politiques et règlement de certification.

Qualification	Examen	Expérience professionnelle	Expérience de projets en cybersécurité	Autres exigences
PECB Certified ISO/IEC 27032 Provisional Cybersecurity Manager	Examen PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager ou équivalent	Aucune	Aucune	Signer le Code de déontologie de PECB
PECB Certified ISO/IEC 27032 Cybersecurity Manager	Examen PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager ou équivalent	2 ans dont 1 an d'expérience en cyberséacurité	Activités de cybersécurité totalisant 200 heures	Signer le Code de déontologie de PECB
PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager	Examen PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager ou équivalent	5 ans dont 2 ans d'expérience en cybersécurité	Activités de cybersécurité totalisant 300 heures	Signer le Code de déontologie de PECB
PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager	Examen PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager ou équivalent	10 ans dont 7 ans d'expérience en cybersécurité	Activités de cybersécurité totalisant 1 000 heures	Signer le Code de déontologie de PECB

Note : *Les personnes certifiées par PECB qui possèdent les certifications Lead Cybersecurity Manager et Lead Incident Manager sont qualifiées pour la certification* ***Master Cybersecurity de PECB****, étant donné qu'elles ont passé 4 examens de base supplémentaires liés à ce programme. Pour des informations plus détaillées sur les examens de base et les exigences générales du Master, veuillez visiter le lien suivant : https://pecb.com/en/master-credentials*

Informations générales

- Les frais de certification sont inclus dans le prix de l'examen
- Un manuel de cours contenant plus de 400 pages d'informations et d'exemples pratiques est fourni
- À l'issue de la formation, un certificat de participation de 31 crédits DPC (Développement professionnel continu) est délivré
- En cas d'échec à l'examen, vous pouvez le repasser dans les 12 mois qui suivent sans frais supplémentaires