ISO/IEC 27032 Lead Cybersecurity Manager (PECB certified) - Including Exam

Durée: 4 Jours **Réf de cours: ISO27032LCM** **Méthodes d'apprentissage: Classe à distance**

Résumé:

Le cours ISO 27032 Lead CyberSecurity Manager permet d'acquérir l'expertise et la compétence nécessaires pour concevoir, déployer, gérer et piloter un programme de cybersécurité, qui s'appuie sur la norme ISO 27032 et le cadre de cyber sécurité du NIST. Pendant ce cours, les stagiaires renforcent leurs connaissances en cyber sécurité, ainsi que sur la relation entre la cybersécurité et les autres démarches de sécurité informatique, et le rôle du sponsor et des différentes parties prenantes dans la gestion d'un programme de cyber sécurité.
Après avoir maîtrisé tous les concepts nécessaires pour une gestion efficace et cohérente du programme de cyber sécurité, les stagiaires passent l'examen PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager, afin de démontrer qu'ils disposent des connaissances et des compétences professionnelles nécessaires pour gérer un plan de cybersécurité, ainsi que les équipes spécialisées.
La norme ISO/IEC 27032 est-elle complémentaire à l'ISO27001 ?
Oui, car le professionnel certifié ISO/IEC 27032 Lead Cybersecurity Manager est en mesure de protéger les données et la confidentialité d'une organisation contre les menaces cybernétiques, renforcer les compétences dans la mise en place et l'amélioration continue d'un programme de cybersécurité, et de réagir plus rapidement en cas d'incident.
La formation ISO27032 Cybersecurity Manager s'articule autour de sept domaines de compétences :
les concepts fondamentaux de la cybersécurité
les rôles et responsabilités des parties prenantes
la gestion des risques en cybersécurité
les mécanismes d'attaque, les contrôles de cybersécurité
la coordination et partage de l'information
l'intégration du programme de cybersécurité dans la gestion de la continuité du métier
la gestion des incidents de cybersécurité, la mesure de la performance.
Mise à jour : 23.05.20223

Classe à Distance - site Client

Cette formation peut être suivie à distance en synchrone depuis n'importe quel site pourvu d'une connexion internet (2 Mb/s en symétrique recommandés). Le programme (théorie et pratique) suit le même déroulé pédagogique qu'en présentiel. La solution technologique adoptée permet aux apprenants à distance de suivre les présentations faites au tableau, de voir et d'entendre l'instructeur et les participants en temps réel, mais également d'échanger avec eux.

Public visé:

Professionnels de la cyber sécurité Experts de la sécurité de l'information Consultants en sécurité Spécialistes informatiques visant un poste de RSO/IT Manager

Objectifs pédagogiques:

- A l'issue de la formation, les participants seront capables de :
- Gérer un programme de cyber sécurité, en conformité avec la norme ISO 27032 et le cadre de cyber sécurité du NIST
- Comprendre la complémentarité et la cohérence entre la norme ISO 27032, le cadre de sécurité du NIST et les autres standards de sécurité
- Maîtriser les concepts, les approches, les standards, les méthodes des techniques utilisées pour une conception, un déploiement et une gestion efficace d'un programme de cyber sécurité au sein d'une organisation
- Maîtriser l'interprétation de la norme ISO 27032 au sein du contexte spécifique de votre organisation
- Etre en mesure de planifier, déployer, gérer, contrôler et maintenir un programme de cyber sécurité conformément à la norme ISO 27032 et le cadres de cyber sécurité du NIST
- Accompagner une entreprise dans la mise en œuvre des meilleures pratiques de cyber sécurité

Pré-requis:

Une expérience dans le domaine de la sécurité de l'information est

Test et certification

Préparation au passage de l'examen PECB Certified ISO/IEC 27032

fortement recommandée.

Il est conseillé, mais pas obligatoire, d'avoir suivi une formation de base en sécurité informatique ou en cyber sécurité, de type ISO 27001 fondation ou ISO 27002 fondation. La certification ITIL est également la bienvenue (le processus de la gestion de la sécurité, du livre conception de services, s'appuie sur ISO 27001).

Lead Cybersecurity Manager. Celui-ci dure trois heures. Il se compose de 150 questions à choix multiple qui couvrent les sept domaines précités. Le score minimal pour la réussite de l'examen des de 70 %, soit 105 bonnes réponses sur 150 questions.

Un voucher sera remis à chaque participant en début de session* afin qu'il puisse planifier le passage de l'examen en ligne selon les créneaux disponibles à l'issue de la formation.

*Sous réserve que l'ensemble des participants de la session aient créé leur compte PECB.

Contenu:

Les concepts fondamentaux de la cyber sécurité

- comprendre et expliquer la structure de la norme ISO 27032 et le cadre de cyber sécurité du NIST
- identifier, analyser et évaluer les recommandations de la norme ISO 27032 et des autres cadres de cyber sécurité
- expliquer et illustrer les principaux concepts de cyber sécurité
- la différence entre la sécurité de l'information et la cyber sécurité
- les relations et les différences entre la norme ISO 27032 et les autres standards

Rôles et responsabilités des parties prenantes

- assignation des rôles et des responsabilités en cyber sécurité, la communication sur ces rôles et responsabilités
- les rôles des différentes parties prenantes et leur contribution pour renforcer la cyber sécurité
- les rôles et responsabilités des fournisseurs et des utilisateurs/clients comme les principales parties prenantes en cyber sécurité
- distinguer les rôles individuels des rôles organisationnels dans le cyberespace
- le rôle du leadership dans la définition des relais des responsabilités des différentes parties prenantes impliquées

La gestion des risques en cyber sécurité

- comprendre le rôle de la gestion des risques en cyber sécurité pour les opérations organisationnelles (dont la mission, les fonctions, l'image ou la réputation), les actifs organisationnels et les individus
- expliquer et illustrer la gestion des risques en cyber sécurité
- définition des buts et des objectifs de la gestion des risques en cyber sécurité
- comprendre et distinguer la gestion des risques globale et la gestion des risques en cyber sécurité
- comprendre et expliquer le cadre de gestion des risques selon la norme ISO 27005

Les mécanismes d'attaque et les contrôles de cyber sécurité

- comprendre l'importance de la mise en œuvre des contrôles de cyber sécurité et leur apport
- distinguer les quatre types de contrôles de cyber sécurité selon la norme ISO 27032
- déployer les contrôles clés de cyber sécurité selon la norme ISO 27032
- expliquer les principales menaces du cyberespace et leurs vecteurs de mitigation

Partage et coordination de l'information

- comprendre et expliquer l'importance et les bénéfices d'un cadre de partage et de coordination de l'information dans le cadre d'une démarche de cyber sécurité
- choisir et déployer la méthode et les processus nécessaires pour la mise en œuvre d'une démarche de partage et de coordination de l'information
- analyser les besoins et fournir des conseils dans l'attribution des rôles et des responsabilités lors de la mise en œuvre et la gestion d'un cadre de coordination et de partage de l'information
- définir et écrire les politiques et les procédures de partage et de coordination de l'information
- se préparer à la gestion opérationnelle du partage et de la coordination de l'information : établir des listes de contacts, mener des programmes de formation et de sensibilisation, etc.

Intégration du programme de cyber sécurité au sein du plan de continuité du métier

- comprendre ce qu'est la continuité du métier au regard de la cyber sécurité
- objectifs et bénéfices de la cohérence de la continuité du métier et du programme de cyber sécurité
- concevoir un plan de continuité en terme de cyber sécurité
- déterminer si le plan de continuité de cyber sécurité doit être intégrée au plan de continuité du métier (business continuity plan) ou au plan de recouvrement suite à un désastre (disaster recovery plan)
- comprendre les approches techniques applicables à l'amélioration du plan de continuité de cyber sécurité

La gestion des incidents cyber sécurité, la mesure de la performance

- définir et mettre en œuvre un processus de gestion des incidents selon les meilleures pratiques
- réduire les impacts potentiels des incidents de cyber sécurité sur les opérations de l'organisation expliquait et illustrer les objectifs de la gestion des incidents de cyber sécurité
- préparer planifier les opérations d'un schéma de gestion efficace et efficient des incidents de cyber sécurité
- collecte de preuves lors des incidents de sécurité selon une politique de type Forensics
- test du système technique pour garantir sa fiabilité
- détermination de la fréquence des objectifs de la mesure de la performance

Entrainement à l'examen de certification

Un voucher sera remis à chaque participant en début de session* afin qu'il puisse planifier le passage de l'examen en ligne selon les créneaux disponibles à l'issue de la formation.

Méthodes pédagogiques :

Cette formation s'équilibre entre un apport théorique et l'application des meilleures pratiques lors de la planification et la mise en œuvre d'un programme de cyber sécurité : de nombreux exemples et retours d'expérience illustrent ce cours des exercices pratiques s'appuient sur des études de cas réels les stagiaires passent un examen blanc afin de se préparer à la certification
Les documents sont accessibles au format électronique via le lecteur Kate (https://pecb.com/kate/) et mis à disposition lors de l'examen.
Notez que la création préalable d'un compte personnel sur le site de PECB est nécessaire non seulement pour suivre la formation, mais également pour créer son profil d'examen en ligne et programmer une session.

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement