Formation ISO 27032 - Lead Cybersecurity Manager

Devenir le garant de la Cyber sécurité dans l'entreprise

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

La norme ISO/IEC27032 définit un cadre stratégique de classification des échanges d'informations dans le Cyberespace. Cette classification permet d'optimiser l'orchestration du management des différentes actions et outils de sécurisation. Pour préparer et mettre en place un programme de cyber sécurité efficace qui intègrera les relations avec d'autres types de sécurité informatique (SI de l'entreprise...), il peut être bénéfique d'intégrer les recommandations de cette norme. Tout en préparant la certification ISO/IEC 27032, les participants à cette formation s'approprieront les lignes directrices de cette norme pour être en mesure d'élaborer des plans stratégiques de management de la cybersécurité, les mettre en application dans l'entreprise, garantir leur opérabilité avec la sécurisation du système d'informations interne, et assurer leur évolution.

Référence	MGR827
Durée	5 jours (35h)
Tarif	3 840 €HT
Certification	prix inclus

Objectifs

| Acquérir l'expertise et les compétences nécessaires pour soutenir un organisme dans la mise en oeuvre et le management d'un programme de cybersécurité basé sur la norme ISO/IEC 27032 et le cadre de cybersécurité du NIST
| Acquérir des connaissances approfondies sur la cybersécurité, la relation entre la cybersécurité et d'autres types de sécurité informatique, et du rôle des parties prenantes dans la cybersécurité
| Se préparer à l'examen qui permet d'obtenir la certification "PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager"

Public

| Professionnels de la cybersécurité
| Experts en sécurité de l'information
| Professionnels cherchant à gérer un programme de cybersécurité
| Personnes responsables de concevoir un programme de cybersécurité
| Spécialistes de la TI
| Conseillers-experts en tech

Prérequis

| Une première expérience dans le domaine de la sécurité de l'information est fortement recommandée
| Il est recommandé d'avoir suivi les formations ISO 27001/ISO 27002 - Les fondamentaux et ITIL® 4 Foundation Certifiant

Programme de la formation

Introduction à la cybersécurité et aux notions connexes, selon la recommandation de la norme ISO/IEC 27032
| Normes et cadres réglementaires
| Notions fondamentales de la cybersécurité
| Programme de cybersécurité
| Lancer un programme de cybersécurité
| Analyser l'organisme
| Leadership

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)
du 13 au 17 mai 2024

PARIS
du 22 au 26 avril 2024

AIX-EN-PROVENCE
du 13 au 17 mai 2024

BORDEAUX
du 13 au 17 mai 2024

LILLE
du 13 au 17 mai 2024

LYON
du 13 au 17 mai 2024

NANTES
du 13 au 17 mai 2024

SOPHIA-ANTIPOLIS
du 13 au 17 mai 2024

STRASBOURG
du 13 au 17 mai 2024

TOULOUSE
du 13 au 17 mai 2024

VOIR TOUTES LES DATES

Politiques de cybersécurité, management du risque et mécanismes d'attaque
| Politiques de cybersécurité
| Gestion du risque de la cybersécurité
| Mécanismes d'attaque

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

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

Passage de l'examen de certification PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager (en ligne après la formation)
| Révision des concepts en vue de la certification et examen blanc

Certification

Cette formation prépare au passage de la certification suivante.
N'hésitez pas à nous contacter pour toute information complémentaire.

PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager
Un voucher permettant le passage du test de certification est adressé à l'issue de la formation y préparant.
Chaque participant doit créer son profil sur l'espace PECB puis, une fois le profil validé, choisir un créneau pour passer l'examen et télécharger l'application PECB Exams. Il est nécessaire de signer le code de déontologie du PECB afin d'obtenir la certification

| Durée : 3h00
| Langue : anglais
| Un score minimum : 70%

Les candidats sont autorisés à utiliser non seulement les supports de cours mais aussi la norme ISO/IEC 27032 qui leurs sera remise. En cas d'échec les candidats bénéficient d'une seconde chance pour passer l'examen dans les 12 mois suivant la première tentative.
L'examen couvre les domaines de compétences suivants :

| Domaine 1 : Principes fondamentaux et notions de la cybersécurité
| Domaine 2: Rôles et responsabilités des parties prenantes
| Domaine 3 : Management du risque en cybersécurité
| Domaine 4 : Mécanismes d'attaque et mesures de contrôle de cybersécurité
| Domaine 5 : Partage et coordination de l'information
| Domaine 6 : Intégration du programme de cybersécurité dans le management de la continuité des activités
| Domaine 7 : Management des incidents de cybersécurité et mesure de la performance

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

HUB Formation - 1-7, Cours Valmy - 92923 Paris - La Defense
01 85 77 07 07 - www.hubformation.com - SIREN 525 287 785

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.