Lead CyberSecurity Manager ISO/IEC 27032

Formation Management / Management de Projet / Gouvernance IT

Que permet cette formation ? Acquérir l'expertise et la compétence nécessaires pour concevoir, déployer, gérer et piloter un programme de cyber sécurité, 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 cyber sécurité 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 cyber sécurité, ainsi que les équipes spécialisées.
Le cours s'articule autour de sept domaines de compétences :
les concepts fondamentaux de la cyber sécurité, les rôles et responsabilités des parties prenantes, la gestion des risques en cyber sécurité, les mécanismes d'attaque, les contrôles de cyber sécurité, la coordination et partage de l'information, l'intégration du programme de cyber sécurité dans la gestion de la continuité du métier, la gestion des incidents de cyber sécurité, la mesure de la performance.

OBJECTIFS

- 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

PUBLIC

Professionnels de la cyber sécurité
Experts de la sécurité de l'information
Consultants en sécurité
Spécialistes informatiques

PRE-REQUIS

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

PROGRAMME

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
Déterminer la différence entre la sécurité de l'information et la cyber sécurité
Repérer les relations et les différences entre la norme ISO 27032 et les autres standards

Rôles et responsabilités des parties prenantes

Assigner les rôles et les responsabilités en cyber sécurité, la communication sur ces rôles et responsabilités
Repérer les rôles des différentes parties prenantes et leur contribution pour renforcer la cyber sécurité
Identifier 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
Saisir le rôle du leadership dans la définition des relais des responsabilités des différentes parties prenantes impliquées

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
Définir les buts et les 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

Compréhension et explication du cadre de gestion des risques selon la norme ISO 27005
Les mécanismes d'attaque et les contrôles de cyber sécurité

A retenir

Durée : **5 jours** soit 35h.
Réf. **IS27032CM**

01 42 93 52 72

Dates des sessions

Paris
13/11/2023

Cette formation est également proposée en formule INTRA-ENTREPRISE.

Inclus dans cette formation

Coaching Après-COURS

Pendant 30 jours, votre formateur sera disponible pour vous aider. CERTyou s'engage dans la réalisation de vos objectifs.

100% SATISFACTION GARANTIE

Votre garantie 100% SATISFACTION

Notre engagement 100% satisfaction vous garantit la plus grande qualité de formation.

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

Explication des 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

Préparation 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
Définir les 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 intégré 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

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
Collecter des preuves lors des incidents de sécurité selon une politique de type Forensics
Tester le système technique pour garantir sa fiabilité
Déterminer la fréquence des objectifs de la mesure de la performance

Horaires, Planning et Déroulement de cette formation

Horaires

- Formation de 9h00 (9h30 le premier jour) à 17h30.
- Deux pauses de 15 minutes le matin et l'après-midi.
- 1 heure de pause déjeuner

DEROULEMENT

- Les horaires de fin de journée sont adaptés en fonction des horaires des trains ou des avions des différents participants.
- Une attestation de suivi de formation vous sera remise en fin de formation.
- Cette formation est organisée pour un maximum de 14 participants.

PROCHAINES FORMATIONS

Réussir la Certification Gestion de Projet PMP du PMI
Réussir la Certification PRINCE2 Foundation
Réussir les Certifications PRINCE2 Foundation et PRINCE2 Practitioner
Réussir la Certification ITIL Foundation
Réussir la Certification Agile certifié SCRUM Master
Réussir les Certifications TOGAF Certified et TOGAF Foundation

CERTyou est certifié Qualiopi

CERTyou a été reconnu par le BUREAU VERITAS pour la qualité de ces procédures et lui a décerné la certification Qualiopi Formation Professionnelle. La certification de services Qualiopi Formation Professionnelle répond aux exigences qualité décrites dans l'article 1 du décret n°2015-790 du 30 juin 2015.

Lead CyberSecurity Manager ISO/IEC 27032

Formation Management / Management de Projet / Gouvernance IT

Qualiopi processus certifié

RÉPUBLIQUE FRANÇAISE

La certification qualité a été délivrée au titre de la catégorie d'actions suivantes : **ACTIONS DE FORMATION**

Retrouvez cette formation sur notre site :
Lead CyberSecurity Manager ISO/IEC 27032