Développez vos talents
Certifiez vos compétences

Gouvernance et Juridique

ISO 27005 - Risk Manager - Avec certification

3 jours (21h00) | ★★★★½ 4,6/5 | ISO-27RM | Code Certif Info : 104035 | Certification PECB 27005 Risk Manager (incluse) | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel [1]

Formations Informatique › Cybersécurité › Gouvernance et Juridique

À l'issue de ce stage vous serez capable de :

- Comprendre la relation entre la gestion des risques de la sécurité de l'information et les mesures de sécurité
- Comprendre les concepts, approches, méthodes et techniques permettant un processus de gestion des risques efficace conforme à la norme ISO/CEI 27005
- Interpréter les exigences de la norme ISO/CEI 27001 dans le cadre du management du risque de la sécurité de l'information
- Conseiller efficacement les organisations sur les meilleures pratiques en matière de gestion des risques liés à la sécurité de l'information.

Niveau requis

Avoir des connaissances fondamentales de la norme ISO/IEC 27005 et des connaissances approfondies sur l'appréciation du risque et la sécurité de l'information.

Public concerné

Professionnels / consultants IT, responsables de la sécurité d'information, membres d'équipe de sécurité de l'information, agents de la sécurité de l'information, agents de la protection des données personnelles, tout individu responsable de la sécurité d'information, de la conformité et du risque dans une organisation, ou toute personne mettant en oeuvre ISO/CEI 27001 et souhaitant se conformer à la norme ISO/CEI 27001 ou impliqué dans un programme de gestion des risques.

(1) Modalité et moyens pédagogique :

Formation délivrée en présentiel ou distanciel * (e-learning, classe virtuelle, présentiel à distance). Le formateur alterne entre méthodes ** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification.

Les moyens pédagogiques mis en oeuvre (variables suivant les formations) sont : ordinateurs Mac ou PC (sauf pour les cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel). Environnements de formation installés sur les postes de travail ou en ligne. Supports de cours et exercices.

* Nous consulter pour la faisabilité en distanciel. ** Ratio variable selon le cours suivi.

Cette formation :

- Est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par M2i Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

Programme

Jour 1

Introduction au programme de gestion des risques conforme à la norme ISO/CEI 27005

- Objectifs et structure de la formation
- Concepts et définitions du risque
- Cadres normatifs et règlementaires
- Mise en oeuvre d'un programme de gestion des risques
- Compréhension de l'organisation et de son contexte

Jour 2

Mise en oeuvre d'un processus de gestion des risques conforme à la norme ISO/CEI 27005

- Identification des risques
- Analyse et évaluation des risques
- Appréciation du risque avec une méthode quantitative
- Traitement des risques
- Acceptation des risques et gestion des risques résiduels
- Communication et concertation relatives aux risques en sécurité de l'information
- Surveillance et revue du risque

Jour 3

Aperçu des autres méthodes d'appréciation des risques liés à la sécurité de l'information et examen de certification

- Méthode OCTAVE
- Méthode MEHARI
- Méthode EBIOS
- Méthodologie harmonisée d'EMR

Exemples de travaux pratiques (à titre indicatif)

- *Réalisation d'une appréciation de risque complète*
- *Travail de groupe*
- *Simulation d'entretien avec un responsable de processus métier*
- *Mise à disposition d'un ordinateur pour mener l'étude*
- *Présentation orale des résultats par chaque groupe*
- *Revue des résultats présentés*

Recommandations et préparation à l'examen

- Les erreurs courantes : les connaître et s'en prémunir
- Outillage
- Recommandations générales

Passage de la certification

- Le prix et le passage de l'examen sont inclus dans la formation
- L'examen (en français) a lieu le dernier jour, à l'issue de la formation et s'effectue en ligne ou sur papier, pour une durée moyenne de 2h00
- Examen composé de questions ouvertes pour un total de 50 points
- Un score minimum de 70% est requis pour réussir l'examen
- Déroulement à "livre ouvert" (autorisé avec support et notes personnelles prises durant la session)

Modalités d'évaluation des acquis

L'évaluation des acquis se fait :

- En cours de formation, par des études de cas ou des travaux pratiques
- Et, en fin de formation, par un questionnaire d'auto-évaluation ou une certification (M2i ou éditeur)

Les + de la formation

Ce cours est animé par un formateur certifié PECB.

Compétences visées

- Décrire les concepts et les processus fondamentaux de la gestion des risques en matière de sécurité de l'information à l'intention des responsables de l'entreprise, en vue de les impliquer dans la mise en oeuvre d'un cadre de prévention
- Elaborer un programme de gestion des risques liés à la sécurité de l'information conforme à la norme ISO 27005, afin d'optimiser la prévention des menaces d'intrusions dans les systèmes et de destruction des données
- Coordonner la mise en place des processus de sécurité de l'information en tenant compte du nécessaire accompagnement des acteurs, en vue d'assurer leur efficacité sur le long terme
- Evaluer et mesurer en continu la performance du programme de gestion des risques au moyen d'indicateurs pertinents, en vue d'optimiser celui-ci grâce à une exacte identification des points d'amélioration
- Conseiller une entreprise sur les meilleures pratiques en matière de sécurité de l'information, afin de renforcer l'efficacité du programme de gestion des risques.