Formation ISO 27005 Risk Manager

Code : RE06 **Durée** : 3 jours **Classe** : Présentiel / à distance

Public

- Chefs de projet
- Consultants
- Architectes techniques
- Toute personne en charge de la sécurité d'information, de la conformité et du risque
- dans une organisation
- Toute personne amenée à mettre en oeuvre ISO/CEI 27001 ou impliquée dans un
- programme de gestion des risques

Prérequis

- Connaitre le guide d'hygiène sécurité de l'ANSSI

Objectifs

- 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 de mettre en place un processus de gestion des risques efficace conforme à la norme ISO/CEI 27005
- Savoir interpréter les exigences de la norme ISO/CEI 27001 dans le cadre du management du risque de la sécurité de l'information
- Être en mesure de conseiller efficacement les organisations sur les meilleures pratiques en matière de gestion des risques liés à la sécurité de l'information

Programme détaillé

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

- Introduction
- Objectifs et structure de la formation
- Concepts du risque :
- Définition scientifique du risque
- Risque et statistiques
- Risque et opportunités
- Perception du risque
- Risque lié à la sécurité de l'information

2- Connaître le cadre normatif et réglementaire

- Normes et méthodologie
- ISO/IEC 31000 et ISO/IEC 31010
- Normes de la famille ISO/IEC 27000

3- Mettre en œuvre un programme de management du risque

- Mandat et engagement de la direction
- Responsable de la gestion du risque
- Responsabilités des parties prenantes
- Mesures de responsabilisation
- Politique de gestion du risque
- Processus de gestion du risque
- Approche et méthodologie d'appréciation du risque
- Planification des activités et allocation des ressources

4- Établir le contexte (mission, objectifs, valeurs, stratégies)

- Établissement du contexte externe
- Établissement du contexte interne
- Identification et analyse des parties prenantes
- Identification et analyse des exigences
- Détermination des objectifs
- Détermination des critères de base
- Définition du domaine d'application et des limites

Formation ISO 27005 Risk Manager

Code : RE06 **Durée** : 3 jours **Classe** : Présentiel / à distance

7- Apprécier les risques avec une méthode quantitative
- Notion de ROSI
- Calcul de la perte annuelle anticipée
- Calcul de la valeur d'une mesure de sécurité
- Politiques spécifiques
- Processus de management de la politique

8- Traiter les risques
- Processus de traitement des risques
- Options de traitement des risques
- Plan de traitement des risques

9- Apprécier et gérer les risques résiduels
- Acceptation des risques
- Approbation des risques résiduels
- Gestion des risques résiduels
- Communication sur la gestion des risques

10- Communiquer sur les risques
- Objectifs de communication
- Communication et perception des risques
- Plan de communication

11- Surveiller les risques
- Surveillance et revue des facteurs de risque
- Amélioration continue de la gestion des risques
- Mesurer le niveau de maturité de la gestion des risques
- Enregistrement des décisions et des plans de communication

12- Découvrir les méthodes d'appréciation des risques
- Méthode OCTAVE : méthodologies et roadmap Allegro
- Méthode MEHARI : analyse des enjeux, classification, évaluation des services, analyse des risques, plans de sécurité
- Méthode EBIOS : 5 modules, établissement du contexte, étude d'événements redoutés, scénarios des menaces, risques et mesures de sécurité

13- Passage de l'examen de certification PECB Certified ISO/CEI 27005 Risk Manager
- Révision des concepts et examen blanc
- Création du profil PECB
- Planification et passage de l'examen en ligne (durée : 2 heures)
- Score minimum requis : 70 %
- Signature du code de déontologie PECB
- Utilisation des supports de cours et de la norme ISO/CEI 27005
- Deuxième tentative possible dans les 12 mois

14- Domaines de compétences de l'examen
- Domaine 1 : Principes et concepts fondamentaux relatifs à la gestion des risques liés à la sécurité de l'information
- Domaine 2 : Mise en œuvre d'un programme de gestion des risques liés à la sécurité de l'information
- Domaine 3 : Processus et cadre de gestion des risques selon ISO/CEI 27005
- Domaine 4 : Autres méthodes d'appréciation des risques de la sécurité de l'information