Formation ISO 27005 : 2011 Risk Manager, préparation à la certification

analyse de risques

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

Ce séminaire, basé en partie sur la norme ISO/CEI 27005:2011, permet aux participants d'acquérir les bases théoriques et pratiques de la gestion des risques liés à la sécurité de l'information. Elle prépare efficacement les candidats à la certification ISO 27005 Risk Manager à partir d'études de cas.

Référence	AIR
Durée	3 jours (21h)
Tarif	2 590 €HT
Repas	repas inclus

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

du 18 au 20 juin 2024
du 1er au 3 octobre 2024
du 3 au 5 décembre 2024

PARIS

du 11 au 13 juin 2024
du 24 au 26 septembre 2024
du 26 au 28 novembre 2024

VOIR TOUTES LES DATES

Objectifs

| Identifier le concept de risque lié à la sécurité de l'information
| Utiliser ISO 27005 pour l'analyse de risque
| Connaître d'autres méthodes (EBIOS, MEHARI)
| Faire un choix rationnel de méthode d'analyse de risque

Public

| RSSI ou correspondants Sécurité
| architectes de sécurité
| directeurs ou responsables informatiques
| ingénieurs
| chefs de projets (MOE, MOA) devant intégrer des exigences de sécurité

Prérequis

| Connaissances de base dans le domaine de la sécurité informatique

Programme de la formation

Introduction
| Terminologie ISO 27000 et ISO Guide 73.
| Définitions de la Menace. Vulnérabilité. Risques.
| Principe général de la sécurité ISO 13335.
| La classification CAID.
| Rappel des contraintes réglementaires et normatives (SOX, COBIT, ISO 27001...).
| Le rôle du RSSI versus le Risk Manager.
| La future norme 31000, de l'intérêt de la norme "chapeau".

Le concept "risque"
| Identification et classification des risques.
| Risques opérationnels, physiques et logiques.
| Les conséquences du risque (financier, juridique, humain...).
| La gestion du risque (prévention, protection, évitement de risque, transfert).
| Assurabilité d'un risque, calcul financier du transfert à l'assurance.
| Les rôles complémentaires du RSSI et du Risk Manager/DAF.

L'analyse de risques selon l'ISO
| La méthode de la norme 27001:2013.
| L'intégration au processus PDCA.
| La création en phase Plan de la section 4.
| La norme 27005:2011 : Information Security Risk Management.
| La mise en oeuvre d'un processus PDCA de management des risques.

| Les étapes de l'analyse de risques.
| La préparation de la déclaration d'applicabilité (SoA).

Les méthodes d'analyse de risques
| Les méthodes françaises. EBIOS 2010.
| Etude du contexte, des scénarios de menaces, des événements redoutés, des risques, des mesures de sécurité.
| EBIOS dans une démarche ISO PDCA de type SMSI 27001.
| MEHARI 2010. L'approche proposée par le CLUSIF.
| Elaboration d'un plan d'actions basé sur les services de sécurité. Alignement MEHARI 27005 et référentiel ISO 27002.
| CRAMM, OCTAVE... Historique, développement, présence dans le monde. Comparaisons techniques.

Choix d'une méthode
| Comment choisir la meilleure méthode ?
| Les bases de connaissances (menaces, risques...).
| La convergence vers l'ISO, la nécessaire mise à jour.
| Etre ou ne pas être "ISO spirit" : les contraintes du modèle PDCA.

Conclusion
| Une méthode globale ou une méthode par projet.
| Le vrai coût d'une analyse de risques.

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.

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.