ISO 27005:2022 Risk Manager, préparation à la certification
analyse de risques

Séminaire de 3 jours - 21h
Réf : AIR - Prix 2024 : 2 890€ HT

Ce séminaire, basé en partie sur la norme ISO/CEI 27005:2022, 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.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Comprendre le concept de risque lié à la sécurité de l'information

Utiliser ISO 27005:2022 pour l'analyse de risque

Connaître d'autres méthodes (EBIOS RM, MEHARI)

Faire un choix rationnel de méthode d'analyse de risque

LE PROGRAMME

dernière mise à jour : 09/2023

1) Introduction

- Terminologie ISO 27000.
- Définitions de la Menace. Vulnérabilité. Risques.
- Les exigences Disponibilité Intégrité et Confidentialité : la prise en compte de la traçabilité/preuve.
- Rappel des contraintes réglementaires et normatives (RGPD, LPM/NIS, PCI DSS...).
- Le rôle du RSSI versus le Risk Manager.
- La norme 31000, de l'intérêt de la norme "chapeau" en référentiel universel.

2) 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.

3) Le management de risques selon l'ISO

- L'appréciation initiale en phase Plan de la section 6 : Planification.
- La norme 27005:2022 : Information Security Risk Management.
- La mise en œuvre d'un processus PDCA de management des risques.
- Le contexte, l'appréciation, le traitement, l'acceptation et la revue des risques.
- Les étapes de l'analyse de risques (identification, analyse et évaluation).
- La préparation de la déclaration d'applicabilité (SoA) et du plan d'actions.
- Le partage des risques avec des tiers (cloud, assurance, …); Le domaine 15 de ISO 27002.
- La méthode de la norme 27001 et son processus « Gestion des Risques ».

PARTICIPANTS

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.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

4) Les méthodes d'analyse de risques

- Approche par conformité vs approche par scénarios de risques.
- La prise en compte des menaces intentionnelles sophistiquées de type APT.
- Les objectifs de EBIOS RM (Identifier le socle de sécurité, Être en conformité, Identifier et analyser, etc).
- Les activités de la méthode.
- CRAMM, OCTAVE... Historique et reste du monde.
- Les méthodes MEHARI (2010, PRO et Manager).

5) Conclusion et choix d'une méthode

- La convergence vers l'ISO, la nécessaire mise à jour.
- Etre ou ne pas être "ISO spirit" : les contraintes du modèle PDCA.
- Une méthode globale ou une méthode par projet.
- Le vrai coût d'une analyse de risques.
- Comment choisir la meilleure méthode ?
- Les bases de connaissances (menaces, risques...).

LES DATES

CLASSE À DISTANCE	PARIS
2024 : 17 juin, 01 oct., 03 déc.	2024 : 11 juin, 24 sept., 26 nov.