ISO 27005:2022 Risk Manager, préparation et certification

Cours Pratique de 3 jours - 21h
Réf : RMG - Prix 2024 : 2 890CHF HT

À l'issue de la formation, l'apprenant sera capable d'apprécier et de gérer les risques liés à la sécurité de l'information, dans le but de définir et d'implémenter les politiques et procédures adaptées. Il sera aussi en mesure d'obtenir la certification "Risk Manager ISO 27005" liée à la gestion des risques dans le cadre d'un SMSI.

OBJECTIFS PÉDAGOGIQUES

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

Connaître les exigences de la norme ISO 27005 sur la gestion des risques sur la sécurité de l'information

Gérer une appréciation des risques dans le cadre d'un SMSI

Établir un processus de gestion des risques conforme à la norme ISO 27005

Préparer et passer la certification Risk Manager ISO 27005 dans de bonnes conditions de succès

CERTIFICATION

L'examen de certification est dirigé en partenariat avec l'organisme de certification LSTI (accrédité COFRAC). Il se déroule pendant la dernière demi-journée. Ce diplôme international officiel ISO vous apportera la plus grande crédibilité dans la conduite de vos projets d'analyse de risques.

PARTICIPANTS

Chefs de projet, consultants, architectes techniques, responsables de la sécurité des SI, toute personne en charge de la sécurité d'information, de la conformité et du risque dans une organisation.

PRÉREQUIS

Connaître un guide de bonnes pratiques (hygiène ANSSI, ISO 27002 ou équivalent), avoir suivi le parcours introductif à la cybersécurité ou posséder des connaissances équivalentes.

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.

LE PROGRAMME

dernière mise à jour : 02/2023

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 SI”

- Identification et classification des risques.
- Origine des menaces (accidentelle, délibérée, environnementale).
- Les conséquences du risque (financier, juridique, humain...).
- La gestion du risque (réduction / diminution, évitement de risque, partage).
- Le cas particulier du risque numérique en "persistance" (APT).
- Comment agir sur le risque (avant, pendant, après l'incident).

3) Le management de risques selon l'ISO

- La méthode de la norme 27001:2022 et son processus de gouvernance par le risque.
- L'appréciation initiale en phase plan de la section 6 - Planification.
- L'évolution majeure de 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'appréciation des risques (identification, analyse et évaluation).
- L'élaboration du plan de traitement sur la base des mesures de la norme ISO 27002.

- Le processus de sélection des mesures sur la base de attributs (Préventive, détective ou corrective).
- La choix des mesures de sécurité pour la déclaration d'applicabilité (SoA).

4) La norme ISO 27005:2022

- Introduction à la nouvelle norme ISO 27005:2022, l'influence de EBIOS RM.
- Le lien des processus de gestion des risques avec les processus du SMSI.
- L'analyse du risque cyber ciblé, comment analyser les APT.
- La cyber kill chain, les nouvelles sources de risques et leurs objectifs.
- Exemple d'échelle de calcul de vraisemblance/conséquences.
- L'approche de la gestion des risques par événement versus par actif.
- La description des scénarios stratégiques et opérationnels.
- La prise en compte du risque à travers l'écosystème.

5) Préparation et révision finale

- Mise en situation, tests de connaissance de type QCM, études de cas.
- Inventaire d'actifs, évaluation des menaces et vulnérabilités.
- Élaboration de plans de traitement des risques, etc.
- Examen blanc et corrigé interactif.
- Les astuces pour éviter les pièges.

6) Passage de l'examen

- Le déroulement de l'examen en ligne sera présenté la première journée de formation : contenu et règles à respecter.
- Les pré-requis techniques pour l'examen en ligne (webcam activée, connexion Internet).
- Le privilège administrateur pour installer le logiciel anti-triche, etc.
- Cet examen se déroule sur la plateforme d'examen en ligne TESTWE (testwe.eu).
- Si cet examen est passé dans les locaux d'Orsys, Orsys prend en charge la préparation du poste de travail du candidat.
- Le passage de l'examen chez Orsys s'accompagne du prêt au format papier des normes décrites durant la formation.
- Pour passer cet examen à distance, le candidat doit acquérir lui-même l'ensemble des normes au format papier.

LES DATES

CLASSE À DISTANCE
2024 : 29 mai, 31 mai, 09 sept., 20 nov.