

ISO 27001:2022, Lead Implementer, certification PECB

Cours Pratique de 5 jours - 35h
Réf : ISZ - Prix 2024 : 3 870CHF HT

Cette formation a pour objectif de revoir les connaissances nécessaires à la certification et de préparer au passage de l'examen. Elle se termine par l'examen proprement dit.

OBJECTIFS PÉDAGOGIQUES

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

- Mettre en œuvre et gérer efficacement un SMSI
- Apprécier les risques et élaborer une déclaration d'applicabilité
- Faire des propositions de plans d'actions
- Comprendre la corrélation entre la norme ISO/CEI 27001 et ISO/CEI 27002, ainsi qu'avec d'autres cadres réglementaires
- Interpréter les exigences de la norme ISO/CEI 27001 dans un contexte spécifique d'organisation

CERTIFICATION

Pour passer cet examen en mode distanciel, le candidat doit acquérir lui-même l'ensemble des normes nécessaires au format papier. L'examen final certifie que vous possédez les connaissances et les compétences nécessaires pour mettre en œuvre un SMSI suivant la norme ISO/IEC 27001:2022. Passage de l'examen de certification en français en fin de session. Il est dirigé en partenariat avec l'organisme de certification PECB.

LE PROGRAMME

dernière mise à jour : 05/2023

1) Norme ISO/CEI 27001 et initialisation d'un SMSI

- Cadres normatifs et réglementaires.
- Principes et concepts fondamentaux du système de management de la sécurité de l'information.
- Analyse du système de management existant.

2) Planification de la mise en œuvre d'un SMSI

- Périmètre du SMSI.
- Politiques de sécurité de l'information.
- Appréciation du risque.
- Déclaration d'applicabilité et décision de la direction pour la mise en œuvre du SMSI.
- Définition de la structure organisationnelle de la sécurité de l'information.

3) Mise en œuvre d'un SMSI

- Définition d'un processus de gestion de la documentation.
- Conception des mesures de sécurité et rédaction des procédures et des politiques spécifiques.
- Gestion des incidents.
- Plan de communication, de formation et de sensibilisation.
- Mise en œuvre des mesures de sécurité.
- Gestion des activités opérationnelles.

4) Surveillance, mesure et amélioration continue

- Surveillance, mesure, analyse et évaluation.
- Amélioration continue.

PARTICIPANTS

Risk managers, RSSI, responsables informatiques, tout acteur SI devant intégrer des contraintes de sécurité.

PRÉREQUIS

Connaissances de base en 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.

5) Préparation de l'audit de certification du SMSI

- L'audit interne, externe, tierce partie. Choisir son auditeur.
- L'audit organisationnel : démarche, méthodes.
- La revue de direction.
- La préparation de l'audit de certification.
- La compétence et évaluation des "implementers".

6) Préparation et certification

- Les normes nécessaires : ISO 27000, ISO 27001, ISO 27002, ISO 27005, ISO 19011, ISO 17021, ISO 27006.
- Pour passer cet examen en mode distanciel, le candidat doit acquérir lui-même l'ensemble de ces normes au format papier.
- Le passage de l'examen chez Orsys s'accompagne du prêt au format papier des normes décrites durant la formation.
- Si cet examen est passé dans les locaux d'Orsys, Orsys prend en charge la préparation du poste de travail du candidat.
- L'examen comporte un questionnaire à choix multiples relatif à la norme ISO/IEC 27001.
- L'examen comporte également des exercices pratiques et une étude de cas.
- Un certificat de participation de 31 crédits DPC (développement professionnel continu) est délivré.

Examen : Examen blanc et correction collective. Passage de l'examen.

LES DATES

CLASSE À DISTANCE

2024 : 08 juil., 21 oct.