Implémenter et gérer un projet ISO 27001:2022 préparation aux certifications LSTI

Séminaire de 3 jours - 21h
Réf : ASE - Prix 2024 : 2 890CHF HT

La norme internationale de maîtrise du risque ISO/CEI 27001 lié à la sécurité de l'information décrit les bonnes pratiques à mettre en place pour qu'une organisation puisse maîtriser efficacement les risques liés à l'information. Ce cours présente les normes ISO de la sécurité du Système d'Information puis les éléments pour mettre en place un système de management (SMSI) du risque de la sécurité de l'information.

OBJECTIFS PÉDAGOGIQUES

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

Expliquer les composants d'un système de management de la sécurité de l'information (SMSI) conforme à ISO 27001

Expliquer le contenu et la corrélation entre ISO 27001 et 27002 ainsi qu'avec d'autres normes et cadres réglementaires

Adapter les exigences de la norme ISO 27001 au contexte spécifique d'un organisme

Interpréter les exigences d'ISO 27001 dans le cadre de l'audit d'un SMSI

Aligner les différentes approches de la gouvernance SSI (ISO, LPM, NIS, …)

CERTIFICAT

Préparation aux certificats ISO 27001 Implementer et Lead Auditor.

CERTIFICATION

En mode distanciel, le candidat doit acquérir lui-même l'ensemble des normes nécessaire (ISO 27000, ISO 27001, ISO 27002, ISO 27005, ISO 27006, ISO 19011, ISO 17021, ISO 27006). En mode présentiel, chez Orsys, les normes sont prêtées au format papier durant la formation.

PARTICIPANTS

RSSI, Risk Managers, directeurs ou responsables informatiques, MOE/ MOA, ingénieurs ou correspondants Sécurité, chefs de projets, auditeurs internes et externes, futurs "audités".

PRÉREQUIS

Connaissances de base 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.

LE PROGRAMME

dernière mise à jour : 01/2023

1) Introduction

- Rappels. Terminologie ISO 27000 et ISO Guide 73.
- La notion de risque (conséquence, vraisemblance).
- La classification minimale CID (Confidentialité, Intégrité, Disponibilité).
- La gestion du risque (réduction, maintien, refus, partage).
- Analyse de la sinistralité. Tendances. Enjeux.
- Les réglementations de sécurité (métiers, juridiques, …) exemple PCI-DSS, NIST, LPM/NIS.
- Pour qui ? Pourquoi ? Interaction avec l'ISO.
- L'alignement ISO avec Gouvernance / Protection / Défense / Résilience.

2) Les normes ISO 2700x

- Historique des normes de sécurité vues par l'ISO.
- Les normes fondatrices (ISO 27001, 27002).
- Les normes indispensables (ISO 27005, 27004, 27003, etc).
- La convergence avec les autres normes « Système de Management ».

3) La norme ISO 27001:2022

- La revue de direction et le traitement des causes pour l'amélioration continue.
- Définition d'un Système de management de Sécurité de l'Information (ISMS).

- Objectifs à atteindre par votre SMSI.
- L'approche "amélioration continue" comme principe fondateur, le modèle PDCA (roue de Deming).
- La norme ISO 27001 intégrée à une démarche globale de gouvernance par le risque.
- De la spécification du périmètre SMSI à la cartographie des actifs.
- Les recommandations de l'ISO 27005 pour le management des risques.
- De l'importance de l'appréciation des risques. Choix d'une méthode type ISO 27005:2022 / ISO 31000.
- Conseils pour l'élaboration du Plan de traitement des risques.
- L'apport des méthodes publiées (ex : EBIOS RM) à l'appréciation des risques cyber.
- L'adoption de mesures de sécurité techniques et organisationnelles efficientes.
- L'élaboration de la déclaration d'applicabilité sur base Annexe A.
- Les audits internes obligatoires du SMSI. Construction d'un programme d'audit.
- La mise en œuvre d'actions correctives (conséquence) et préventives.

4) Les bonnes pratiques, référentiel ISO 27002:2022

- La structuration du premier niveau : mesures organisationnelles, liées aux personnes, d'ordre physique, technologiques.
- Le traitement des risques (#Prévention, #Détection, #Correction).
- Les concepts de cybersécurité : #Identification, #Protection, #Détection, #Traitement, #Récupération.
- Les capacités opérationnelles : #Gouvernance, #Gestion_des_actifs, Protection_des_informations, #Sécurité_des_RH.
- #Sécurité_physique, #Sécurité_système_et_réseau, #Sécurité_des_applications, #Configuration_sécurisée.
- #Gestion_des_identités_et_des_accès.
- Les domaines de sécurité (#Gouvernance_et_écosystème, #Protection, #Défense, #Résilience)
- La norme ISO 27002:2022 : aperçu des 93 bonnes pratiques.
- Nouvelles pratiques ISO 27002:2022, les mesures supprimées de la norme ISO 27002:2017. Les modifications, agrégations.
- Exemples d'application du nouveau référentiel à son organisme : les mesures de sécurité clés indispensables.

5) La mise en œuvre de la sécurité dans un projet SMSI

- Des spécifications sécurité à la recette sécurité.
- Comment respecter la PSSI et les exigences de sécurité du client/MOA ?
- De l'analyse de risques à la construction de la déclaration d'applicabilité.
- Intégration de mesures de sécurité au sein des développements spécifiques.
- Les règles à respecter pour l'externalisation.
- Assurer un suivi du projet dans sa mise en œuvre puis sa mise en exploitation.
- Les rendez-vous "Sécurité" avant la recette.
- Intégrer le cycle PDCA dans le cycle de vie du projet.
- La recette du projet, comment la réaliser ? Quels types d'audit ?
- Préparer les indicateurs. Indicateurs d'efficacité et de conformité.
- Mettre en place un tableau de bord de gouvernance. Exemples.
- L'apport de la norme 27004 :2016 dans la construction des métriques.

6) Les audits de sécurité normes ISO 19011 et ISO 17021

- Processus continu et complet. Étapes, priorités.
- La construction du programme d'audits internes.
- Les catégories d'audits, organisationnels, techniques, etc.
- L'audit interne, externe, tierce partie.
- Le déroulement type ISO de l'audit, les étapes clés.
- Les objectifs d'audit, la qualité d'un audit.
- La démarche d'amélioration pour l'audit.
- Les qualités des auditeurs, leur évaluation.
- L'audit de la gouvernance du Système de Management : démarche, méthodes.

7) La certification ISO de la sécurité du SI : le certificat SMSI

- Intérêt de cette démarche, la recherche du "label".
- Les critères de choix du périmètre. Domaine d'application. Implication des parties intéressées.
- L'ISO : complément indispensable des cadres réglementaires et standards ?
- Les enjeux business et/ou réglementaires escomptés.
- Organismes certificateurs, choix en France et dans le monde.
- Démarche d'audit, étapes et charges de travail.
- Normes ISO 17021 et ISO 27006, obligations pour les certificateurs.
- Coûts de la certification, ROI.

LES DATES

CLASSE À DISTANCE
2024 : 10 juin, 23 sept., 25 nov.