ISO 27001:2022 Implementer, certification LSTI
Implémenter et gérer un projet ISO 27001:2022

Cycle de 5 jours - 35h
Réf : PIZ - Prix 2024 : 4 050€ HT

La norme internationale de maîtrise du risque ISO/CEI 27001 liée à la sécurité de l'information décrit, sous forme d'exigences, les bonnes pratiques à mettre en place pour qu'une organisation puisse maîtriser efficacement les risques liés à l'information. Ce séminaire vous présentera dans un premier temps l'ensemble des normes ISO traitant de la sécurité du système d'information puis vous apportera les éléments nécessaires pour mettre en place un système de management (SMSI) du risque de la sécurité de l'information.

Ce cycle est composé de :

- Implémenter et gérer un projet ISO 27001:2022 (Réf. ASE, 3 jours)
- ISO 27001:2022 Implementer, mise en pratique, certification LSTI (Réf. LED, 2 jours)

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

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

Préparer et passer l'examen "Implementer 27001:2022"

TRAVAUX PRATIQUES

Préparation aux certificats ISO 27001 Implementer et Lead Auditor.

CERTIFICATION

Pour passer cet examen en mode distanciel, le candidat doit acquérir lui-même l'ensemble des normes nécessaire au format papier. L'examen final certifie que vous possédez les connaissances et les compétences nécessaires pour mettre en oeuvre un SMSI suivant la norme ISO/IEC 27001:2022. Cet examen est dirigé en partenariat avec l'organisme de certification LSTI (premier organisme accrédité ISO 27K par le COFRAC).

LE PROGRAMME

dernière mise à jour : 12/2022

1) Introduction

- Rappels. Terminologie ISO 27000 et ISO Guide 73.
- Définitions : menace, vulnérabilité, protection.
- La notion de risque (conséquence, impact, 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 ?
- L'alignement ISO avec Gouvernance / Protection / Défense / Résilience.

2) Les normes ISO 2700x

- Historique des normes de sécurité vues par l'ISO.

FINANCEMENT

Ce cours fait partie des actions collectives Atlas.

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.

- Les standards BS 7799, leurs apports à l'ISO.
- Les normes actuelles (ISO 27001, 27002).
- Les normes complémentaires (ISO 27005, 27004, 27003...).
- La convergence avec les normes qualité 9001 et environnement 14001.
- L'apport des qualiticiens dans la sécurité.

3) La norme ISO 27001:2022

- 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 de la SSI.
- Détails des phases Plan-Do-Check-Act.
- De la spécification du périmètre SMSI au SoA (Statement of Applicability).
- Les recommandations de l'ISO 27001 pour le management des risques.
- De l'importance de l'appréciation des risques. Choix d'une méthode type ISO 27005:2018 / ISO 31000
- L'apport des méthodes publiées (exemple EBIOS) dans leur démarche d'appréciation.
- L'adoption de mesures de sécurité techniques et organisationnelles efficientes.
- Les audits internes obligatoires du SMSI. Construction d'un programme d'audit.
- L'amélioration SMSI. La mise en œuvre d'actions correctives et préventives.
- L'annexe A comme support référentiel - lien avec la norme 27002.

4) Les bonnes pratiques, référentiel ISO 27002:2022

- La structuration du premier niveau : mesures organisationnelles, liées aux personnes, d'ordre physique, technologiques.
- Les thèmes et attributs (#Prévention, #Détection, #Correction).
- Les concepts de cybersécurité (#Identification, #Protection, #Détection, #Traitement, #Récupération).
- Les capacités opérationnelles (#Gouvernance, #Gestion_des_actifs, Protection_des_informations...)
- Les domaines de sécurité ((#Gouvernance_et_écosystème, #Protection, #Défense, #Résilience).
- La norme ISO 27002:2022 : aperçu des 93 bonnes pratiques.
- Les nouvelles bonnes pratiques ISO 27002:2022, les mesures supprimées de la norme ISO 27001:2017. Les modifications
- 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) 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.

7) Préparation et passage de l'examen

- Les normes nécessaires : ISO 27000, ISO 27001, ISO 27002, ISO 27005, ISO 19011, ISO 17021, ISO 27006.
- 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).
- Cet examen se déroule sur la plate forme 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 en mode distanciel, le candidat doit acquérir lui-même l'ensemble de ces normes au format papier.

Examen : L'examen est composé d'un questionnaire à choix multiples/questions à trous. Il dure 2h30. Il est valorisé à 100 points. Si au moins 50% des réponses sont correctes l'examen est réussi.

LES DATES

Ce parcours est composé d'un ensemble de modules. Les dates indiquées ci-dessous correspondent aux premières sessions possibles du parcours.

CLASSE À DISTANCE	PARIS	LYON
2024 : 10 juin, 23 sept., 25 nov.	2024 : 03 juin, 16 sept., 18 nov.	2024 : 10 juin, 23 sept., 25 nov.