ISO 27001 Lead Implementer (examen inclus) Certification : ISO 27001

Programme *(Mis à jour le 06/04/2023)*

JOUR 1 : Introduction à la norme ISO/IEC 27001 : 2022 et initiation d'un SMSI

- Objectifs et structure de la formation
  - Introduction
  - Informations générales
  - Objectifs d'apprentissage
  - Avantages d'ISO/IEC 27001:2022
- Système de management de la sécurité de l'information (SMSI)
  - Définition de système de management
  - Normes relatives aux systèmes de management
  - Systèmes de management intégrés
  - Définition d'un SMSI
  - Approche processus
  - Vue d'ensemble – articles 4 à 10
  - Vue d'ensemble – Annexe A
- Concepts et principes fondamentaux de la sécurité de l'information
  - Information et actif
  - Sécurité de l'information
  - Confidentialité, intégrité et disponibilité
  - Vulnérabilité, menace et impact
  - Risque de sécurité de l'information
  - Classification des mesures de sécurité
- Initiation de la mise en œuvre du SMSI
  - Définition de l'approche de la mise en œuvre du SMSI
  - Approches de mise en œuvre proposées
  - Application des approches de mise en œuvre proposées
  - Choisir un cadre méthodologique pour gérer la mise en œuvre d'un SMSI
  - Approche et méthodologie
  - Alignement sur les bonnes pratiques
- Compréhension de l'organisation et de son contexte
  - Mission, objectifs, valeurs et stratégies de l'organisation
  - Objectifs du SMSI
  - Définition préliminaire du périmètre
  - Environnement interne et externe
  - Principaux processus et activités
  - Parties intéressées
  - Exigences métier
- Domaine d'application du SMSI
  - Limites du SMSI
  - Limites organisationnelles
  - Limites de la sécurité de l'information
  - Limites physiques
  - Énoncé du périmètre du SMSI

JOUR 2 : Planification de la mise en œuvre d'un SMS

- Leadership et approbation du projet
  - Étude de faisabilité
  - Exigences relatives aux ressources
  - Plan du projet SMSI
  - Équipe de projet SMSI
  - Approbation de la direction
- Structure organisationnelle
  - Structure organisationnelle

Référence

THIP3088

Durée

5 jours / 35 heures

Prix HT / stagiaire

3650€

Objectifs pédagogiques

- Expliquer les concepts et principes fondamentaux d'un système de management SMSI basé sur ISO/IEC 27001
- Initier et planifier la mise en œuvre d'un SMSI basé sur ISO/IEC 27001, en utilisant la méthodologie IMS2 de PECB et d'autres bonnes pratiques
- Interpréter les exigences d'ISO/IEC 27001 pour un SMSI du point de vue d'un responsable de la mise en œuvre
- Préparer un organisme à un audit de certification par une tierce partie
- Soutenir un organisme dans le fonctionnement, le maintien et l'amélioration continue d'un SMSI basé sur ISO/IEC 27001

Niveau requis

- La certification ISO 27001 Foundation ou des connaissances de base sur la norme ISO 27001 sont recommandées
- La formation est dispensée sur la version 2022 de la norme ISO/CEI 27001
- Il est conseillé aux participants de se munir d'un exemplaire de la norme pour suivre la formation et passer la certification dans des conditions optimales

Public concerné

- Responsables ou consultants impliqués dans le management de la sécurité de l'information
- Conseillers spécialisés désirant maîtriser la mise en œuvre d'un Système de management de la sécurité de l'information
- Toute personne responsable du maintien de la conformité aux exigences du SMSI
- Membres d'une équipe du SMSI

Formateur

Les formateurs intervenants pour Themanis sont qualifiés par notre Responsable Technique Olivier Astre pour les formations informatiques et bureautiques et par Didier Payen pour les formations management.

Conditions d'accès à la formation

Délai : 3 mois à 1 semaine avant le démarrage de la formation dans la limite des effectifs indiqués

Moyens pédagogiques et techniques

Salles de formation (les personnes en situation

- Coordinateur de la sécurité de l'information
- Rôles et responsabilités des parties intéressées
- Rôles et responsabilités des principaux comités

- Analyse du système existant
  - Détermination de l'état actuel
  - Réalisation de l'analyse des écarts
  - Établissement des objectifs de maturité
  - Publication d'un rapport d'analyse des écarts
- Politique de sécurité de l'information
  - Types de politiques
  - Modèles de politiques
  - Politique de sécurité de l'information
  - Politiques de sécurité spécifiques
  - Approbation de la politique de management
  - Publication et diffusion
  - Sessions de formation et de sensibilisation
  - Contrôle, évaluation et revue
- Gestion des risques
  - ISO 31000
  - ISO/IEC 27005
  - Établissement du contexte
  - Identification des risques
  - Analyse des risques
  - Évaluation des risques
  - Traitement des risques
  - Communication et consultation
  - Enregistrement et élaboration de rapports
  - Surveillance et revue
- Déclaration d'applicabilité
  - Rédaction de la Déclaration d'applicabilité
  - Approbation de la direction
  - Revue et sélection des mesures de sécurité de l'information applicables
  - Justification des mesures de sécurité sélectionnées
  - Justification des mesures de sécurité exclues

JOUR 3 : Mise en œuvre du SMSI

- Gestion des informations documentées
  - Valeur et types d'informations documentées
  - Liste maîtresse des informations documentées
  - Création de modèles
  - Processus de gestion de l'information documentée
  - Mise en œuvre d'un système de management de l'information documentée
  - Gestion des enregistrements
- Sélection et conception des mesures
  - Architecture de sécurité de l'organisation
  - Préparation de la mise en œuvre des mesures
  - Conception et description des mesures
- Mise en œuvre des mesures
  - Mise en œuvre des processus et des mesures de sécurité
  - Introduction des mesures de l'Annexe A
- Tendances et technologies
  - Mégadonnées (Big data)
  - Les trois V des mégadonnées
  - Intelligence artificielle
  - Apprentissage automatique (Machine learning)
  - Apprentissage automatique (Machine learning)
  - Externalisation des opérations
  - Impact des nouvelles technologies en sécurité de l'information
- Communication
  - Principes d'une stratégie de communication efficace
  - Processus de communication de sécurité de l'information
  - Définition des objectifs de communication
  - Identification des parties intéressées
  - Planification des activités de communication
  - Réalisation d'une activité de communication
  - Évaluation de la communication
- Compétence et sensibilisation
  - Compétences et développement du personnel
  - Différence entre formation, sensibilisation et communication
  - Détermination des besoins en compétences

- Planification des activités de développement des compétences
- Définition du type et de la structure du programme de développement des compétences
- Programmes de formation et de sensibilisation
- Organisation des formations
- Évaluation des résultats des formations

- Gestion des opérations de sécurité
  - Planification de la gestion du changement
  - Gestion des opérations
  - Gestion des ressources
  - ISO/IEC 27035-1 et ISO/IEC 27035-2
  - ISO/IEC 27032
  - Politique de gestion des incidents en sécurité de l'information
  - Processus et procédure de gestion des incidents
  - Équipe de réponse aux incidents
  - Mesures de sécurité pour la gestion des incidents
  - Processus forensiques
  - Enregistrement des incidents de sécurité de l'information
  - Mesure et revue du processus de gestion des incidents

JOUR 4 : Suivi, amélioration continue et préparation à l'audit de certification

- Suivi, mesure, analyse et évaluation
  - Détermination des objectifs de mesure
  - Définition de ce qui doit être surveillé et mesuré
  - Établissement des indicateurs de performance du SMSI
  - Rapport de résultats
- Audit interne
  - Qu'est-ce qu'un audit ?
  - Types d'audits
  - Création d'un programme d'audit interne
  - Désignation d'une personne responsable
  - Établissement de l'indépendance, de l'objectivité et de l'impartialité
  - Planification des activités d'audit
  - Réalisation des activités d'audit
  - Suivi des non-conformités
- Revue de direction
  - Préparation d'une revue de direction
  - Conduite d'une revue de direction
  - Résultats de la revue de direction
  - Activités de suivi de la revue de direction
- Traitement des non-conformités
  - Processus d'analyse des causes fondamentales
  - Outils d'analyse des causes fondamentales
  - Procédure d'actions correctives
  - Procédure d'actions préventives
- Amélioration continue
  - Processus de surveillance continue
  - Maintien et amélioration du SMSI
  - Mise à jour continue des informations documentées
  - Documentation des améliorations
- Préparation à l'audit de certification
  - Sélection de l'organisme de certification
  - Préparation à l'audit de certification
  - Étape 1 de l'audit
  - Étape 2 de l'audit
  - Suivi d'audit
  - Décision de certification
- Clôture de la formation
  - Schéma de certification de PECB
  - Processus de certification PECB
  - Autres services PECB
  - Autres formations et certifications PECB

JOUR 5 : Préparation et Passage de la certification

- L'examen couvre les domaines de compétences suivants :
  - Domaine 1 : Principes et concepts fondamentaux du Système de management de la sécurité de l'information
  - Domaine 2 : Système de management de la sécuritén de l'information

• Domaine 3 : Planification de la mise en œuvre d’un SMSI selon la norme ISO/CEI 27001:2022
• Domaine 4 : Mise en œuvre d’un SMSI conforme à la la norme ISO/CEI 27001:2022
• Domaine 5 : Évaluation de la performance surveillance et mesure d’un SMSI selon la norme ISO/CEI 27001;2022
• Domaine 6 : Amélioration continue d’un SMSI selon la norme ISO/CEI 27001;2022
• Domaine 7 : Préparation de l’audit de certification d’un SMSI

- CERTIFICATION PREPAREE
  L’examen PECB Certified ISO/CEI 27001 Lead Implementer remplit les exigences relatives au programme
  d’examen et de certification de PECB. Le taux de réussite de cette certification en 2022 est de 89%.