IMPLÉMENTER UN PROJET ISO 27001

INFORMATIONS

Référence : AF-IM701

Prix de la formation : 3000 € HT par personne

Durée : 4 jours

Pauses café et déjeuners offerts

Cours pratique en présentiel ou en classe à distance

ÉQUILIBRE THÉORIE / PRATIQUE : Formation orientée sur la pratique : 70% de pratique et 30% de théorie.

VÉRIFICATION DES CONNAISSANCES : QCM de 15 questions à réaliser en amont de la formation.

Délai d'accès : 1 mois de délai à compter de la réception de la demande de formation

AVIS GÉNÉRAL

★★★★★ 4.7/5

HANDICAP

Les locaux dans lesquels ont lieu les formations sont tous par @Fortilio et choisis des lieux tous possède les conditions d'accueil et d'accès de plain-pied et de gestion de handicap. La prestation invite s'adapter aux personnes en situation de handicap.

DESCRIPTION

La sécurité des systèmes d'information est une préoccupation majeure de toutes les Directions des Systèmes d'information, quel que soit le secteur d'activité de l'entreprise.

Cette formation vous permettra d'acquérir l'expertise nécessaire pour accompagner une organisation dans la mise en place, la mise en œuvre, la gestion et la mise à jour d'un SMSI conforme à la norme ISO/IEC 27001:2022. En outre, cette formation vous prépares à la certification ISO 27001 Lead Implementer.

OBJECTIFS

À l'issue de la formation, le participant sera en mesure de :

- Comprendre les tenants et les aboutissants de la mise en œuvre un système de management basé sur la norme ISO/IEC 27001.
- Savoir planifier, diriger et assurer le suivi d'un audit de système de management conformément à la norme ISO/IEC 19011.
- Comprendre le rôle et les attentes autour de la fonction d'auditeur.
- Savoir interpréter et auditer les exigences de la norme ISO/IEC 27001.
- Obtenir la note de passage requise à l'issue de l'évaluation de l'atelier.

PUBLIC CONCERNÉ

Ce stage pratique s'adresse à : DPO, RSSI, Correspondant sécurité, Technicien réseau et systèmes...

PRÉREQUIS

- **Connaissances des bases des réseaux**
- **Connaissances des bases systèmes Linux et Windows**
- **Connaissances des bases de la SSI**
- **Quelques connaissances en développement peuvent être un plus**

SOLUTION DE FINANCEMENT

Pour trouver la meilleure solution de financement adaptée à votre situation : contactez votre conseiller formation.
Il vous aidera à choisir parmi les solutions suivantes :

- Le plan de développement des compétences de votre entreprise : rapprochez-vous de votre service RH.
- Le dispositif FNE-Formation.
- L'OPCO (opérateurs de compétences) de votre entreprise.
- Pôle Emploi sous réserve de l'acceptation de votre dossier par votre conseiller Pôle Emploi.

HORAIRES

En présentiel, les cours ont lieu de 9h à 12h30 et de 14h à 17h30. Les participants sont accueillis à partir de 8h45. Les pauses et déjeuners sont offerts. En classe à distance, la formation démarre à partir de 9h. Pour les stages pratiques de 4 ou 5 jours, quelque soit la modalité, les sessions se terminent à 16h30 le dernier jour.

S'inscrire à la formation

Télécharger au format PDF

PROGRAMME DE LA FORMATION

1 - INTRODUCTION, PRINCIPES FONDAMENTAUX DE LA SÉCURITÉ DE L'INFORMATION

- Les bases de la cybersécurité
- Le rôle du Lead SMVP
- Les outils du Lead SMVP
- Les normes ISO
- Comment lire une norme ISO
- Définition du SMVP
- Structure des normes et le PDCA
- Les exigences de l'ISO 27701
- Le contenu des annexes A et B de l'ISO 27701
- Les livrables attendus

EXERCICE PRATIQUE EN GROUPE :

Les stagiaires devront reprendre la norme et en extirper les exigences en indiquant les livrables et les responsabilités associés pour chaque exigence.

2 - PRÉPARATION ET PLANIFICATION DU PROJET SMVP

- Le lancement du projet SMVP
- Compréhension de l'organisme
  - Rédaction du plan projet
  - Enjeux interne et externes
  - Présentation d'outils
  - Cartographie de l'existant
  - Cartographie des flux
  - Revue des processus
  - Analyse des écarts
  - Définition du domaine d'application
- Matrice des compétences
  - RSSI
  - DPO
  - Responsable du traitement des données personnelles
  - Sous-traitant du traitement des données personnelles
  - Répartition des rôles
- Leadership et management
  - Business Case
  - Présentation du projet à la Direction
  - Avantages juridique, économiques et internes du SMVP
  - Budgétisation
- Politique de sécurité de l'information et politique de protection des données
  - Introduction
  - Domaine d'application
  - Objectifs
  - Principes
  - Rôles et responsabilités
  - Principaux éléments attendus
  - Politiques connexes
  - Diffusion de la politique
- L'analyse de risque
  - La méthodologie d'appréciation du risque
  - L'identification des risques
  - L'appréciation du risque
  - L'évaluation du risque
  - Le traitement du risque
  - Le risque résiduel et acceptation du risque
  - Plan de traitement des risques
- L'analyse d'impact sur la protection des données
  - Compréhension du contexte
  - Mesures mis en œuvre pour le respect des 6 principes du RGPD
  - Mesures mis en œuvre pour le respect des droits des personnes concernées
  - L'appréciation des risques sur la vie privée
  - L'évaluation des risques sur la vie privée
  - Le traitement du risque sur la vie privée
  - Le suivi et la communication des risques
- Déclaration d'applicabilité

3 - MISE EN PLACE DU SMVP :

- La mise en place d'un processus de gestion documentaire
  - La création de modèle
  - Le contenu type d'un document
  - La classification
  - La gestion des enregistrements
  - Le cycle de vie documentaire
- Plan de formation et de sensibilisation
  - Définition de la compétence, de la formation et de la sensibilisation
  - Conception et planification de la sensibilisation
  - Support de sensibilisation
  - Programme de formation
  - La matrice de compétence
  - Résultats des campagnes de sensibilisation et de formation
- Plan de communication
  - Les principes de communication
  - Les objectifs de communication
  - L'identification des parties intéressés
  - Les supports de communication
  - Les activités de communications
- Gestion des incidents et des violations de données personnelles
  - La politique de gestion des incidents
  - Les processus de remontée des incidents
  - Les CERT
  - Les mesures de réponses à incidents
  - L'analyse forensique
  - Sauvegarde et stockage des incidents de sécurité
  - Revue et interprétation des incidents de sécurité
- Autres mesures à mettre en œuvre
  - La gestion des actifs
  - La gestion des identités et des accès
  - La gestion du chiffrement
  - La protection des réseaux
  - Les relations avec les fournisseurs
  - La sécurité du développement
  - La continuité d'activité
  - Le choix des indicateurs

4 - SURVEILLANCE, REVUE ET AMÉLIORATION CONTINUE DU SMVP :

- Le suivi et la mesure des performances
  - L'ISO 27004
  - Indicateur de performance
  - Indicateur d'efficacité
  - Interprétation du tableau de bord
- L'audit interne
  - Audit interne (1ère partie) *externe* (2nde et tierce partie)
  - Les objectifs de l'audit interne
  - Nomination d'un responsable d'audit
  - Déroulé d'un audit interne (pont avec la 19011)
  - Relevé de non-conformités (majeure et mineure)
  - Suivi des non-conformités
- Revue de direction
  - Périodicité de la revue de direction
  - Exemple d'ordre du jour
  - Plan d'action pour le traitement des non-conformités
  - Opportunités d'amélioration continue
  - Rapport de revue de direction
- Le traitement des non-conformités
- L'amélioration continue

AVIS CLIENTS

★★★★★ 4.7/5

Moyenne calculée sur l'ensemble des formations animées par @Fortilio pour divers clients sur l'année 2022