



Appréhender et mettre en place son Système de Management de la Sécurité de l'Information (SMSI) – 28 h

Programme détaillé page 2

Pré requis :

- Aucun prérequis n'est nécessaire pour suivre cette formation, toutefois une expérience professionnelle en sécurité informatique est un plus.

Objectifs :

- Apprendre à mettre en œuvre la norme ISO 27 001 et son annexe A
- Identifier les actions à mettre en œuvre pour répondre aux exigences
- Déterminer les modalités de maintien du système à niveau en continu

Durée :

- 28 h sur 4 jours (*Adaptation possible sur plusieurs jours et demi-journées*)

Modalités et délais d'accès :

- Intra entreprise ou inter entreprise – Session de 6 à 12 personnes
- En présentiel (*Sur le site du client ou dans un tiers lieu*) et / ou en distanciel.
- Mise en place de la session de formation dans un délai moyen de 3 mois sous réserve de l'effectif minimum d'une session.

Tarif :

- Inter : 400 € HT par participant - Intra : 4 000 € HT la session. Possibilité de prise en charge par votre OPCO*
* *Certificat QUALIOP1 disponible sur le site internet de ITSET CONSULTING [ici](#)*

Contact :

- Christophe TESTI – Gérant et formateur – testi@itset.fr – 06 66 64 59 56

Méthodes mobilisées :

- Présentations théoriques des concepts.
- Exercices de compréhension et d'analyse.
- Mises en situation
- Vérification / Adaptation / Production des livrables adaptés à votre organisme.

Modalités d'évaluation :

- Quizz à l'entrée et en sortie de la formation
- Evaluation en fin de chaque module
- Enquête de satisfaction

Accessibilité aux personnes en situation de handicap :

Cette formation est accessible aux personnes en situation de handicap, cependant pour toute situation de handicap, merci d'en informer le gérant à l'aide des coordonnées dès la prise de contact pour analyser la faisabilité de l'action par rapport aux contenus, locaux, etc.



Appréhender et mettre en place son Système de Management de la Sécurité de l'Information (SMSI) – 28 h

- Tour de table
- Quiz à l'entrée en formation

MODULE 1 – INTRODUCTION AUX SYSTEMES DE MANAGEMENT (2 h)

- Notions de SM & SMSI – Structure des normes HLS
- Le modèle PDCA (Plan Do Check Act)
- La certification : principes, enjeux et objectifs
- Quiz d'évaluation

MODULE 2 – PRESENTATION DETAILLEE DE LA NORME ISO 27001 (5 h)

Pour chaque indicateur, une vérification de la conformité de vos documents avec les exigences sera réalisée, des propositions de modifications et/ou de création seront réalisées le cas échéant.

- Contexte de l'organisation
- Leadership
- Planification
- Support
- Fonctionnement
- Evaluation des performances
- Amélioration
- Quiz d'évaluation

MODULE 3 – PRESENTATION DETAILLEE DE LA NORME ISO 27002 (7 h)

Pour chaque chapitre de la norme, une vérification de la conformité de quelques-uns de vos documents avec les exigences sera réalisée, des propositions de modifications et/ou de création seront réalisées le cas échéant.

- Contexte de l'organisation
- Leadership
- Planification
- Support
- Fonctionnement
- Evaluation des performances
- Amélioration
- Quiz d'évaluation

MODULE 4 – LES PROCESSUS DANS UN SMSI (3 h)

Pour chaque chapitre de la norme, une vérification de la conformité de quelques-uns de vos documents avec les exigences sera réalisée, des propositions de modifications et/ou de création seront réalisées le cas échéant.

- Processus support
- Gestion des exigences légales et Réglementaires
- Gestion des risques
- Implémentation et suivi des mesures de sécurité

- Gestion des incidents
- Gestion documentaire
- Evaluation de la performance
- Exemple d'outils : cartographie des processus – carte d'identité
- Quiz d'évaluation

MODULE 5 – LA GESTION DES RISQUES ET LA NORME ISO 27 005 (4 h)

- Vocabulaire : risque, menace, vulnérabilité, etc.
- Critères de gestion de risque
- Appréciation des risques, acceptation du risque, communication du risque
- Déclaration d'applicabilité (DdA/SoA)
- Réexamen du processus de gestion de risques et suivi des facteurs de risques
- Présentation des méthodes ebios et Mehari
- Quiz d'évaluation

MODULE 6 – LA GESTION DES EXIGENCES LEGALES ET REGLEMENTAIRES (1 h)

- Protéger les données à caractère personnel
- Outils de veille juridique
- Gestion des engagements contractuels
- Gestion des fournisseurs et prestataires
- Contractualiser la sécurité
- Quiz d'évaluation

MODULE 7 – L'ÉVALUATION DES PERFORMANCES (1 h)

- La surveillance au quotidien.
- Les indicateurs
- Le programme d'audit et les différents types d'audit
- La revue de direction
- Quiz d'évaluation

MODULE 8 : METTRE EN ŒUVRE L'AMÉLIORATION CONTINUE ET SE PRÉPARER AUX AUDITS (5h)

- Le PDCA
- Le traitement des non-conformités
- Les audits
- Exercice pratique : réalisation d'un audit interne sur une partie de votre système
- Rechercher un organisme certificateur
- Quiz d'évaluation
- Enquête de satisfaction