Formation Responsable Système de Management de la Sécurité de l'Information (ISO 27001)

Ref. ***CRSMSI-10***
Durée : 5.0 jour(s) / 35.0 heures

La digitalisation de notre société a engendré une forte dépendance sur le tout numérique et les differents cœurs de métiers. Cet écosytème nécessite la mise en place d'un management de la sécurité de l'information afin de garantir une cohérence sur la protection de l'information de chaque entreprise.
La norme ISO 27001-2022 permet la mise en place d'un tel système de management et garantir le respect d'exigences attendues.

Cette Formation permet de valider les savoirs pour toute personne en charge de participer à la mis en œuvre d'un SMSI. Elle valide un ensemble de savoirs requis pour les fiches métiers de l'ANSSI suivantes :
Auditeur de sécurité organisationelle, consultant en cybersécurité, RSSI, Formateur en cybersécurité, Chef sécurité de projet.

Pré-requis :

Connaissance du fonctionnement managérial et organisationnel d'une organisation et connaissance de base en sécurité de l'information

Personnes concernées :

DSI
RSSI
Risk manager
Chef de projet sécurité
Auditeur sécurité
Consultants sécurité

Objectifs :

Définir le processus de management d'un SMSI.
Reproduire les bonnes pratiques d'implémentation
Pratiquer la mise en œuvre d'un SMSI
Gérer la performance et l'efficacité d'un SMSI
Organiser, planifier, préparer la mise en œuvre d'un SMSI

Programme :

JOUR 1

Les principes fondamentaux de la sécurité de l'information et de la protection des données:

Les normes ISO
Vocabulaire
Le CID
Le risque
Définition du SMSI
Structure des normes et le PDCA
Les exigences de l'ISO 27001
Le contenu de l'annexe A de l'ISO 27001
Les livrables attendus

Exercice pratique en groupe : Etude de la norme

JOUR 2

Préparation et planification du projet SMSI :

Le lancement du projet SMSI
Compréhension de l'organisme.
Cartographies
Analyse des écarts.
Définition du domaine d'application.
Matrice des compétences

TD : Etude de cas

Leadership et management
Business Case.
Politique de sécurité de l'information
Domaine d'application
Rôles et responsabilités
Principaux éléments attendus.
Politiques connexes.
Comitologie
Communication
Ressources

TD : Etude de cas

JOUR 3

L'analyse de risque

Le processus de management du risque
Le risque résiduel et acceptation du risque
Plan de traitement des risques
Les méthodologies d'analyse de risque

TD: Exercices d'idetnification des risques pour les SI

Déclaration d'applicabilité

Présentation des exigences
justifications

TD : étude de cas : DDA

Mise en place du SMSI :

gestion documentaire
Plan de formation et de sensibilisation
Plan de communication
Gestion des incidents
Autres mesures à mettre en œuvre

TD: Exercices et etude de cas

JOUR 4

Suivi et amélioration Le suivi et la mesure des performances
L'audit interne
Revue de direction
Le traitement des non-conformités
L'amélioration continue

TD: Exercices et etude de cas

JOUR 5

Préparation certification : quizz et étude de cas
Examen : QCM sur les fondamentaux de la norme, vocabulaire et points clés. Mise en situation spécifique sur le processus d'implémentation du SMSI.
Etude de cas globale

Démarche pédagogique :

Formation orientée sur la pratique
70% de pratique et 30% de théorie
Cybersecurity Educator ECSF

Evaluation et validation :

EXAMEN : PASSAGE DE LA CERTIFICATION DE PERSONNES
Partie théorique et pratique
Le temps destiné au passage de la certification est de 3H.
L'examen est composé de 3 parties :

- QCM
- Mise en situation sur points spécifiques
- Mise en situation sur cas concrets

Chaque domaine de compétences est couvert par l'examen et sera stipulé lors des exercices.
Il peut se dérouler à distance.

Bureau Veritas Certification assure l'examen final de ce programme de formation.
L'accès au support de cours, aux travaux pratiques est assuré pendant trois semaines à compter du début de session.
Le passage de la certification doit être réalisé en ce laps de temps.
En cas d'échec au premier passage de la certification le candidat a la possibilité de réaliser un second passage dans les 15 j suivants le premier passage.

L'examen valide des domaines de compétences en relation avec les profils métiers identifiés par l'European union agency for cybersecurity via l'European Cybersecurity Skills Framework