Formation Responsable Système de Management de la vie privée (ISO 27701)

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

Depuis 2018 le RGPD est entré en vigueur afin de pouvoir mieux protéger les données personnelles. Cette règlementation change en profondeur les actions et responsabilités entre les responsables de traitement, les sous traitants et définis des principes et des droits pour chaque personne concrnée. Toute entreprise se doit de se mettre en conformité vis-à-vis du RGPD. Un des moyens d'y arriver est de mettre en place un Système de management de la vie privée. C'est la norme ISO 27701 qui porte les exigences d'un tel système.
Cette certification permet l'acquisition et validation des savoirs utilent pour la mise en œuvre d'un SMVP.

ECSF METIERS ASSOCIES :
CISO,
Cybersecurity risk manager
Cyber legal policy and compliance officer
Cybersecurity Auditor,

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.
Chef de projet sécurité.
Développeurs.
Consultants sécurité.
Auditeurs.

Objectifs :

Définir le processus de management d'un SMPD.
Reproduire les bonnes pratiques d'implémentation
Pratiquer la mise en œuvre d'un SMPD
Gérer la performance et l'efficacité d'un SMPD
Organiser, planifier, préparer la mise en œuvre d'un SMPD
Elaborer une étude d'impact sur la vie privée

Programme :

JOUR 1

Les principes fondamentaux de la sécurité de l'information et de la protection des données :
Les normes ISO.
Fondamentaux vie privée
Le risque
Définition du SMVP.
Les exigences de l'ISO 27701.
Le contenu de l'annexe A de l'ISO 27701.
Le contenu de l'annexe B de l'ISO 27701.
Les livrables attendus.

Exercice pratique en groupe : Etude de la norme et Quiz.

JOUR 2

Préparation et planification du projet SMSI :
Le lancement du projet SMVP
Compréhension de l'organisme
Catographies
Revue des processus
Définition du domaine d'application
Matrice des compétences

TD: définition du contexte de l'organisation

Leadership et management
Business Case.
Avantages juridique, économiques et internes du SMVP.
Politiques
Domaine d'application.
TD: Etude de cas.

JOUR 3

Analyse des risques sur la vie privée

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

TD: Etude de cas

Mise en place du SMVP:
La mise en place d'un processus de gestion documentaire
Plan de formation et de sensibilisation
Plan de communication
Gestion des incidents liés à des violations de données personnelles
Autres mesures à mettre en œuvre La gestion des actifs

TD: Etude de cas

JOUR 4

Le suivi et la mesure des performances
L'audit interne
Revue de direction
Lien avec le SMSI
Les annexes

JOUR 5

Préparation Examen : quizz et étude de cas sur la mise en œuvre d'un SMPD.
Examen final : QCM sur points de la norme, vocabulaire, exigences. Mise en situations spécifiques et étude de cas sur un SMPD

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.

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