Formation RiskManager (ISO 27005)

Ref. **CRM-06**
Durée : 3.0 jour(s) / 21.0 heures

Les menaces sur nos systèmes d'information sont réelles et omniprésentes. Il est essentiel voire vital de comprendre des risques qui pèsent sur notre environnement digital et de pouvoir alors adopter une position en adéquation avec les besoins et la vision de l'entreprise.
La norme ISO 27005-2022 permet d'aborder le processus de management des risques dans tous ses détails et en adéquation avec les normes internationnales en vigueurs.

Cette Formation permet de valider la maitrise des savoirs indispensables pour mener à bien une analyse des risques. 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 d'une organisation et connaissance de base en analyse de risque.

Personnes concernées :

DSI
RSSI
Risk manager
Chef de projet sécurité

ECSF METIERS ASSOCIE :
Cyber information Security officer, Cyber security risk manager, Cyber security auditor

Objectifs :

Décrire les concepts de bases liés à la gestion des risques.
Appliquer le guide
Evaluer le contexte d'une organisation souhaitant mettre en œuvre une analyse des risques dans un SMSI.
Evaluer les principaux concepts de gouvernance et ses principaux enjeux et implication en matière de sécurité de l'information.
Elaborer un cadre sur l'analyse des risques et son suivi associé

Programme :

JOUR 1

Introduction Management du Risque
Le risque manager : présentation de la mission
Les types de risques
Concepts et vocabulaire
Les outils du RM
Règlementation et risques
Exercices : échange sur étude de cas
Les normes ISO
Les normes : présentation de la structure d'une norme ISO
L'ISO 31000, L'ISO 29134
L'ISO 27005
Exercices : étude de la norme

JOUR 2

Le processus d'appréciation du risque
Appréhender le contexte
Comprendre les cartographies, et la stratégie
Trouver les actifs primordiaux et actifs supports critiques associés
Les composantes : menaces, actifs, vulnérabilités
Les échelles, conception, et compréhension
Evaluer le risque
Le traitement du risque
Les options de traitements
Exercices sur les options de traitement
Les mesures de sécurité
Les risques résiduels
Propriétaires des risques
Le Plan de Traitement des Risques et gestion de projet associée
Exercices : mise en place d'un PTR
Les indicateurs et tableau de bord
La communication
L'amélioration continue

TD : réalisation d'une analyse de risque en suivant le processus de l'ISO 27005-2022

JOUR 3

préparation à la certification : Quizz et étude de cas

Examen final : QCM sur les fondamentaux et vocabulaire de la norme. Mise en situation spécifiques sur des points clés du processus de management des risques, 2tudes de cas et élaboration d'un cadre de management des risques liées à la sécurité de l'information et de la vie privée

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