Formation « ISO 27005 Risk Manager »

Réf : ISO27RM

Une fois que les bonnes pratiques ont été appliquées, la sécurité des systèmes d'information a besoin d'être ajustée aux besoins et au contexte de chaque organisme. Partant de ce constat, les experts en sécurité ont placé la gestion des risques au cœur des processus de gestion de la cybersécurité. Aujourd'hui, systèmes de management, homologations, et RGPD sont basés par une approche sur le risque, de même que de nombreuses certifications (ISO27001, HDS, PCI-DSS, ISO22301, etc). La gestion des risques reste pourtant une démarche parfois d'abord difficile et qui conditionne souvent la réussite du système de management ou du projet associé.
La norme ISO27005 :2022 est la méthode de gestion des risques en sécurité de l'information reconnue internationalement, et un des principaux guides de la série des normes ISO27001. ISO 27005 :2022 est pragmatique, elle vise la gestion des risques dans la durée, et elle impose la prise de responsabilité par le propriétaire du risque, généralement la direction générale. Elle est la méthode préconisée pour toute appréciation des risques dans le cadre d'un SMSI (Système de Management de la Sécurité de l'Information). Elle peut être également utilisée pour l'appréciation des risques imposée en plus du BIA (Business Impact Analysis) dans un SMCA (Système de Management de la Continuité d'Activité) et dans beaucoup d'autres cadres.

Objectifs

- **Acquérir une compréhension globale des concepts, de la norme, des méthodes et des techniques de gestion des risques**
- **Apprendre à mettre en œuvre la méthode ISO 27005 :2022 dans son contexte**
- **Appliquer la méthode ISO27005 avec efficacité là où celle-ci accorde de la liberté à l'implémenteur**
- **Maîtriser le processus de gestion des risques et son cycle de vie**
- **Savoir apprécier les risques et présenter ses propositions de traitement aux propriétaires des risques**

Durée & horaires

- **3 jours soit 21 heures réparties en 2,5 jours de cours et 0,5 d'examen.**
- **Horaires : de 9h30 à 12h et de 13h30 à 17h30/18h00.**

Nombre de participant

- **Minimum 6 participants – Maximum 24 participants**

Public visé

- **Consultants**
- **RSSI**
- **Chefs d projet**
- **Toute personnes devant réaliser des appréciations des risques en cybersécurité**

Pré-requis

- **Pour assister à cette formation, il est recommandé de posséder des connaissances en informatique.**

Méthode pédagogique

La méthode pédagogique se base sur les cinq points suivants :

- **Approche du sujet de manière interactive où les stagiaires remplissent un tableur édité par l'instructeur et déroulent la méthode sans la connaître**
- **Cours magistral basé sur la norme ISO 27005 :2022**
- **Des exemples et études de cas tirés de cas réels**
- **Des exercices réalisés individuellement**

- **Mise en œuvre d'une appréciation des risques et d'un traitement des risques sur une étude de cas, en groupe, à l'aide d'un tableur**
- **Formation nécessitant 1 heure de travail personnel et ce quotidiennement durant la session.**

Supports

- **Support de cours au format papier en français**
- **Cahier d'exercices et corrections des exercices**
- **Tous les documents nécessaires à la formation en français ou anglais**
- **Certificat attestant de la participation à la formation**
- **Clef USB permettant de conserver le travail réalisé durant la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **Cette formation est suivie d'un examen de certification HS2 ISO 27005 Risk Manager. L'examen est composé de deux parties : un QCM avec la norme sous les yeux et une étude de cas permettant de vérifier la capacité d'application pratique de la méthode. Une attestation de stage nominative est envoyée au service formation du client à l'issue de la formation.**

Programme

Introduction

- Normes ISO270XX
- ISO 27005 et les autres méthodes dont Ebios, Mehari, etc
- Vocabulaire du management du risque selon l'ISO 27005 :2022

Présentation interactive du vocabulaire fondamental et de l'approche empirique du management du risque avec la participation active des stagiaires à un exemple concret

- Identification et valorisation d'actifs
- Menaces et vulnérabilités
- Identification du risque et formulation sous forme de scénarios
- Estimation des risques
- Vraisemblance et conséquences d'un risque
- Évaluation des risques
- Différents traitements du risque
- Acceptation des risques
- Notion de risque résiduel

Norme ISO 27005 :2022

- Introduction
- Gestion du processus de management du risque
- Cycle de vie du projet et amélioration continue (modèle PDCA)
- Établissement du contexte
- Identification des risques
- Estimation des risques
- Évaluation des risques
- Traitement du risque
- Acceptation du risque
- Surveillance et réexamen des facteurs de risque
- Communication du risque

Exercices

Mise en situation : étude de cas

- Réalisation d'une appréciation de risque complète sur ordinateur
- Travail de groupe
- Simulation d'entretien avec un responsable de processus métier
- Présentation orale des résultats par le meilleur groupe
- Revue des résultats présentés

Examen de certification conçu, surveillé et corrigé par HS2