ISO 27005

Durée : 2 à 5 jours

Objectifs de la Formation

- Saisir les concepts fondamentaux de la sécurité de l'information et des normes ISO/IEC 27001 et 27005.
- Appliquer diverses méthodologies de gestion des risques en pratique
- Conduire des évaluations des risques efficaces et communiquer les résultats aux parties prenantes
- Identifier les actifs, les menaces et évaluer les risques de sécurité associés
- Etablir des plans de traitement des risques avec des mesures de sécurité appropriées Réussir l'examen de certification ISO/IEC 27005

Public Concerné

- Consultants en sécurité de l'information
- Gestionnaires des risques
- Risk managers

Prérequis

- Connaissances générales en sécurité des systèmes d'information

Programme de la Formation

Fondamentaux de la gestion des risques

- Définition du risque (ISO/IEC 27005:2022, EBIOS Risk Manager)
- Composantes du risque (actif, vulnérabilité, menace, scénario, calcul)
- Exercice 1 : Composer un risque · Vue d'ensemble des normes ISO/IEC
- Relation ISO 27001 et 27005 · Développement d'un programme de gestion des risques

Présentation de la norme ISO/IEC 27005 : 2022

- Structure de la norme · Cycle · PDCA (roue de Deming)
- Approche processus · Evolution : ISO/IEC 27005:2011 versus 2022

Phase de contexte

- Définition d'une organisation · Appétit pour le risque
- Exercice 2 : Etablir le contexte organisationnel
- Critères d'acceptation, d'évaluation et de probabilité des risques
- Exercice 3 : Etablir les critères organisationnels

Cycle d'analyse

- Approche basée sur les événements versus approche basée sur les actifs

Phase d'identification des risques

- Identification des actifs, vulnérabilités, menaces, conséquences
- Exercices 4 à 8 : Identifier actifs, événements, parties prenantes, chemins d'attaque, scénarios

Phase d’estimation et d’évaluation

- Approches qualitatives versus quantitatives · Diverses méthodes de calcul des risques
- Exercices 9 à 12 : Estimer gravité, probabilité, niveau de risque, prioriser

Phase de traitement et d’acception

- Options de traitement · Comparaison avec l'Annexe A d'ISO/IEC 27001
- Production d'une Déclaration d'Applicabilité (SoA) · Exercices 13 et 14

Communication et surveillance

- Plan de communication · Mise en place d'indicateurs PDCA

Alignement SMSI

- Contexte organisationnel · Leadership et engagement
- Exercices 15 et 16 : Matrice de communication · Scénario de surveillance
- Action corrective · Amélioration continue

Moyens Techniques et Humains

- Intervenant : Formateur professionnel spécialisé dans la continuité d’activité.
- Utilisation d'outils pédagogiques adaptés.

Méthodes Pédagogiques Mobilisées

- Alternance entre méthodes affirmatives, interrogatives et actives.
- Utilisation de ressources formatives, évaluatives et de mémorisation.

Évaluation

- **Tests intermédiaires :** exercices jalonnant l'ensemble de la formation
- **Projet pratique :** Simulation d'un environnement réel
- **Examen final :** Questions théoriques et exercices pratiques