

## ISO27035 Lead Incident Manager

Cette formation permet de développer les compétences pour maîtriser un modèle de mise en oeuvre des processus de gestion des incidents, en utilisant la norme ISO 27035 comme cadre de référence.

À partir d'exercices pratiques, les participants acquerront les connaissances et les compétences nécessaires pour gérer les incidents de sécurité à temps en prenant connaissance de leur cycle de vie.

Cette formation présente aux participants la norme ISO 27035 Gestion des incidents de la sécurité de l'information, un modèle pour concevoir et développer des processus de gestion des incidents des organisations, ainsi que la façon dont les entreprises peuvent utiliser la norme.

Cette formation est entièrement compatible avec la norme ISO 27035 qui soutient la norme ISO 27001 en fournissant des conseils pour la gestion des incidents.



### Détails

- **Code** : ISO-27035
- **Durée** : 5 jours ( 35 heures )

#### Public

- Membre d'une équipe de réponse aux incidents
- Responsable de la conformité réglementaire
- Responsable de la gestion des incidents
- Responsable de la gestion du risque de la sécurité de l'information
- Responsable des processus de l'entreprise

#### Pré-requis

- Connaissances de base en gestion d'incident.

### Objectifs

- Acquérir les compétences nécessaires à la mise en oeuvre, la gestion et la maintenance d'un programme de la gestion des incidents de la sécurité de l'information selon la norme ISO 27035.
- S'initier aux concepts, approches, méthodes et techniques permettant une gestion efficace des incidents de la sécurité de l'information selon la norme ISO 27035.
- Comprendre, interpréter et fournir des conseils sur la façon de mettre en oeuvre et de gérer les processus de la gestion des incidents, basés sur les meilleures pratiques de la norme ISO 27035 et d'autres normes associées.
- Acquérir les compétences nécessaires pour conseiller efficacement une organisation sur les meilleures pratiques en gestion de la sécurité de l'information.

### Programme

#### JOUR 1 - Introduction, Cadre de gestion des incidents selon la norme ISO 27035

- Concepts et définitions liés à la sécurité de l'information et à la gestion des incidents
- Normes et meilleures pratiques de la gestion des incidents
- Choisir un cadre de gestion des incidents

- Comprendre une organisation et son contexte

#### JOUR 2 - Planification de la mise en oeuvre des processus de gestion des incidents de l'organisation, basés sur la norme ISO 27035

- Stratégie de gestion des incidents et de gestion du projet

- Planification de la mise en C des processus efficaces de la gestion des incidents
- Analyse préliminaire et sélection d'une approche et d'une méthodologie
- Concevoir et documenter la détection des incidents, rapports et processus de gestion
- Définition des rôles et des responsabilités dans le contexte de la mise en œuvre et de la gestion des processus de gestion des incidents

### JOUR 3 – Mise en œuvre des processus de gestion des incidents

- Définir les documents et les processus de gestion des enregistrements
- Procédures et politiques de gestion des incidents
- Mise en œuvre des processus de sécurité et des contrôles liés à la gestion des incidents

- Processus de gestion des changements
- Processus d'analyse des incidents
- Communication efficace et stratégies de communication
- Créer une équipe de réponse aux incidents de la sécurité de l'information

### JOUR 4 – Surveillance , mesure et amélioration des processus de gestion des incidents

- Surveillance et évaluation de l'efficacité des processus de gestion des incidents dans les activités
- Développement des métriques, des indicateurs de performance et des tableaux de bord
- Revue de direction
- Mise en œuvre d'un programme d'amélioration continue
- Développer et proposer les meilleurs plans d'actions correctives et préventives

### JOUR 5 – Examen

#### Modalités

- **Type d'action** :Acquisition des connaissances
- **Moyens de la formation** :Formation présentielle - 1 poste par stagiaire - 1 vidéo projecteur - Support de cours fourni à chaque stagiaire
- **Modalités pédagogiques** :Exposés - Cas pratiques - Synthèse
- **Validation** :Exercices de validation - Attestation de stages