

CYBERSÉCURITÉ

## ISO / IEC 27035 : Gestion des incidents de sécurité

5 jours (35h00) | CS00015 | Num form : form-191 | Perfectionnement / Avancé

INFORMATIQUE / SÉCURITÉ IT / CYBERSÉCURITÉ

### À l'issue de ce stage vous serez capable de :

- Maîtriser les concepts, les approches, les méthodes, les outils et les techniques qui permettent une gestion efficace des incidents de sécurité de l'information selon l'ISO/CEI 27035
- Connaître la corrélation entre la norme ISO/CEI 27035 et les autres normes et cadres réglementaires
- Acquérir l'expertise nécessaire pour accompagner une organisation durant la mise en œuvre, la gestion et la tenue à jour d'un plan d'intervention en cas d'incident de la sécurité de l'information
- Acquérir les compétences pour conseiller de manière efficace les organismes en matière de meilleures pratiques de gestion de sécurité de l'information
- Comprendre l'importance d'adopter des procédures et des politiques bien structurées pour les processus de gestion des incidents
- Développer l'expertise nécessaire pour gérer une équipe efficace de réponse aux incidents

Ce Contenu de formation est proposé par [PECB](#)

### Niveau requis :

Pour suivre cette formation ISO 27035 Lead Incident Manager, une compréhension fondamentale de l'ISO / CEI 27035 et des connaissances approfondies sur la sécurité de l'information sont nécessaires. Vous pouvez les acquérir en suivant la formation ISO 27035 - Introduction (SGIS).

### Public concerné :

- Gestionnaires des incidents de sécurité de l'information
- Responsables des TIC
- Auditeurs des technologies de l'information

- Responsables souhaitant mettre en place une équipe de réponse aux incidents
- Responsables souhaitant apprendre davantage sur le fonctionnement efficace d'une équipe de réponse aux incidents
- Responsables des risques liés à la sécurité de l'information
- Administrateurs professionnels des systèmes informatiques
- Administrateurs professionnels de réseau informatique
- Membres de l'équipe de réponse aux incidents
- Personnes responsables de la sécurité de l'information au sein d'une organisation

## **Programme :**

### **Jour 1 - Introduction aux concepts relatifs à la gestion des incidents de sécurité de l'information, tels que définis par l'ISO/CEI 27035**

Objectifs et structure de la formation  
Cadres normatifs et réglementaires  
Gestion des incidents liés à la sécurité de l'information  
Processus de base de la norme ISO/CEI 27035  
Principes fondamentaux de la sécurité de l'information  
Corrélation avec la continuité des activités  
Questions légales et déontologiques

### **Jour 2 - Conception et préparation d'un plan de gestion des incidents de sécurité de l'information**

- Lancement d'un processus de gestion des incidents de sécurité de l'information  
Compréhension de l'organisation et clarification des objectifs de la gestion des incidents de sécurité de l'information  
Planifier et préparer  
Rôles et fonctions  
Politiques et procédures

### **Jour 3 - Lancement d'un processus de gestion des incidents et traitement des incidents de sécurité de l'information**

- Planification de la communication  
Premières étapes de la mise en oeuvre  
Mise en place des éléments de support  
Détection et rapport  
Évaluation et décisions  
Réponses  
Leçons apprises  
Transition aux opérations

### **Jour 4 - Suivi et amélioration continue du plan de gestion des incidents liés à la sécurité de l'information**

- Analyse supplémentaire  
Analyse des leçons apprises  
Mesures correctives  
Compétence et évaluation des gestionnaires  
d'incidents  
Clôture de la formation

### **Jour 5 - Examen de certification**

Ce Contenu de formation est proposé par [PECB](#)