ISO/IEC 27035 Lead Incident Manager, certification PECB

Code : NRE16 **Durée** : 5 jours **Classe** : Présentiel / à distance

Public

- Gestionnaires des incidents desécurité de l'information,responsables des TIC,administrateurs professionnels des systèmes informatiques, administrateurs professionnels de réseau informatique...

Prérequis

- Avoir une connaissance générale des processus de gestion des incidents, des principes de sécurité de l'information et de la famille de normes ISO/IEC 27000.

Objectifs

À l'issue de la formation l'apprenant sera en mesure de :

- Expliquer les principes fondamentaux de la gestion des incidents.
- Élaborer et mettre en oeuvre des plans de réponse aux incidents, sélectionner une équipe de réponse aux incidents.
- Réaliser des appréciations approfondies des risques afin d'identifier les menaces potentielles au sein d'un organisme.
- Appliquer les bonnes pratiques issues de diverses normes internationales.
- Effectuer une analyse après l'incident et identifier les leçons tirées de l'expérience.

Programme détaillé

1) Introduction aux concepts liés à la gestion des incidents de sécurité de l'information età la norme ISO/IEC 27035

- Objectifs et structure de la formation.
- Normes et cadres réglementaires.
- Concepts fondamentaux de la gestion des incidents.
- Gestion des incidents de sécurité de l'information.
- Établissement du contexte.
- Politiques et procédures.

2) Conception et préparation d'un plan de gestion des incidents de sécurité de l'information

- Management du risque.
- Plan de gestion des incidents.
- Équipe de gestion des incidents.
- Relations internes et externes.
- Assistance technique et autre.
- Sensibilisation et formation aux incidents de sécurité de l'information.

3) Détection et signalement des incidents liés à la sécurité de l'information

- Tests.
- Surveillance des systèmes et des réseaux.
- Détecter et alerter.
- Collecte d'informations sur les incidents.
- Signalement des événements liés à la sécurité de l'information.
- Appréciation des événements liés à la sécurité de l'information.

4) Surveillance et amélioration continue du processus de gestion des incidents liés à la sécurité de l'information

- Résolution des incidents liés à la sécurité de l'information.
- Confinement, éradication et récupération.
- Enseignements tirés.
- Surveillance, mesure, analyse et évaluation.
- Amélioration continue.

ISO/IEC 27035 Lead Incident Manager, certification PECB

Code : NRE16 **Durée** : 5 jours **Classe** : Présentiel / à distance

5) Certification

Domaines de compétences couverts par l'examen :

- Domaine 1 : Principes et concepts fondamentaux de la gestion des incidents de sécurité de l'information.
- Domaine 2 : Processus de gestion des incidents de sécurité de l'information basé sur la norme ISO/ IEC 27035.
- Domaine 3 : Conception d'un processus organisationnel de gestion des incidents basé sur la norme ISO/IEC 27035.
- Domaine 4 : Préparation et exécution du plan de réponse aux incidents liés à la sécurité de l'information.
- Domaine 5 : Mise en oeuvre de processus de gestion des incidents liés à la sécurité de l'information ce en différé.
- Domaine 6 : Amélioration des processus et des activités de gestion des incidents.