

ISO 27035 - Gestion des incidents de sécurité de l'information - Lead Incident Manager

Référence : SEC27035LI

Durée : 5 jours

Certification : ISO 27035

Code CPF : RS4326

CONNAISSANCES PREALABLES

- Une compréhension fondamentale de l'ISO / CEI 27035 et des connaissances approfondies sur la sécurité de l'information..

PROFIL DES STAGIAIRES

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

OBJECTIFS

- 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 .

CERTIFICATION PREPAREE

- PECB Certified ISO/CEI 27035 Lead Incident Manager. Pour en savoir plus sur cette certification [cliquez ici](#) et accédez aux informations complètes fournies par France Compétences

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Management de la sécurité

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

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

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

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 œuvre
- Mise en place des éléments de support
- Détection et rapport
- Évaluation et décisions
- Réponses
- Leçons apprises
- Transition aux opérations

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

Examen de certification

- Révision et passage de l'examen de certification