ISO/IEC 27035 Lead Incident Manager (PECB certified) - Including Exam

Durée: 5 Jours **Réf de cours: ISO27035LI** **Version: 2.0**

Résumé:

La formation **ISO/IEC 27035 Lead Incident Manager** vous permet d'acquérir l'expertise nécessaire pour accompagner une organisation dans la mise en œuvre d'un **plan de gestion des incidents de sécurité de l'information**, conformément à la norme **ISO/IEC 27035**. Au cours de cette formation, vous développerez une connaissance approfondie d'un modèle de processus pour concevoir et élaborer un plan organisationnel de gestion des incidents. La compatibilité de cette formation avec **ISO/IEC 27035** soutient également la mise en œuvre de **ISO/IEC 27001**, en fournissant des orientations pour la gestion des incidents de sécurité de l'information.

Après avoir maîtrisé tous les concepts nécessaires à la gestion des incidents de sécurité de l'information, vous pourrez passer l'examen et demander la certification **PECB Certified ISO/IEC 27035 Lead Incident Manager**. En obtenant le certificat PECB Lead Incident Manager, vous serez en mesure de démontrer que vous possédez les connaissances pratiques et les compétences professionnelles nécessaires pour soutenir et diriger une équipe dans la gestion des incidents de sécurité de l'information.

Mise à jour : 14.01.2026

Public visé:

Gestionnaires des incidents de sécurité de l'information Responsables informatiques (IT Managers) Auditeurs informatiques (IT Auditors) Managers souhaitant établir une équipe de réponse aux incidents (IRT) Managers souhaitant en savoir davantage sur le fonctionnement efficace des IRT Gestionnaires des risques en sécurité de l'information Professionnels de l'administration des systèmes informatiques Professionnels de l'administration des réseaux informatiques Membres des équipes de réponse aux incidents Personnes responsables de la sécurité de l'information au sein d'une organisation

Objectifs pédagogiques:

- A l'issue de la formation vous saurez :
- Maîtriser les concepts, approches, méthodes, outils et techniques permettant une gestion efficace des incidents de sécurité de l'information conformément à l'ISO/IEC 27035
- Reconnaître la corrélation entre l'ISO/IEC 27035 et d'autres normes et cadres réglementaires
- Acquérir l'expertise nécessaire pour aider une organisation à mettre en œuvre, gérer et maintenir efficacement un plan de réponse aux incidents de sécurité de l'information
- Acquérir la compétence pour conseiller efficacement les organisations sur les meilleures pratiques en matière de gestion des incidents de sécurité de l'information
- Comprendre l'importance d'établir des procédures et des politiques bien structurées pour les processus de gestion des incidents
- Développer l'expertise nécessaire pour gérer une équipe de réponse aux incidents de manière efficace

Pré-requis:

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

Test et certification

Certification :

- L'examen PECB dure 3 heures et comprend 80 questions (QCM).
- Un score de 70 % minimum est requis pour l'obtention de la certification PECB Lead Incident Manager – ISO/IEC 27035.
- Livre ouvert autorisé
- Un voucher pour passer l'examen sera remis par Global Knowledge au candidat à la certification au moment de sa formation.
- Après sa formation, le candidat planifiera le passage de son examen en s'inscrivant sur le site de PECB
- L'examen se fera en ligne sous la surveillance d'un « Proctor »
- Le formateur donnera toutes les indications utiles pour l'inscription et les conditions de passage

- En cas d'échec, un Second passage est possible dans l'année
- La certification est délivrée par PECB, et reste valable sans limite de durée.
- Un temps de préparation est recommandé entre la formation et le passage de la certification

Contenu:

Jour 1 : Introduction à la gestion des incidents de sécurité de l'information

Démarrage de la formation

- Présentation des enjeux, tour de table des participants, identification des attentes, présentation du déroulé pédagogique et des modalités d'évaluation.

Module 1 – Présentation du cours :

- Objectifs de la formation, parcours, attentes des participants

Module 2 – Vue d'ensemble de la norme ISO/CEI 27035 :

- Terminologie, historique, structure des parties ISO/IEC 27035 (1, 2, 3)

Lien avec ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 22301

Module 3 – Concepts fondamentaux de gestion des incidents :

- Cycle de vie de l'incident, classification, distinction événements vs incidents

Module 4 – Gouvernance et rôles organisationnels :

- Rôles des responsables, coordination transversale, implication de la direction

Jour 2 : Préparation organisationnelle à la gestion des incidents

Module 5 – Politique et objectifs de gestion des incidents :

- Alignement stratégique, documentation, intégration dans le SMSI

Module 6 – Définition de l'équipe de gestion des incidents (CSIRT) :

- Structure, responsabilités, compétences clés, coordination avec les parties externes

Module 7 – Ressources et capacités techniques :

- Journalisation, outils de détection, systèmes SIEM, capacités de réponse

Module 8 – Sensibilisation et formation :

- Plans de communication, simulations régulières, culture sécurité

Jour 3 : Processus opérationnels de réponse aux incidents

Module 9 – Identification et enregistrement des incidents :

- Sources de détection, canaux d'alerte, priorisation, enregistrement

Module 10 – Évaluation et classification :

- Évaluation de l'impact, typologie des incidents, gravité, seuils d'escalade

Module 11 – Réponse aux incidents :

- Processus de contention, éradication, remédiation, retour au fonctionnement normal

Module 12 – Communication pendant un incident :

- Notification interne/externe, parties prenantes, obligations réglementaires (CNIL, ANSSI, etc.)

Jour 4 : Suivi post-incident, amélioration et continuité

Module 13 – Analyse post-incident (lessons learned) :

- Revue d'incident, identification des faiblesses systémiques, rapport formel

Module 14 – Intégration avec la continuité d'activité :

- Relations avec le PCA, PRA, processus critiques, résilience

Module 15 – Amélioration continue :

- Définition d'indicateurs, revue des incidents, audit et révision de la procédure

Module 16 – Atelier de simulation de crise :

- Étude de cas en conditions réelles : coordination CSIRT, communication, décision

Jour 5 : Révision générale et préparation a l'examen PECB

Session de révision :

- Quiz, résumé des points critiques, échange de bonnes pratiques
- Examen blanc
- Étude de cas + QCM simulant l'examen officiel PECB
- Correction collective avec justification des réponses.
- Clôture de la session et remise des conseils personnalisés.
- Préparation à l'examen
- Séance de questions/réponses
- Conseils méthodologiques pour réussir l'examen (structure, types de questions)
- Gestion du temps

Clôture de la formation

o Bilan à chaud, restitution des acquis, recueil des impressions des participants.

Méthodes pédagogiques :

Répartition Théorie/Pratique
55 % de théorie : La maîtrise des normes, concepts et principes de la gestion des incidents de sécurité de l'information. La gouvernance, la structuration des équipes, les politiques, et l'intégration dans le SMSI.
45% de pratique : Ateliers opérationnels (analyse post-incident, classification des incidents, planification d'actions correctives), jeux de rôle et simulations (communication en temps de crise, coordination d'un CSIRT), Exercices appliqués (étude de cas, gestion d'incident simulée, rédaction de rapports, préparation à l'examen PECB).

Documentation :
Les documents sont accessibles au format électronique via le lecteur Kate (https://pecb.com/kate/) et mis à disposition lors de l'examen. Notez que la création préalable d'un compte personnel sur le site de PECB est nécessaire non seulement pour suivre la formation, mais également pour créer son profil d'examen en ligne et programmer une session.

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement