EduGroupe
Accompagner pour réussir

ISO/IEC 27035 - Information Security Incident Management - Manager

Référence : **SEC27035LIA** Durée : **5 jours (35 heures)** Certification : **ISO/IEC 27035 - Security Incident Manager de PECB**

Connaissances préalables

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

Profil des stagiaires

- RSSI, consultants ou auditeurs en cybersécurité, chefs de projet SSI ou gestion de crise, ou toute personne impliquée dans la gestion des incidents de sécurité de l'informatique

Objectifs

- Connaître l'ensemble des principes, techniques et méthodologie de la gestion des incidents de la sécurité de l'information
- Connaître la relation entre la norme ISO/IEC 27035 et les autres normes et cadres réglementaires
- Gérer une équipe adéquate pour le suivi et la gestion des incidents
- Mettre en place et piloter un processus de gestion des incidents
- Analyser les incidents et améliorer les processus

Certification préparée

Durée de l'examen : 3 heures. Format : réponses rédigées à 12 questions portant sur des études de cas en français. Modalité : en-dehors du temps de formation, via Internet, sous e-surveillance, à livre ouvert. Le support de cours contient les extraits de norme(s) nécessaires au passage de l'examen. Un deuxième passage est offert dans un délai d'un an si la première tentative n'est pas couronnée de succès.

Méthodes pédagogiques

- Groupes de 4 à 12 personnes
- Apports théoriques illustrés d'exemples concrets
- Exercices pratiques
- Étude de cas fil rouge
- Accès à une documentation pédagogique numérique
- Utilisation d'outils collaboratifs (Miro, Wooclap) pour la co-construction
- Signature d'une feuille d'émargement pour attester de la présence à chaque demi-journée de formation

Formateur

- Consultant-Formateur expert Gestion d'incident cybersécurité, certifié ISO27035

Méthodes d'évaluation des acquis

- Participation et réalisation d'exercices tout au long de la formation
- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestations des compétences acquises et de fin de stage adressée à chaque participant

Contenu du cours

1. JOUR 1 - Introduction aux concepts de gestion des incidents liés à la sécurité de l'information et à la norme ISO/IEC 27035 (7 heures)

2. Section 1 : Objectifs et structure de la formation (0h30)

- Introduction
- Informations générales
- Objectifs d'apprentissage
- Approche éducative
- Examen et certification
- À propos de PECB

3. Section 2 : Normes et cadres réglementaires (0h40)

- Qu'est-ce que l'ISO ?
- La famille de normes ISO/IEC 27000
- ISO/IEC 27035-1, ISO/IEC 27035-2 et ISO/IEC 27035-3
- Avantages de la série ISO/IEC 27035
- 💡 *Quiz*

4. Section 3 : Concepts fondamentaux de la gestion des incidents (1h20)

- Sécurité de l'information
- Triade CIA
- Vulnérabilités et menaces
- Risques liés à la sécurité de l'information
- Événement lié à la sécurité de l'information et incident lié à la sécurité de l'information
- Gestion des incidents
- Plan de réponse aux incidents
- Confidentialité des informations
- Classification des mesures
- Quiz
- Exercice 1

5. Section 4 : Gestion des incidents liés à la sécurité de l'information (0h50)

- Objectifs de la gestion des incidents
- Gestion des incidents liés à la sécurité de l'information et SMSI
- Approche structurée de la gestion des incidents liés à la sécurité de l'information
- Cadre de gestion des incidents liés à la sécurité de l'information de PECB
- 💡 *Quiz*

6. Section 5 : Mise en place du contexte (1h)

- Définir le domaine d'application de la gestion des incidents
- Envisager les limites du domaine d'application de la gestion des incidents
- Analyser l'environnement interne et externe
- Identifier et analyser les parties intéressées
- Effectuer une analyse des lacunes
- 💡 *Quiz*

7. Section 6 : Politiques et procédures (2h40)

- Politiques, plans et processus
- Politique de gestion des incidents
- Rédaction d'une politique de gestion des incidents
- Communication des politiques et des procédures
- 💡 *Quiz*
- 💡 *Discussion commune à partir d'un scénario*

8. JOUR 2 - Conception et préparation d'un plan de gestion des incidents liés à la sécurité de l'information (7 heures)

9. Section 7 : Gestion des risques (0h70)

- Détermination de l'approche d'identification des risques
- Techniques d'analyse des risques
- Appréciation des niveaux de risque
- Priorisation des risques
- Options de traitement des risques
- Plan de traitement des risques
- 💡 *Quiz*

10. Section 8 : Plan de gestion des incidents (0h80)

- Plan de gestion des incidents
- Fonctions et responsabilités
- Contenu du plan de gestion des incidents
- Examen des processus et procédures documentés
- 💡 *Quiz*
- 💡 *Exercice 2*

11. Section 9 : Équipe de gestion des incidents (0h50)

- Équipe de gestion des incidents
- Fonctions et responsabilités
- Coordinateur des incidents
- Structure de l'équipe de réponse aux incidents
- 💡 *Quiz*

12. Section 10 : Relations internes et externes (1h)

- Relations avec les autres parties de l'organisme
- Relations avec les parties intéressées externes
- Partage d'informations concernant des incidents avec des parties extérieures
- Principes d'une stratégie de communication efficace
- Informations documentées
- 💡 *Quiz*

13. Section 11 : Assistance technique et autres types d'assistance (0h40)

- Définition de l'assistance technique et d'autres types d'assistance
- Exemples d'assistance technique
- Exemples d'autres types d'assistance
- 💡 *Quiz*

14. Section 12 : Sensibilisation et formation aux incidents liés à la sécurité de l'information (2h)

- Programmes et activités de sensibilisation
- Besoins, programmes et activités de développement des compétences
- Évaluation du développement des compétences
- 💡 *Quiz*
- 💡 *Discussion commune à partir d'un scénario*

15. JOUR 3 - Détection et signalement des incidents liés à la sécurité de l'information (7 heures)

16. Section 13 : Tests (1h)

- Systèmes de test
- Techniques de test
- Déterminer les étapes du test
- Déterminer les techniques de test
- Préparation du test et de la documentation
- Activités post-tests
- 💡 *Quiz*

17. Section 14 : Surveillance des systèmes et réseaux (1h)

- Surveillance de la capacité de réponse aux incidents
- Surveillance des réseaux
- Surveillance des systèmes
- Surveillance continue de la sécurité de l'information (SCSI)
- Surveillance de la sécurité
- Évaluation de la performance
- Indicateurs de sécurité de l'information
- 💡 *Quiz*

18. Section 15 : Détection et alerte (1h20)

- Détection et signalement
- Mécanismes de détection des incidents de sécurité
- Méthodologie et objectifs des attaquants
- Signes d'un incident
- Processus de classification des incidents
- Niveaux de classification des incidents
- 💡 *Quiz*
- 💡 *Exercice 3*

19. Section 16 : Collecte d'informations pour les incidents (0h40)

- Approche de la collecte d'informations
- Sources d'information
- Conscience de la situation
- Collecte d'informations sur les incidents liés à la sécurité de l'information
- 💡 *Quiz*

20. Section 17 : Signalement des événements liés à la sécurité de l'information (1h)

- Signalement des événements liés à la sécurité de l'information
- Fournir des informations fondamentales sur l'incident de sécurité de l'information
- Analyser l'incident
- Documenter les dommages et les blessures
- Soumettre un rapport
- 💡 *Quiz*

21. Section 18 : Appréciation des événements liés à la sécurité de l'information (2h)

- Appréciation des événements liés à la sécurité de l'information
- Principales activités de la phase d'appréciation et de décision
- Évaluation des événements de sécurité de l'information et prise de décision
- Signalement des événements liés à la sécurité de l'information
- Priorisation de l'incident
- Quiz
- Discussion commune à partir d'un scénario

22. JOUR 4 - Surveillance et amélioration continue du système de management de la sécurité de l'information (7 heures)

23. Section 19 : Résolution des incidents liés à la sécurité de l'information (1h)

- Cycle de vie de la réponse aux incidents
- Fonctions et responsabilités au cours de la phase de réponse
- Réponse aux incidents de sécurité de l'information
- 💡 *Quiz*

24. Section 20 : Endiguement, éradication et rétablissement (1h30)

- Stratégie d'endiguement
- Critères de détermination de la stratégie
- Isolement de l'incident
- Identification des indicateurs de compromission
- Documentation des preuves
- Évaluation des options de sauvegarde
- 💡 *Quiz*
- 💡 *Exercice 4*

25. Section 21 : Apprentissage des enseignements (1h)

- Apprentissage des enseignements
- Identification des domaines à améliorer
- Amélioration du plan de gestion des incidents liés à la sécurité de l'information
- Évaluation de l'équipe de gestion des incidents (EGI)
- Amélioration de la mise en œuvre des mesures de sécurité de l'information
- Amélioration des résultats de l'appréciation des risques liés à la sécurité de l'information et de la revue de direction
- 💡 *Quiz*

26. Section 22 : Surveillance, mesurages, analyse et évaluation (1h)

- Déterminer les objectifs de mesure
- Définir ce qui doit être surveillé et mesuré
- Établir des indicateurs de performance pour la gestion des incidents liés à la sécurité de l'information
- Déterminer la fréquence et la méthode de surveillance et de mesure
- Signaler les résultats
- 💡 *Quiz*

27. Section 23 : Amélioration continue (2h10)

- Surveillance continue des facteurs de changement
- Maintien et amélioration de la gestion des incidents liés à la sécurité de l'information
- Mise à jour permanente des informations documentées
- Documentation des améliorations
- 💡 *Quiz*
- 💡 *Discussion commune à partir d'un scénario*

28. Section 24 : Clôture de la formation (0h20)

- Programme de certification de PECB
- Processus de certification PECB
- 💡 *Quiz*

29. JOUR 5 - Révisions encadrées (7 heures)

- Rappel structuré des acquis des Jours 1 à 4
- 💡 *Quiz de réactivation global*
- Étude de cas intégrative
- Audit blanc
- 💡 *Élaboration d'un plan d'amélioration*
- 💡 *Simulation d'examen*
- Synthèse finale et projection

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.