EduGroupe
Accompagner pour réussir

Risk Manager - Certification ISO/IEC 27005

Référence : **SECRM27005A** Durée : **3 jours (21 heures)** Certification : **ISO/IEC 27005 Risk Manager de PECB**

Connaissances préalables

- Une connaissance de base sur la gestion du risque et sur la sécurité des systèmes d'information

Profil des stagiaires

- RSSI, Chefs de projets, consultants ou toute personne en charge de la sécurité d'information, de la conformité et du risque dans une organisation

Objectifs

- Comprendre les concepts clés de la gestion des risques comme définis par la norme ISO/IEC 27005
- Interpréter les exigences de la gestion des risques au sein d'un SMSI conforme à la norme ISO/IEC 27001
- Identifier, évaluer et traiter les risques liés à la sécurité de l'information

Certification préparée

Durée de l'examen : 2 heures. Format : un QCM de 60 questions 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. Taux de réussite constaté chez EduGroupe pour cette certification en 2024 : 94%

Méthodes pédagogiques

- Groupe 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 GRC (Gouvernance, Risk & Compliance), certifié ISO27001, ISO27005 Risk Manager et EBIOS Risk Manager

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 à la norme ISO/IEC 27005 et à la gestion des risques (7 heures)

2. Section 1 : Objectifs et structure de la formation (0h20)

- Introduction
- Informations générales
- Objectifs de la formation
- Approche éducative
- Examen et certification

3. Section 2 : Normes et cadres réglementaires (1h10)

- Qu'est-ce que l'ISO ?
- La famille de normes ISO/IEC 27000
- ISO/IEC 27001
- ISO/IEC 27005
- ISO 31000
- IEC 31010
- Avantages de la gestion des risques
- 💡 *Quiz*

4. Section 3 : Principes et concepts fondamentaux de la gestion des risques liés à la sécurité de l'information (2h)

- Sécurité de l'information
- Confidentialité, intégrité et disponibilité
- Définitions des notions d'événement, d'opportunité, de conséquence et de vraisemblance
- Menace et vulnérabilité
- Définition des notions de risque et de risque lié à sécurité de l'information
- Types de mesures de sécurité
- Principes de gestion des risques
- 💡 *Quiz*
- 💡 *Exercice 1*

5. Section 4 : Programme de gestion des risques liés à la sécurité de l'information (1h10)

- Leadership et engagement
- Responsabilités et obligations
- Processus de gestion des risques
- Cycles de gestion de risques
- 💡 *Quiz*

6. Section 5 : Établissement du contexte (2h20)

- L'organisation et son contexte
- Exigences des parties intéressées
- Objectifs de gestion des risques et critères de risque
- Domaine d'application et limites
- Méthode de gestion des risques liés à la sécurité de l'information
- Activités pour l'appréciation des risques
- 💡 *Quiz*
- 💡 *Discussion commune sur le scénario 1*

7. JOUR 2 - Appréciation des risques, traitement des risques, communication des risques et concertation selon ISO/IEC 27005 (7 heures)

8. Section 6 : Identification des risques (1h20)

- Détermination de l'approche d'identification des risques
- Techniques de collecte de l'information
- Identification des risques liés à la sécurité de l'information
- Identification des propriétaires des risques
- 💡 *Quiz*

9. Section 7 : Analyse des risques (1h20)

- Techniques d'analyse des risques
- Appréciation des conséquences potentielles
- Appréciation de la vraisemblance
- Détermination des niveaux de risque
- 💡 *Quiz*

10. Section 8 : Évaluation du risque (1h10)

- Évaluation des niveaux de risque
- Hiérarchisation des risques
- Exemples d'appréciation des risques
- 💡 *Quiz*

11. Section 9 : Traitement du risque (1h20)

- Options de traitement du risque
- Plan de traitement du risque
- Évaluation du risque résiduel
- 💡 *Quiz*

12. Section 10 : Communication et concertation relatives aux risques de sécurité de l'information (1h50)

- Principes d'une stratégie de communication efficace
- Objectifs de communication des risques
- Plan de communication des risques
- Communication interne et externe
- 💡 *Quiz*
- Discussion commune sur le scénario 2

13. JOUR 3 - Enregistrement et rapports des risques, surveillance et revue, et méthodes d'appréciation des risques

14. Section 11 : Communication et concertation relatives aux risques liés à la sécurité de l'information (1h20)

- Documentation des processus de gestion des risques
- Valeur des informations documentées
- Documentation des résultats de gestion des risques
- Registres des risques
- Rapports des processus de gestion des risques
- 💡 *Quiz*

15. Section 12 : Surveillance et revue des risques de sécurité de l'information (1h)

- Surveillance et revue des facteurs de risque
- Surveillance et revue de la gestion des risques
- Actions correctives
- Amélioration continue
- 💡 *Quiz*

16. Section 13 : Méthodologies OCTAVE et MEHARI (1h10)

- Méthodologie OCTAVE
- OCTAVE-S
- OCTAVE Allegro
- OCTAVE FORTE
- MEHARI
- 💡 *Quiz*

17. Section 14 : Méthode EBIOS et cadre de gestion NIST (1h10)

- Qu'est-ce que l'EBIOS ?
- Une démarche itérative en 5 ateliers
- Processus de gestion des risques selon NIST
- Cadre de gestion des risques NIST
- Étapes du cadre de gestion NIST
- 💡 *Quiz*

18. Section 15 : Méthodes CRAMM et EMR (2h)

- Méthode CRAMM
- Étapes de la méthode CRAMM
- Appréciation des risques CRAMM
- EMR
- 💡 *Quiz*
- 💡 *Discussion commune sur le scénario 2*

19. Section 16 : Clôture de la formation (0h20)

- Programme de certification PECB
- Processus de certification de PECB

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.